*TECHNO REVIEW* | 2022 | ISSN 2695-9933
*International Technology Science and Society Review / Revista Internacional de Tecnología Ciencia y Sociedad*
https://doi.org/10.37467/revtechno.v11.4486


# DERECHOS HUMANOS Y NUEVAS TECNOLOGÍAS

Human rights and new technologies

ROSA MARÍA RICOY CASAS
Universidad de Vigo, España

**KEYWORDS**

*Fundamental Rights*
*Technologies*
*Artificial intelligence*
*Algorithms*
*Social score*
*Data protection*
*Politics*

**ABSTRACT**

*Numerous risks have been evidenced not only for data protection, but in general for the fundamental rights of the person such as equality and freedom with the use of numerous technological applications. Ethical biases and dilemmas in the application of artificial intelligence and algorithms, interference in electoral processes or control and social score techniques for political purposes are analyzed. It reflects on the dysfunctions and inequities of many of these new tools for citizenship, and proposes solutions that generate well-being for our democratic societies.*

**PALABRAS CLAVE**

*Derechos fundamentales*
*Tecnología*
*Inteligencia artificial*
*Algoritmos*
*Control social*
*Protección de datos*
*Política*

**RESUMEN**

*Se han evidenciado numerosos riesgos no solo para la protección de datos, sino en general para los derechos fundamentales de la persona como la igualdad y la libertad con la utilización de numerosas aplicaciones tecnológicas. Se analizan los sesgos y dilemas éticos en la aplicación de la Inteligencia artificial y los algoritmos, la injerencia en los procesos electorales o las técnicas de control y social score con fines políticos. Se reflexiona sobre las disfunciones e inequidades de muchas de estas nuevas herramientas para la ciudadanía, y se proponen soluciones que generen bienestar a nuestras sociedades democráticas.*

Recibido: 17/ 08 / 2022
Aceptado: 16/ 10 / 2022

## 1. Introducción

Vivimos en la denominada "Revolución 4.0" por el desarrollo de las tecnologías disruptivas que forman parte de su ecosistema ("Internet of Things IoT y 5G, big/smart data, blockchain, inteligencia artificial y algoritmos, impresión 3D y 4D, robótica, realidad virtual y aumentada, hologramas, coches y armas autónomas, etc.). Se habla incluso de cambios clave en la democracia, debido principalmente a la capacidad de la que disponen estos sistemas para perfilarnos con una exactitud increíble (por ejemplo los data brokers); ningún partido político desprecia sus utilidades (neuromarketing, geomarketing, microtargeting, etc.) y conocen nuestros propios sesgos (de confirmación, asortatividad, homofilia, etc.) y cómo nos relacionamos en el ámbito social, especialmente a través de las redes sociales (echo cameras, burbujas filtro, etc.), para "persuadirnos" políticamente con precisión de cirujano (gracias a los spin doctors, los asesores de los líderes políticos). De hecho, en España ya ha tenido que actuar el Tribunal Constitucional para derogar preceptos controvertidos relacionados a procesos electorales, aspectos clave de un sistema democrático (lo mismo que en el ámbito de la Unión Europea (UE) e incluso Internacional como el caso de (CA) Cambridge Analytica). Ello ha evidenciado numerosos riesgos no solo para la protección de datos, sino en general para los derechos fundamentales básicos de la persona como la igualdad y la libertad.

Es necesaria una nueva declaración de derechos humanos adaptada a las nuevas tecnologías que modifican nuestra vida con una intensidad y gravedad perturbadoras. Es próximo incluso el denominado "momento de la singularidad" (cuando las máquinas, gracias a la inteligencia artificial, sean capaces de auto-mejorarse, creando una generación de computadores muy superiores a la inteligencia humana). Este trabajo pretende reflexionar sobre las disfunciones e inequidades de muchas de estas nuevas herramientas para la ciudadanía, y proponer soluciones que generen bienestar a nuestras sociedades democráticas. También debe aproximar estas cuestiones a las personas, en un lenguaje y con una comprensión del problema que las empodere con criticismo.

Este trabajo ha partido para su realización de una revisión a través de las principales bases de datos bibliográficas, documentación de organismos públicos y privados, y noticias de prensa. Se definieron criterios de inclusión y exclusión, y un conjunto de variables para analizar las características de los artículos seleccionados. A partir de esta información se realizó el trabajo de carácter descriptivo, profundizando y reflexionando sobre su actualidad, el futuro y la importancia de estas herramientas en relación con la política.

## 2. Inteligencia artificial y algoritmos. Sesgos y dilemas éticos

Es esa Inteligencia Artificial (IA)[1] que a veces ni siquiera percibimos, la que ya tiene un desarrollo considerable[2], y no tanto en esos robots apocalípticos de la filmografía, que se proponen dominar el mundo, como la película EVA, donde se aborda el hito de la máquina que empieza a tener carácter y se aminora su deber de obediencia al humano marcado por las tres reglas de Isaac Asimov. Ya existe cierta preocupación sobre la posibilidad de que los sistemas de inteligencia artificial alcancen o superen las capacidades equivalentes humanas (la llamada superinteligencia). Son recurrentes los debates sobre la tecnoética del transhumanismo, pues existen casos en los que el sueño de la creación del ser humano biónico, el *ciborg*, es, ya casi, una realidad.

Los algoritmos están en los buscadores de Internet, en las películas sugeridas por las plataformas digitales, en las aplicaciones para ligar, para cribar quién pasa primero en la cola de urgencias de un hospital, para asignar prestaciones de desempleo, decidir quién mantiene un puesto de trabajo o quién da el perfil para una entrevista, etc. Los avances tecnológicos se visten de objetividad. Parecen neutros, sin ideología, y a veces son solo comprensibles por los técnicos. Eso facilita que sus fórmulas permanezcan fuera del escrutinio público y muy alejadas de otro tipo de controles, como el parlamentario. Incluso, en algunos foros se empieza a hablar de „algocracia". Hay cuatro aspectos que deben resaltarse en relación al funcionamiento de la IA y los algoritmos: 1) No son infalibles: numerosos ejemplos corroboran la idea de que es un tipo de tecnología no ajena al error; 2) Heredan sesgos de los programadores, usuarios y bases de datos o fuentes de información de las que se nutren;

1 Sobre el concepto, desarrollo, principales aplicaciones y políticas públicas en la Unión Europea de la inteligencia artificial: (Ricoy-Casas, 2019).

2 Estamos utilizando IA: a) cuando buscamos información en internet; b) cuando alguna plataforma de servicios audiovisuales nos recomienda un programa o una película según nuestros gustos; c) cuando utilizamos el móvil para hacer una foto y el recuadro reconoce los rostros; d) para traducir de un idioma a otro; e) para generar subtítulos en los vídeos; f) para bloquear el correo electrónico no solicitado (spam); g) en los asistentes virtuales de las principales plataformas como: Siri de Apple, Google Assistant de Google, Cortana de Microsoft, o Alexa y Echo de Amazon); h) en las respuestas automatizadas; i) en la clasificación de imágenes; j) para la conversión en texto a diálogo y viceversa; k) en los vehículos autónomos; l) cuando usamos una aplicación móvil para encontrar la mejor manera de ir a nuestro próximo destino; m) en casa (por ejemplo, un termostato inteligente puede reducir las facturas de energía hasta en un 25% al analizar los hábitos de las personas que viven en ella y ajustar la temperatura en consecuencia) (Hay, 2016); n) en el sector sanitario, por ejemplo los algoritmos pueden ayudar a los dermatólogos a realizar un mejor diagnóstico, detectando el 95% de los cánceres de piel, aprendiendo de grandes conjuntos de imágenes médicas (The Guardian, 2018); o) permite indexar probabilísticamente imágenes de texto manuscrito, lo que permite realizar búsquedas textuales en colecciones masivas de este tipo de documentación histórica sin transcribir, por ejemplo, de colecciones de interés para la arqueología subacuática pertenecientes al Archivo General de Indias como las realizadas por el Proyecto Carabela (2019); p) un sistema de inteligencia artificial desarrollado por el MIT permite descifrar lenguas desaparecidas o que ya no se usan, y conocer más sobre las personas que las hablaron (Victoria y Nadal, 2020); q) pueden ayudar a las empresas a identificar qué máquinas necesitan mantenimiento antes de averiarse (Thomas, 2019); y r) la IA puede mejorar la detección e investigación de actividades delictivas (por ejemplo, lavado de dinero, fraude fiscal); entre otras.

3) Es difícil su verificabilidad 100% debido a su sistema de aprendizaje autónomo; 4) No son completamente transparentes, y las empresas se amparan en derechos de propiedad intelectual e industrial para no tener que explicar los detalles de su programación, de ahí que se denominen "Black boxes".

1) No son infalibles: numerosos ejemplos corroboran la idea de que es un tipo de tecnología no ajena al error: a) Microsoft se vio obligada a retirar en marzo de 2016 su *chatbot* de inteligencia artificial llamado *Tay*. Tras apenas 100.000 tuits, 155.000 seguidores y 16 horas de vida, comenzó a emitir juicios y opiniones políticamente incorrectos, lo que llevó a sus creadores a apagarla (*The Guardian*, 2016) (*El País*, 2016) (*El Mundo*, 2016) (*Público*, 2017); b) En junio de 2015, un usuario de *Google Photos* descubrió que el programa etiquetaba a sus amigos negros como gorilas. La inteligencia artificial de Google no era capaz de distinguir una tez oscura de humano de la de simios como gorilas y chimpancés. Para que el programa no confunda a humanos con gorilas, sacaron a los gorilas del buscador, y a los chimpancés, y a los monos (*El País*, 2018) (*El Mundo*, 2018); c) La empresa estadounidense *Northpointe desarrolló un algoritmo para predecir la probabilidad de que un delincuente reincidiera y este empezó a juzgar que las personas de color eran más proclives a volver a cometer un crimen que los blancos* (Fundación Telefónica, 2017); d) Se han constatado numerosos fallos en vehículos autónomos, por ejemplo, el accidente mortal ocurrido en Tempe (Arizona) EE.UU., con un coche de Uber (*El País*, 2018b); e) El "Promobot IR77" era un robot ruso que estaba siendo diseñado con el fin de tener interacciones cara a cara con humanos y aprender de los mismos. Se estaba sometiendo a pruebas de movilidad y se programó para que se moviera libremente por una habitación durante una hora y luego regresara a un lugar designado. En una de las pruebas, salió por segunda vez de las instalaciones, y se dirigió a una carretera cercana hasta que se agotó la batería, quedándose frente a un autobús de cercanía y con el tráfico paralizado. El experto afirmó que habían programado el robot para tratar de evitar obstáculos, y no se había pensado que buscaría maneras de abandonar el centro de investigación (*The Washington Post*, 2016) (*Mirror,* 2016). *Los personajes no controlados por jugadores del videojuego Elite: Dangerous comenzaron a desarrollar por su cuenta armas que no estaban en el diseño original del juego. De esta forma, los jugadores humanos se enfrentaban a naves equipadas con armamento grotesco que los destruía en pedazos* (Fundación Telefónica, 2017). Sin duda, también constituyen ejemplos y metáforas de algunos de los temores con los robots y en general con aplicaciones que utilicen este tipo de inteligencia artificial o superinteligencia, que la autonomía derive en un comportamiento perjudicial para los seres humanos.

Según lo señalado, muchas de estas situaciones no se producen de manera deliberada, y es el propio sistema el que, en el procesamiento de información, puede producir errores asociando los datos. Téngase presente que, en el caso de sistemas con capacidad de aprendizaje (*machine learning*), la lógica computacional no está predeterminada, no se trata de "*locked softwares*"; permite a la máquina no solo analizar y procesar, sino aprender de miles o millones de datos para ofrecer soluciones de forma autónoma. De esta manera, en no pocas ocasiones, se desconoce la forma en que se ha producido un resultado determinado ni cómo se han procesado los datos por la máquina. Estas capacidades de aprendizaje otorgan a los algoritmos cierto grado de autonomía, lo que hace que las tareas de IA sean difíciles de predecir, lo que obstaculiza la identificación y reparación de desafíos éticos en el diseño y operación de algoritmos. Por lo tanto, no son infalibles, y además tampoco transparentes. En ese sentido, puede ponerse como ejemplo el denominado "*trading* de alta frecuencia"[3], con el que han crecido las incertidumbres, porque el mercado queda en manos de máquinas, y ya tenemos precedentes como el ocurrido en 2010 cuando se produjo una "caída repentina" y el mercado entró en caída libre durante cinco traumáticos minutos y luego se enderezó en otros cinco, sin razón aparente.

Asimismo, aun cuando las decisiones algorítmicas puedan basarse en datos objetivos, no siempre son las mejores. Un estudio realizado en Australia con repartidores, demostró que las *apps* les marcaban un sitio, pero ellos iban por donde había sombra para evitar morirse de sed o tener un golpe de calor. El algoritmo detectaba que iban por un sitio más lento y no tenía en cuenta la temperatura o el cansancio. La necesidad de resguardarse es una explicación que le valdría a cualquier ser humano, pero no a un algoritmo que no hubiera sido programado con esta variable. Ante la necesidad de llevar dinero a su casa, aparece la duda: los trabajadores se arriesgan más de lo que deberían (Montero, 2021).

2) Heredan sesgos de los programadores, usuarios y bases de datos o fuentes de información de las que se nutren. El peligro que puede producirse con la utilización de algoritmos basados en inteligencia artificial es que los datos que utilicen estén sesgados (de manera fortuita), o realicen la elección estableciendo discriminaciones (de manera intencionada). Ello ha ocurrido en el reclutamiento de trabajadores en algunas empresas (cada vez realizadas en mayor medida a través de preselecciones virtuales y automatizadas -*screening*-), condicionando la

3 Se le conoce en Estados Unidos, "HTF" (High Frequency Trading), un tipo de operación en mercados financieros basado en el uso de ordenadores y programas informáticos que compran y venden en milisegundos, todo tipo de activos financieros. Cada una de esas máquinas rastrea permanentemente el mercado, analizando las diferentes plataformas de contratación sean estas bolsas, mercados de renta fija o materias primas- prácticamente a la velocidad de la luz. Su objetivo es encontrar tendencias en la evolución de los precios de los activos, o anormalidades en el mercado. Por ejemplo, una acción de una empresa puede cotizar durante unos segundos un céntimo más cara en Frankfurt que en Londres. En ese caso, el ordenador compra esas acciones en Londres y las vende en Frankfurt. O puede estar lanzando constantemente órdenes de compra y venta, buscando infinitesimales diferencias de precios con las que hacer beneficio. En el fondo, es el clásico "comprar barato y vender caro", pero con márgenes de decimales y en tiempos que no superan los 0,0025 segundos. Los márgenes son minúsculos, pero el volumen de las operaciones, inmenso (Pardo, 2010).

selección de personas de una determinada raza o nacionalidad[4]; a partir de una edad[5]; o género –por ejemplo mujeres en edad de tener hijos[6]. Las mujeres sufren discriminación directa e indirecta en el trabajo, y es posible que antes de que esta balanza se equilibre, nuevas fórmulas puedan asistir al mantenimiento de este tipo de desigualdades basadas en estereotipos que deberían estar superados a inicios del siglo XXI.

El sesgo racial ya se ha visibilizado también en otros ámbitos de la administración pública. El sistema de atención médica de EE. UU. utiliza algoritmos comerciales para guiar las decisiones de salud. Se ha encontrado la evidencia de sesgo racial en un algoritmo ampliamente utilizado, de modo que los pacientes negros asignados al mismo nivel de riesgo por el algoritmo, están más enfermos que los pacientes blancos. Los autores estimaron que este sesgo racial reduce a más de la mitad el número de pacientes negros identificados para recibir atención adicional. El sesgo se produce porque el algoritmo utiliza los costos de salud como un indicador de las necesidades médicas. Se gasta menos dinero en pacientes negros que tienen el mismo nivel de necesidad y, por lo tanto, el algoritmo concluye falsamente que los pacientes negros son más saludables que los pacientes blancos igualmente enfermos. Reformular el algoritmo para que ya no utilice los costos como un sustituto de las necesidades, elimina el sesgo racial al predecir quién necesita atención adicional (Obermeyer, Powers, Vogeli, Mullainathan, 2019).

3) es difícil su verificabilidad 100% debido a su sistema de aprendizaje autónomo y 4) no son completamente transparentes, amparándose las empresas en derechos de propiedad intelectual e industrial para no tener que explicar los detalles de su programación, de ahí que se denominen "*Black boxes*". Si los algoritmos son lo que venden muchas empresas, lo último que ofrecerán es transparencia (O´Neil, 2016). Según algunos analistas, en el futuro los organismos públicos podrían formular leyes con robots (Coglianese y Lehr, 2017) y está claro que están surgiendo nuevas formas de gobernanza que dependen de manera considerable del procesamiento de grandes cantidades de datos digitales de todas las fuentes disponibles, utilizan análisis predictivos para prever el riesgo, automatizan la adopción de decisiones y eliminan a los responsables de estas su poder discrecional. Ello puede comprobarse con supuestos que se están produciendo en Juzgados y Tribunales.

La introducción de la Inteligencia Artificial (IA) en al ámbito judicial, promete aumentar el acceso a la justicia, debido a la reducción del costo de dichos procedimientos, y muchas autoridades públicas ya han identificado beneficios presupuestarios que podrían obtenerse mediante la sustitución de algunos funcionarios judiciales por sistemas automatizados. Tal vez también porque es probable que el uso de algoritmos permita un seguimiento muy detallado y sofisticado de la actividad judicial de cada tribunal, de la ejecución de decisiones, e incluso una exhaustiva evaluación de cada juez (por ejemplo el volumen de trabajo que ha desarrollado en un plazo determinado, o el análisis de supuestos sesgos en sus patrones de comportamiento). Ello sería coherente con el cada vez más observable uso de herramientas de control laboral, cuyo perfeccionamiento está en expansión, aunque muchos también cuestionan su deseabilidad. Existen muchas dudas también en su aplicación en torno al cumplimiento de los principios del Reglamento General de Protección de Datos (RGPD); sobre la garantía y verificabilidad de la neutralidad y objetividad de las herramientas de IA; sobre la facilidad de discernir entre los datos procedentes de su aplicación y otros datos del caso; sobre el acceso a las mismas por parte de todos los operadores jurídicos implicados y la posibilidad de discutir y cuestionar sus resultados; sobre la delegación o no del poder de decisión del Juez; y sobre la afectación a los derechos fundamentales, entre otros.

*La empresa Northpointe*, que creó la aplicación COMPAS, *desarrolló un algoritmo para predecir la probabilidad de que un delincuente reincidiera y este empezó a juzgar que las personas de color eran más proclives a volver a cometer un crimen que los blancos* (Fundación Telefónica, 2017), y los acusados blancos fueron etiquetados erróneamente como de bajo riesgo con más frecuencia que los acusados negros (Angwin, Larson, Mattu, Kirchner, 2016). El caso estadounidense *Loomis*, que terminó en la Corte Suprema del estado de Wisconsin, ilustra este fenómeno, y numerosos Estados lo están ensayando o implementando (Ricoy-Casas, 2021). Este tipo de situaciones agravará el ya intolerable desequilibrio racial en las poblaciones de las prisiones de algunos países como Estados Unidos (Harcourt, 2010). El sesgo racial ya se ha visibilizado también en otros ámbitos como el de salud (Obermeyer, Powers, Vogeli, Mullainathan, 2019).

4 Existe una gran preocupación pública sobre los sistemas de entrevistas por video como HireVue (proveedor de software de reconocimiento de voz de reclutamiento con sede en Utah). Su sistema de IA graba videos de solicitantes de empleo que responden preguntas de entrevistas a través de la cámara web y el micrófono de su computadora portátil, pero este sistema puede funcionar mal, especialmente para personas con acentos regionales y no nativos (Tatman, 2016, 2017) (Harwell, 2018). Asimismo, los sistemas de análisis facial pueden tener dificultades para leer los rostros de las mujeres con piel más oscura (Boulamwini, 2017).

5 Se ha constatado que ciertas palabras específicas de género tienen sesgos adicionales más allá en los buscadores: el de abuela (está más cerca respecto a los cuidados de los niños), el abuelo (está más cerca de la sabiduría que la chica y el chico), y asimismo esta última muestra también una diferencia por edad. Asimismo, a raíz de una denuncia de Pro Publica, Facebook fue demandada por discriminación laboral y residencial en 2016 (Mobley v. Facebook. 5:16-cv-06440, N.D. Cal. 2016). La justificación de la demanda era que Facebook les permitía a los anunciantes decidir por "afinidad étnica" el público de sus anuncios. Al contratar los servicios de Facebook, los anunciantes podían excluir determinados grupos étnicos. El caso fue conciliado en 2019 y Facebook eliminó la posibilidad de decidir la audiencia de los anuncios laborales, residenciales y crediticios utilizando categorías como edad, género, etnicidad o código postal. Este no es un caso de discriminación algorítmica no intencionada, sino de una estructura que permitía la discriminación directa (Ramírez-Bustamante y Páez, 2020).

6 En un estudio, en el que se aplicaron técnicas de aprendizaje automático para entrenar a una inteligencia artificial utilizando Google News, se resolvió la analogía "hombre es a programador de ordenadores", "lo que mujer es a x". La respuesta automática fue que "x = ama de casa" (Bolukbasi, Chang, Zou, Saligrama, Kalai, 2016).

Asimismo, debe resaltarse que los algoritmos heredan sesgos y prejuicios presentes en su elaboración (creadas de manera fortuita o fomentadas por los programadores que los desarrollan), de personas que tienen sus propios sesgos (imaginemos que se trata de un hombre de mediana edad, blanco, de ciertos países, de un determinado perfil económico) o en la adquisición de información de determinadas bases de datos (en su propia implementación o actividad si se alimenta de información errónea). Esto también pone el acento en un aspecto importante: las herramientas automáticas se están desarrollando fuera del sistema judicial. Técnicos, informáticos e ingenieros, deberían como nunca trabajar, en este caso mano a mano, con jueces y abogados (técnicos del sector judicial), algo extrapolable a cualquier otra administración pública.

A estos problemas, se añade el de la incertidumbre sobre su funcionamiento real. Los modelos de aprendizaje automático, al comportarse en cierta medida de manera autónoma, siguen siendo en su mayoría "cajas negras" (*black boxes*). Aunque se elaborase un manual para detallar los datos incorporados, la forma en que se ha programado, podría conocerse con detalle cómo gestiona la información. Ni siquiera los expertos en el campo de la IA pueden ser capaces de prever las „decisiones" tomadas por un sistema de IA, o explicar el proceso por el cual esas decisiones fueron tomadas. Por tanto, se evidencian brechas importantes, no es posible su implementación con garantías y, por ende, su aplicación en este momento haría más vulnerable la defensión de los acusados. De lo contrario, de usarse estos sistemas en la actualidad, se estarían utilizando resultados que van más allá del razonamiento humano, lo cual podría conducir a decisiones de la Corte mal justificadas y motivadas, limitando el derecho a la defensa. Explicabilidad, transparencia, trazabilidad y equidad son algunos de los elementos que deben perfeccionarse para la implementación de la IA.

Las máquinas, los robots, así como otro tipo de tecnología, y la inteligencia artificial, bien utilizados, son y serán un soporte importante para la vida y desarrollo de la humanidad. Sin embargo, teniendo en cuenta estas situaciones críticas, su desarrollo debe ser mucho mayor y más cauteloso para evitar problemas sociales, éticos, morales, jurídicos, políticos, tecnológicos, y no puede dejarse que tomen decisiones importantes sin control humano, especialmente en aquellos casos cuyo resultado pueda crear afecciones a la vida o a elementos clave en el funcionamiento de una sociedad. Cualquier decisión, a la postre, va a tener consecuencias no solo sociales, sino también políticas y jurídicas. Por poner un ejemplo, ¿qué debería decidir un automóvil autónomo que tiene que elegir entre conducir al pasajero contra una pared (pudiendo propiciar la muerte de su conductor), o chocar contra un peatón (con el riesgo de matarlo)?

Podría haberse programado para elegir la solución más prosocial y cooperativa, pero existen dudas acerca de que potenciales compradores de este automóvil estuviesen de acuerdo en esta elección. Algunos autores eligen la posibilidad de que el botón de apagado sea fácilmente accesible, para que los usuarios conserven su derecho a decidir por sí mismos (Perc et al., 2019). Millar (2016) sugiere que el usuario de la tecnología, en este caso el pasajero del auto sin conductor, debería poder decidir qué principios éticos o de comportamiento debería seguir el robot. Este autor incluso sugiere la posibilidad de que las personas puedan elegir su configuración de ética después de comprar un vehículo nuevo. No obstante, elegir cómo reacciona el automóvil con anticipación, ¿podría verse como un daño premeditado? Este es uno de los múltiples debates o dilemas éticos que podemos sustanciar en relación a la utilización de la IA, el *machine learning* y los algoritmos.

## 3. Actividades electorales y tecnología

Las empresas comienzan a predecir lo que quiere el consumidor antes de que lo pida, y por eso realizan investigación online y offline. Si el *big data* supone la recopilación y utilización de grandes cantidades de datos, el *smart data* se focaliza en el uso inteligente de los datos necesarios para un fin. A través de esos y otros medios, nos hemos convertido en el blanco perfecto para una campaña política inescrupulosa. Mediante la utilización de sitios web que publican engaños, millones de perfiles automatizados en redes sociales y una legión de *bots*, que son capaces de convertir una mentira en una tendencia compartida millones de veces. *Los bots en redes sociales llegaron a ser origen del 20% de los mensajes sobre Hillary Clinton y Donald Trump en la campaña electoral estadounidense de 2016* (Gutiérrez-Rubí, 2016). El modelo de negocio de las redes sociales se beneficia particularmente de aquel contenido que genera más interacción entre los usuarios (Zuckerberg, 2018). Los medios tradicionales han perdido el monopolio de la historia de la realidad y el ciudadano, si no tiene un espíritu crítico mínimo, se traga sin cuestionar todo lo que entra por las redes sociales y las manifestaciones culturales.

Y la propagación y diseminación de este tipo de información se ve favorecida, entre otras, por el denominado sesgo de confirmación (tendencia a favorecer, buscar, interpretar, y recordar, la información que confirma las propias creencias o hipótesis). Asimismo, por las denominadas por Eli Pariser (2011, 2017) como *echo cameras,* pues pasamos tiempo con iguales y la información, ideas o creencias en este entorno son amplificadas por transmisión y repetición en un sistema "cerrado", donde visiones diferentes son minoritariamente representadas, e incluso censuradas. También "filtros burbuja", que son el resultado de una búsqueda personalizada en el que el algoritmo de una página web selecciona, a través de predicciones, la información que al usuario le gustaría ver, basándose en información sobre él mismo –según elementos como su localización, su historial de búsquedas, los elementos en los que hizo "clic" en el pasado, los "*likes*" o "me gusta" que haya expresado, etc.

Un buen día te despiertas y te encuentras con que todo el mundo piensa como tú. En palabras de Gordon Allport y Leo Postman, "cada rumor tiene su audiencia" (las personas suelen escuchar lo que esperan ver u oír, en base a la experiencia pasada). Eduard Punset (2008) ha afirmado que incluso cuando el cerebro percibe una explicación distinta a lo que él cree, no solo la cuestiona, corta los circuitos de comunicación para que no penetre. Por eso muchas personas, más allá de las convicciones, se resisten al cambio de voto (es lo que se denomina disonancias). Es decir, nuestro cerebro bloquea la información racional que podría hacernos cambiar de opinión, ya que preferimos las convicciones emocionales o morales a las confirmaciones racionales o epistemológicas. Cabría reflexionar como lo hace Sunstein (2003); solo vemos lo que queremos ver, oímos lo que queremos oír y leemos lo que queremos leer. ¿Es eso bueno para la democracia?

Somos "animales pirateables", como ha expresado Harari (2015, 2019), somos "el producto" al que se le aplica *neuromarketing, microtargeting,* algoritmos, utilizados en toda la información que producimos, por ejemplo a través del móvil (con la ubicación, los lugares que frecuentamos), el ordenador (las páginas que consultamos), el televisor (lo que vemos, de lo cual es posible fácilmente deducir ideología, nivel cultural), lo que consumimos con la tarjeta del súper (se puede inferir gustos, hábitos), la tarjeta de crédito (nivel económico), el smartwatch (el estado de salud) y un largo etcétera. No olvidemos que casi toda nuestra "vida" está concentrada en estos 6 dispositivos, en breve algunos más como la domótica o los electrodomésticos conectados. Emerge una nueva colaboración clave, además de los *spin doctors*, en este escenario político; la de los *data brokers* como Expedian, Equifax, Oracle o Acxiom, sin contar las grandes tecnológicas que controlan *per se,* esta información, tales como Google, Amazon, Facebook, Apple, Microsoft (GAFAM). Su labor de bucear en la red para rastrear, perfilar y enviar publicidad a potenciales votantes con mensajes muy cuidadosamente elaborados lleva más de una década produciéndose. La privacidad ha dejado de ser una decisión individual. Si creemos que, por no manifestar nuestra orientación política o sexual o no participando en redes sociales, preservamos nuestra intimidad, estamos equivocados. Son los denominados *shadow profiles* (perfiles en la sombra o perfiles fantasma). Ello no es por arte de magia, aunque podríamos denominarlo como truco de "presti-digitación", gracias a que los humanos solemos conectarnos con los iguales a uno (homofilia) y, por lo tanto, la predilección de los usuarios en las redes a conectar con quieres comparten alguna característica (asortatividad).

Algunos autores nos hablan también de la "segmentación electoral". Existen datos fiables sobre el modo de vida y hábitos de consumo de demócratas y republicanos que permiten a los equipos de campaña incidir o colocar publicidad en determinados productos o soportes, así como ir a buscar a sus votantes allí donde están. Un ejemplo fue en 2008, cuando los anuncios de Obama aparecían frecuentemente en "Dos hombres y medio", serie que según las encuestas gusta a los demócratas. Gracias a estas encuestas, los equipos de campaña pueden saber, también, que el 46% de los republicanos tiene perro, por solo un 30% de los demócratas; o que los demócratas prefieren ver la MTV o jugar a videojuegos mientras los republicanos ven programas y series como 'Dancing with the stars' (el 'Mira quien baila' americano), '*The Office'* y 'El Mentalista'; o que la mayoría de los republicanos prefiere el fútbol americano o la NASCAR mientras los demócratas prefieren ver la NBA (Peytibi, 2012). Los *spin doctors* utilizan esta información para lanzar su mensaje con precisión de cirujano.

En 2012, Facebook patentó una tecnología para determinar la personalidad de los usuarios a partir de sus datos de perfil, que luego fue utilizada por Cambridge Analytica (Nowak & Eckel) (usa la "escala OCEAN de rasgos de personalidad")[7]. Han trabajado en aproximadamente 200 elecciones alrededor del mundo, incluidas las de Nigeria, Kenia, República Checa, India, Argentina, México, en Estados Unidos a favor de Donald Trump en 2016, a favor del Brexit en 2016, y en Kenia, para lograr la victoria del presidente titular, Uhuru Kenyatta, del partido Jubilee, en las elecciones nacionales celebradas a principios de 2017. Su victoria fue luego anulada por el Tribunal Supremo. Así, con toda nuestra huella digital (la información que proporcionamos en diversos formatos), y el perfilado psicográfico, pueden publicar decenas de anuncios dirigidos a ciertos tipos de personalidad específicos, adaptados a los miedos, necesidades, gustos, emociones, etc. de las personas, para ganar unas elecciones. Obviamente, no podemos analizar en retrospectiva (en elecciones que sabemos que se ha utilizado esta metodología), quién votó, de qué manera, debido a qué anuncios, pues hay múltiples variables. Otro problema es si la identidad virtual o psicografía creada no es correcta (no sabemos qué datos existen de nosotros, el perfilado podría no ajustarse a la realidad). Quizás queda por conocer un montón de detalles del sistema mientras se perfecciona, pero está claro que su uso no irá en retroceso, a pesar de los aparentes esfuerzos, y las nuevas regulaciones como las aprobadas en la UE. *Los escándalos suscitados por Assange y Snowden son la premonición de unas distopías totalitarias en*

7 La "escala OCEAN de rasgos de personalidad" formada por cinco rasgos que forman su acrónimo: factor O (Openness o apertura a nuevas experiencias) ¿estás dispuesto a vivir cambios o aventuras?, factor C (Conscientiousness o responsabilidad) ¿eres perfeccionista?, factor E (Extraversion o extraversión) ¿te encantan las fiestas?, factor A (Agreeableness o amabilidad) ¿eres solidario? y factor N (Neuroticism o inestabilidad emocional) ¿te preocupas o enfadas fácilmente? Frases como "no hablo mucho", "rara vez me siento triste", "soy el alma de la fiesta", "me enfado fácilmente", "siento las emociones de los demás", o posicionamientos sobre las armas, el cambio climático, se usan para calcular una puntuación en cada uno de estos rasgos. Con esos rasgos mencionados, han clasificado a las personas en tipos de personalidad, por ejemplo, la persona aventurera (sería una persona abierta, un poco neurótica y que ama la variedad). Los psicólogos definen la personalidad como una combinación de tus pensamientos, sentimientos y comportamientos. En función de la escala OCEAN, y utilizando el algoritmo, esta información según dichos investigadores es muy precisa, así, tan solo 100 "me gusta" puede deducir qué tipo de persona eres, mejor que las personas de tu trabajo; con "150 me gusta" es más preciso que tus padres, y con "300 me gusta" es mejor para predecir tu personalidad que tu pareja (BBC, 2018).

*las que puede considerarse que las tecnologías digitales pueden convertirse en instrumentos de control y no en herramientas de emancipación.*

La intensidad y velocidad a la que se producen este tipo de acontecimientos ha fomentado una renovada y más intensa preocupación de la UE por la información y la protección de datos, aprobándose un nuevo Reglamento de protección de datos de la UE (RGPD)[8] que se aplica desde el 25 de mayo de 2018, y que ha obligado, igual que el resto de los Estados miembros, a reformar la actual normativa española en la materia, aprobándose la nueva Ley Orgánica de Protección de Datos española (LOPDGDD)[9]. La propia Comisión Europea ha señalado que se *ha convertido en una cuestión clave; no solo para las personas, sino también para el funcionamiento de nuestras democracias, porque constituye una grave amenaza para un proceso electoral limpio y democrático y puede socavar el debate abierto, el juego limpio y la transparencia que son esenciales en una democracia* (COM (2018) 638 final)[10].

El RGPD da margen a los Estados para regular algunos aspectos, y eso es precisamente lo que pretendía el Legislativo con la nueva normativa española. Pese a que en todo el texto había aspectos que no gustaban a especialistas y activistas, tanto ellos como las asociaciones que luchan por la libertad de expresión en la red, centraron sus críticas en cuatro artículos que, por un lado, podrían abrir la puerta a que los políticos tuvieran libertad para espiar todos los perfiles de un ciudadano en la red, y por ende esto pudiera también cambiar la forma en la que utilizamos internet. Estos puntos eran los arts. 85, 93, 94 y 58 bis. Centrándonos tan solo en este último, precisamente titulado: "Utilización de medios tecnológicos y datos personales en las actividades electorales", introducido por una disposición final en la norma, podemos ver las razones de la polémica e inquietud que generó.

Muchos, al leerlo, entendimos que se otorgaba una habilitación a los partidos políticos para recoger datos sobre opiniones políticas de los ciudadanos obtenidos en páginas web y otras fuentes de acceso público para la realización de actividades políticas durante el periodo electoral, y también se concedía "carta blanca" a dichas formaciones para enviar propaganda electoral por medios electrónicos o sistemas de mensajería (por ejemplo WhatsApp, SMS, o e-mail), a partir de esos datos, es decir, "spam electoral" sin que se interprete como información comercial. Si lo que se buscaba, según el Gobierno, era evitar que un caso como el de (CA) ocurriese en España, íbamos en la dirección contraria. Lo que se habilitaría con la redacción del articulado propuesto, era crear bases ideológicas (queremos suponer que sólo a través de la recopilación de información pública), una vez rastreada la red y analizados los datos "abiertos". A su vez, con ello se generarían perfiles de ciudadanos y sus opiniones políticas, y se enviaría propaganda electoral con gran precisión en función del electorado. Para que fuera legal, sólo se necesitaría tener unas "garantías básicas" –no especificadas-. Quiero pensar además que ningún partido, una vez rastreada la web y elaborando una base de datos como la señalada, legalmente, tendría la tentación de crear una lista de opositores eventualmente utilizada para tomar decisiones en el ámbito de la Administración Pública, algo que, por otra parte, es cierto que ya puede hacerlo ahora (obviamente, en ambos casos, de manera ilícita).

Finalmente, el 22 de mayo de 2019, el Tribunal Constitucional (TC) en pleno, y por unanimidad de sus miembros, declaró la inconstitucionalidad del apartado primero de este art. 58 bis de la LOREG (STC 76/2019, de 29 de mayo)[11]. Eso sí, ha sido inusitada la rapidez con la que el TC estimó el recurso de amparo interpuesto por el Defensor del Pueblo el 5 de marzo de 2019 contra dicho artículo. Como bien resume la Sentencia en su fundamento jurídico segundo, la demanda alega que dicha disposición es inconstitucional porque no ha determinado la finalidad del tratamiento más allá de la genérica referencia al que denomina "interés público" (que justificaría la intromisión en el derecho), no establece las limitaciones al tratamiento (las limitaciones a esa habilitación generalmente prohibida), y no establece las garantías adecuadas para proteger los derechos fundamentales afectados (garantías para su ejercicio), precisamente cuando se trata de una categoría especial de datos, los datos de contenido político. Debido a esas insuficiencias, pues tales cuestiones deberían haberse recogido en una norma con rango de ley (además, en aras a una mayor seguridad jurídica), el precepto impugnado habría incurrido en una doble y simultánea vulneración, la de los arts. 18.4 y 53.1 CE, por infringir la reserva de ley y por no respetar el contenido esencial del derecho fundamental a la protección de datos personales (Los derechos fundamentales pueden ser limitados en su ejercicio, siempre que esa restricción se realice mediante una ley orgánica: artículos 53 y 81 de la CE). Por su parte, la Abogacía del Estado se limita a señalar que las garantías y limitaciones a las que se refiere la Ley están o bien en el RGPD o en la LOPDGDD, en la interpretación que de la misma hace la señalada Circular 1/2019 de la AEPD.

Estoy de acuerdo con algún autor en que, *teniendo en cuenta, el conflicto de interés concurrente en la elaboración de la disposición – los partidos políticos son los usuarios potenciales de los datos recabados para llevar a cabo sus actividades de campaña –, no hubiera estado de más reforzar las cautelas y haberse aplicado la conducta*

8 Reglamento 2016/679/UE, de 27 de abril, de protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, y por el que se deroga la Directiva 95/46/CE

9 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), BOE núm. 294, de 6 de diciembre de 2018.

10 Bruselas, 12.9.2018 COM (2018) 638 final: Elecciones libres y limpias. Documento de orientación. Orientaciones de la Comisión relativas a la aplicación de la legislación sobre protección de datos de la Unión en el contexto electoral.

11 STC 76/2019, de 29 de mayo, respuesta al recurso de inconstitucionalidad n. 1405-2019 (BOE n.151, de 25 de junio de 2019).

*tradicionalmente exigida a la mujer del César* (Pascua 2019). En mi opinión, queda claro que el mantenimiento de la dicción inicial aprobada en el artículo 58 bis de la LOREG, consecuencia directa de que no establecía ni el interés público que la inspira, ni las garantías y límites del posible tratamiento, habría supuesto coartar la libertad de expresión (especialmente en páginas web y otras fuentes de acceso público), y seguidamente la libertad ideológica. No debemos olvidar que, precisamente a los partidos políticos (federación de partidos y agrupaciones electorales), desempeñan actividades de una relevancia constitucional básica. Debe reprocharse la actitud reactiva y no proactiva de la AEPD en un caso tan importante como el aquí analizado. Cabría reprochar que también el legislador europeo ha sido muy impreciso a la hora de regular estos contenidos, no concretando tampoco contenidos como el mencionado "interés público", "opiniones políticas", "si el funcionamiento democrático lo exige", "el marco de actividades electorales", etc., aunque, por otro lado, estoy de acuerdo con Rosa García en que, por ejemplo, *determinar qué son "opiniones políticas" puede tener una muy difícil concreción en el mundo virtual de Internet* (García, 2019).

La "apropiación" de los datos (incluso los más sensibles) de los ciudadanos ha ido *in crescendo*, también en la UE. Resulta preocupante lo fácil que resulta ahora el acopio y tratamiento a gran escala de datos con un solo *click,* que pueden revelar datos sensibles como la tendencia política sin consentimiento de los ciudadanos, pudiéndose realizar incluso perfilados ideológicos erróneos, y el intrusivo y masivo *spam* por medios tecnológicos que se produce en ocasiones, en el contexto electoral. Diversos autores han advertido ya la obsolescencia de la normativa electoral y sus perniciosas consecuencias (Holgado, 2017). Obviamente es al legislador a quien debe dirigirse de manera principal este reproche. Y todo ello con la finalidad de modificar, forzar o desviar la voluntad de los electores sin que estos sean conscientes de ello. Los poderes públicos deben promover las condiciones para que la libertad e igualdad sean reales y efectivas, y se protejan los derechos fundamentales, pero precisamente son juez y parte interesada, con exiguas discusiones sobre el tema en los resortes de los parlamentos nacionales.

Por ahora, algunas de estas intentonas como la señalada en el caso español, parece fallida, pero es necesario tener en cuenta los grupos selectos de partes interesadas, influyentes e inescrupulosas, que logran volar bajo el radar. La democracia está siendo *hackeada*, incluso con la coartada de importantes centros de investigación y Universidades situadas en la Meca (*Silicon Valley*) de las tecnológicas. La libertad difícilmente puede darse en un entorno tecnológico en el que las modernas técnicas de análisis de la conducta sobre la base del tratamiento masivo de datos y la inteligencia artificial permiten procedimientos complejos orientados a modificar, forzar o desviar la voluntad de los electores y sin que estos sean conscientes de ello. El problema es que polarizar una sociedad con *fake news*, inteligencia artificial y algoritmos puede ayudar a ganar una elección, pero luego también puede hacer que el país sea ingobernable (Comisión Europea, 2018) (Hern, 2017).

## 4. Social Score: control social de la ciudadanía con fines políticos

Como hemos visto, los rápidos avances tecnológicos (no exentos de errores), junto con el gran volumen de datos que pueden recopilarse (*big data*) y su análisis (*smart data*), ejecutando algoritmos incluso en los dispositivos más pequeños, está creando importantes desafíos sociales y legales*.* Existen ya múltiples temores en relación a su utilización: en relación a la accesibilidad e integridad de los datos personales; la intromisión en la intimidad de las personas; fallos técnicos y de seguridad que pueden producir graves daños y/o perjuicios (a las personas, a las infraestructuras críticas); su inclusión podría ocasionar la destrucción de trabajo (eliminación de ciertos sectores o menor empleabilidad por la introducción de máquinas); toma de decisiones discriminatorias sin cumplir criterios éticos, por ejemplo en la selección de empleados y en ciertas contrataciones por empresas y administraciones (sesos algorítmicos); e incluso la modificación de la propia cultura y los valores actuales. Es por ello, que la identificación, reflexión y regulación de casos como los señalados, resultan decisivos. Debe evidenciarse que el uso de sistemas de IA para adoptar decisiones, implica claramente no solo aspectos económicos, sino también sociales y éticos (por la forma en que los sistemas están diseñados y programados, su propio funcionamiento, o las fuentes de información de las que se nutren), de ahí la importancia de los aportes de otras disciplinas más allá de las meramente tecnológicas, como la ciencia política y el derecho.

A pesar de los esfuerzos en materia de protección de datos, la "apropiación" de los datos de los ciudadanos ha ido *in crescendo* a nivel internacional y en la propia UE. Múltiples ejemplos refuerzan esta idea: juguetes[12], televisores[13]y aspiradoras que espían[14] y otros dispositivos caseros. La mayoría de las empresas no cuidan la

12 Muñecas como "Mi amiga Cayla" como los robots "iQue", permitían establecer conexiones Bluetooth no autorizadas desde cualquier teléfono o tableta en una distancia de unos 15 metros. Estos robots incluso accedían a la cámara de los dispositivos que utilizaba. El escándalo estalló cuando la Agencia Federal de Redes prohibió la venta de la muñeca por el riesgo de que el juguete registre y transfiera las conversaciones entre el niño y otra persona, sin el conocimiento de los padres, e incluso que los menores sean espiados directamente por una empresa. La asociación europea en defensa de los consumidores BEUC ya había alertado de los peligros de estos juguetes conectados en diciembre, y celebró la decisión de las autoridades alemanas.

13 En febrero de 2017, la Comisión Federal de Comercio (EE.UU.) multó al mayor fabricante de televisores de Estados Unidos por espiar a 11 millones de hogares. La agencia se ocupa de los derechos de los consumidores y vigila aquellas prácticas que atentan contra la libre competencia. Vizio (EE.UU.) estaba usando el sistema SmartCast de sus televisores para recoger información geográfica, demográfica y datos „extremadamente específicos, segundo a segundo, de los hábitos televisivos" de sus desprevenidos usuarios para vendérsela a anunciantes y empresas de publicidad.

14 iRobot, el fabricante de la popular aspiradora inteligente Roomba, quiere vender los datos con los planos y la distribución de los hogares que proporciona la máquina a terceros. La empresa, nacida en el MIT en 1990 y cuya finalidad inicial era crear robots que desactivan bombas, ha reconocido

seguridad informática de sus equipos de impresión y multifuncionales, pero este tipo de *hardware* ya incluyen muchos de los componentes de una computadora (disco duro, memoria) y están conectados a las redes corporativas o domésticas, fijas o *wifi*. Y usualmente las compañías y los usuarios utilizan una clave débil o no usan ninguna en estos equipos. Además, la ciudadanía se conecta a móviles, memorias USB y otros dispositivos que no son seguros. También aparatos médicos como marcapasos (en ocasiones se avisa a los pacientes que actualicen sus marcapasos para evitar *hackeos* que podrían tomar el control de dichos dispositivos) o de uso personal como los *smartwatch.*

Muchos empleadores han querido introducir este tipo de dispositivos en el ámbito laboral, justificando que podrían verificar sus constantes vitales para prevenir riesgos, o facilitar el acceso a determinados espacios y ordenadores, como modo extra de seguridad a través de "microchips" NFC (tecnología de comunicación de campo cercano) o RFID (identificación por radiofrecuencia). También se utilizan frente a secuestros, y podrían utilizarse en sustitución de los pasaportes, las tarjetas bancarias y abonos de transporte o incluir información médica que para conocer el tipo sanguíneo de un herido inconsciente al que hay que atender urgentemente, o si es alérgico a algún medicamento. Se puede incluso imaginar un futuro con implantes más avanzados que midan parámetros médicos en tiempo real, como el azúcar en la sangre de un diabético o la presión arterial en alguien con problemas cardiovasculares: El laboratorio de sistemas integrados de la Escuela Politécnica de Lausana (Suiza) ha desarrollado chips con biosensores que miden la temperatura, el pH o la densidad de moléculas como la glucosa o el colesterol y envía los datos al móvil u ordenador vía Bluetooth.

Estos aspectos controvertidos han obligado a la UE a aprobar normativa protectora específica, y ha creado intensos debates sobre si ¿es lícito permitir la realización de análisis o recabar información sensible en el ámbito laboral? El conocimiento de esta información por parte de los empleadores, ¿podrá condicionar la concesión de un empleo a un individuo -por ejemplo, por la mera probabilidad estadística de ser genéticamente vulnerable a una cierta enfermedad laboral-? ¿y para contratar un seguro? Se comienza a extender la exigencia de facilitar información sensible como los datos biométricos para pasaportes e incluso información del ADN para entrar en un país. La Ley 78/2015 de Kuwait, ha sido la primera en el mundo que recoge la obligación de que todos los ciudadanos, residentes y visitantes del país proporcionen muestras de ADN a las autoridades para que sean incluidos en la base de datos policial con el fin de controlar y colaborar con el Ministerio de Interior. Miles de cámaras con reconocimiento facial invaden nuestras calles, en algunos países como China de una manera más que intensiva, empresas como Facebook han sido llevadas a los Tribunales y ante Instituciones como el Congreso de los EE.UU. y la UE por recoger y almacenar de manera ilegal datos biométricos de fotos de manera secreta y sin consentimiento inicialmente para una función de la red social que permite a sus usuarios etiquetar a sus amigos en una foto con nombres, y otras tantas empresas han sido sancionadas por aplicaciones como *Google Street View*. La AEPD sancionó al gigante de Internet porque no solo captaban imágenes de la calle (callejeros, vías, carreteras, etc.), sino que también captaban y guardaban sin consentimiento datos de la localización de redes wifi y datos de tráfico asociados a esas redes, un hecho que la compañía reconoció y alegó que captó „por error".

Podemos observar que el hecho de que exista una normativa y numerosos esfuerzos institucionales, no evita la vulneración constante de la protección de datos, es una realidad en todo el mundo, algo de extrema relevancia y que resulta preocupante para nuestras actuales democracias y el propio Estado de Derecho. De manera concurrente, hay varios hechos que promocionan y/o permiten la vulneración de la protección de datos: 1.-Casi toda nuestra información está en unos cuantos dispositivos que utilizamos a diario e incluso de los que no nos separamos en todo el día tales como el móvil, el *smartwacht* o el ordenador; 2.-Cada vez compramos más a través de internet, tenemos más aparatos "inteligentes" conectados a la *wifi* (televisión, impresora, refrigerador, basura, lavadora...) y con ello perfiles sobre nuestros gustos, basados en los que compramos y vemos; 3.-Este perfilado y la cesión de gran parte de nuestra información se completa con los permisos que autorizamos al suscribirnos y utilizar la mayoría de aplicaciones móviles (apps) y redes sociales, a través de las cuales también pueden perfilarnos económicamente, ideológica y políticamente, sobre nuestra religión, identidad sexual y entorno social; 4.-De manera gradual nos estamos aproximando a la administración pública 100% online, en la que toda nuestra información de interacción con organismos e instituciones (pago de tributos, tasas, impuestos, multas, recursos, alegaciones, solicitudes, permisos, etc.) se archivarán en pocas carpetas digitales accesibles en un "clic", de gran interés para *hackers* (esta accesibilidad en la casi total virtualización del control de muchos de los sistemas será especialmente problemático en relación a las infraestructuras críticas); 5.-Nuestros datos biométricos también están siendo recabados a través de las redes sociales y aplicaciones móviles, por miles de cámaras (por cuerpos y fuerzas de seguridad del Estado, consorcios de seguridad entre países, por corporaciones empresariales), a través de los pasaportes que disponen de esta información, para hacer *checking* con algunas compañías en la puerta de embarque, y en ciertos países para algo tan sencillo como pedir un menú en un restaurante o coger papel de baño en las instalaciones de un lugar de gran afluencia turística; 6.-Toda esta información, este gran *big data,* puede almacenarse automáticamente en algunos *bunkers* de información y el cual puede ser analizado a través de

que quiere compartir la información de las casas de sus clientes con otros fabricantes como Google o Apple. Dos de sus modelos se conectan con Alexa, el asistente de voz de Amazon. De modo que se pueden ejecutar órdenes del tipo: "Alexa, pasa la aspiradora en el salón". Una posible utilidad de estos mapas podría ser preguntar a los asistentes de voz, ya sea Siri, Alexa o Google, dónde hemos dejado alguno de nuestros dispositivos electrónicos.

inteligencia artificial y algoritmos para extraer la información considerada relevante para cada caso. ¿Cómo y por quiénes podrá utilizarse toda esta información? ¿Con qué fines?

Los bancos nos puntúan como clientes, lo hacen en base a nuestra información financiera (nuestros ingresos, patrimonio, inversiones, gastos, en qué gastamos, deudas, etc.). En base a esta puntuación, las entidades financieras nos conceden o no una tarjeta de crédito, un préstamo, una hipoteca, y otras condiciones contractuales. Por ahora esa información es privada en la UE (salvo la de algunos cargos políticos sujetos al deber de hacer públicas declaraciones comprensivas de la situación patrimonial en la toma de posesión o cese). Imaginemos que esa puntuación fuera pública, que todo el mundo (tus amigos, vecinos, expareja, compañeros de trabajo, etc.) pudiera comprobar tu situación financiera, y que esa puntuación no solamente fuera económica, sino que incluyera otros múltiples aspectos de tu vida como lo que compras en las tiendas de alimentación, de ropa, a qué clubs sociales o asociaciones perteneces, dónde vives, qué coche tienes, dónde pasas las vacaciones, cuáles son tus hábitos de ocio, las multas de tráfico que has tenido, los impuestos que pagas, y así con un largo etcétera.

Un sistema similar a este, en el que se puntúa por todos tus aspectos (financieros, laborales, de consumo, de ocio, etc.), es muy parecido al que se está ensayando en China. Como explica Amanda Lee (2020), el sistema de crédito social de China es un conjunto de bases de datos e iniciativas que monitorean y evalúan la confiabilidad de individuos, empresas y entidades gubernamentales. A cada entrada se le asigna un puntaje de crédito social, con recompensas para quienes tienen una calificación alta y castigos para quienes tienen puntajes bajos. Las bases de datos son administradas por el planificador económico de China, la Comisión Nacional de Desarrollo y Reforma (NDRC), el Banco Popular de China (PBOC) y el sistema judicial del país.

El subdirector de la Oficina de Gestión de Crédito Social de Rongcheng, He Junning, ha explicado para Foreign Policy, que el sistema asigna 1.000 puntos al principio a cada uno (en la actualidad 950) de los 740.000 residentes adultos de Rongcheng. *La puntuación varía de 350 a 950, con cinco categorías: súper (700-950), excelente (650-700), bueno (600-650), bueno (550-600) y no tan bueno (350-550). La puntuación se deriva de cinco dimensiones: historial crediticio, capacidad de realización, características personales, comportamiento y preferencias, y relaciones interpersonales* (Fei, 2019). Esta autora señala que el historial de crédito, la capacidad de cumplimiento y los datos de comportamiento y preferencias, provienen de los datos de transacciones de uno en las aplicaciones de *Alipay*. Los datos de características personales son opcionales y completados por los propios usuarios. Incluyen nivel de educación, licencia de conducir e información de registro de vehículos, etc. La última categoría, las relaciones interpersonales, suena algo aterradora y extraña. Implica que, si tienes amigos con buen puntaje de crédito, entonces también serás un buen individuo. Por el contrario, si tu red social está llena de amigos de baja confianza, entonces tu puntaje será menor.

A partir de los puntos iniciales, comienzas a perder o a ganarlos: Si te han puesto una multa de tráfico; pierdes cinco puntos. También pierdes puntos si no detienes el coche en el paso de peatones. *Se puede evitar que las personas en la lista compren boletos de avión, tren bala o boletos de tren de primera clase o clase ejecutiva; vender, comprar o construir una casa; o matricular a sus hijos en costosas escuelas de pago. Hay restricciones para que los infractores se afilien o sean promovidos en el partido y el ejército, y para recibir honores y títulos. Si el moroso es una empresa, ésta no podrá emitir acciones o bonos, aceptar inversiones extranjeras ni trabajar en proyectos gubernamentales* (*The Economist*, 2016). Sin embargo, si has ganado un premio a nivel de ciudad (por ejemplo, por cometer un acto heroico, hacer negocios ejemplares o ayudar a tu familia en circunstancias difíciles inusuales), tu puntaje se incremente en 30 puntos. También puedes ganar puntos donando a organizaciones benéficas, o como voluntario en el programa de la ciudad.

Este sistema también ha incluido a las empresas: si están al día de sus impuestos y otras obligaciones, y evitan multas por cuestiones como producir y/o vender productos de baja calidad o insalubres, obteniendo alta puntuación, pasarán por menos obstáculos en las licitaciones públicas y obtendrán mejores condiciones de préstamo. *A unas 6000 empresas se les restringió el acceso a la financiación en función de las puntuaciones de crédito social, que también cubren las infracciones ambientales y el dumping* (Needham, 2018). *Las empresas que han sido incluidas en la lista negra podrían enfrentar tasas de inspección más altas y auditorías específicas, restricciones en las aprobaciones gubernamentales de derechos de uso de la tierra y permisos de inversión. También pueden quedar excluidos de políticas preferenciales, como subsidios y rebajas de impuestos, así como enfrentar restricciones en la contratación pública* (Lee, 2020). Debe tenerse en cuenta que son frecuentes las estafas y los escándalos de seguridad alimentaria en el país (Bhandari, 2018), e incluso ha habido críticas de la población sobre la mala calidad de las viviendas, vacunas vencidas, etc. (*The Economist*, 2016).

Según el documento fundacional del sistema, publicado por el Consejo de Estado en 2014, el esquema debería „permitir que los confiables deambulen por todas partes bajo el cielo, mientras dificulta que los desacreditados den un solo paso“. Así, en algunas ciudades como la de Rongcheng, justificado en “un intento de promover la confiabilidad en su economía y sociedad”, se experimenta con un sistema de crédito social, que incluye desde *clasificaciones calculadas por proveedores de pagos en línea hasta puntajes repartidos por vecindarios o empresas. Los viajeros de alto vuelo reciben beneficios como descuentos en las facturas de calefacción y préstamos bancarios favorables, mientras que los deudores malos no pueden comprar boletos de tren o avión de alta velocidad* (Mistreanu,

2018). Las „familias civilizadas“ de Roncheng (las mejor puntuadas en este sistema) se muestran en tablones de anuncios públicos, tal vez para que sirva como escaparate de los comportamientos que deben realizar los demás. *La administración del ciberespacio mantiene una „lista blanca“ de empresas de medios favoritas que pueden vender sus artículos a otros medios* (*The Economist*, 2016).

No obstante, también se avergüenza públicamente a los "*Lao Lai*" (holgazanes que no pagan sus facturas) a través de un sitio web de *Credit China* que había sido visitado por 500 millones de personas, y algunas provincias también han comenzado a transmitir fotografías de las personas incluidas en la lista negra en pantallas gigantes en lugares públicos (Needham, 2018). Estoy de acuerdo con Campbell (2019) en que algunos elementos son realmente dignos de una ficción distópica. Explica que, en ciertas áreas de China, llamó por teléfono a una persona incluida en la lista negra y escuchó una sirena y un mensaje grabado que dice: "Advertencia, esta persona está en la lista negra. Ten cuidado e instálalos a pagar sus deudas". Otra cuestión controvertida es una especie de "lista negra" que hace pública la Corte Suprema de China, de la que forman parte 170,000 incumplidores, a quienes se les prohíbe comprar boletos de tren de alta velocidad, o de avión, o alojarse en hoteles de lujo, como un medio para presionarlos a pagar su deuda. Aunque inicialmente se aplicaba de manera voluntaria, ahora ya se requiere para múltiples actividades sociales y laborales, cuya pretensión es que se convierta en obligatorio. Algunas personas podrían quedar atrapadas en la red de crédito social de China. Es "un juego" en el que tener una buena puntuación te otorga recompensas (menos burocracia o descuentos en billetes de tren y avión, etc.), pero también donde una baja puntuación puede convertir a una persona en un "marginado social". Es por eso que podría utilizarse el "crédito social", para expandir el poder de los fuertes y comprimir aún más el espacio para los derechos civiles.

Hoy en día la mayoría de los Estados y las empresas tecnológicas empiezan a tener a su disposición la mayor parte de nuestra información, y por eso este sistema es un vistazo a un futuro distópico; un lugar donde todos los ciudadanos son observados y calificados por el gobierno, que distribuye recompensas o castigos en consecuencia; un panóptico de vigilancia digital de 360 grados, incluso en el ámbito de datos tan sensibles como los de salud (Chen y Grossklags, 2020) (Horwitz y Goh, 2020) (Mozur, Zhong y Krolik, 2020), con el poder de las grandes tecnológicas dominando el ecosistema. Este sistema donde un gobierno intenta controlar cada parte de la vida de las personas, no difiere demasiado a lo descrito por George Orwell en su novela1984.

A medida que el Estado continúa persiguiendo a las minorías religiosas como los uigures y silenciando a los académicos francos, la preocupación es a qué métricas se extenderán los sistemas de crédito social a continuación. Este sistema podría dividir aún más a la sociedad, creando clases de personas dependiendo de su crédito social, provocando desigualdad social y pérdida del pensamiento crítico. China no es el único régimen autoritario del mundo, pero es uno de los más ricos, fuertes y avanzados tecnológicamente. También uno de los oponentes más peligrosos de las sociedades abiertas definido por la UE como operador sistémico. Un sistema así, le daría el control total sobre los ciudadanos. Resulta por ello muy sugerente el libro de la profesora de la Universidad de Harvard, Shoshana Zuboff titulado La era del capitalismo de vigilancia. La lucha por un futuro humano en las nuevas fronteras del poder (Zuboff, 2018).

## 5. Conclusiones

Como ha señalado el Consejo de Derechos Humanos de las Naciones Unidas (Human Rights Council, 2019), en numerosos países, los sistemas de asistencia y protección social se basan cada vez más en datos y tecnologías digitales que se utilizan para automatizar, predecir, identificar, vigilar, detectar, singularizar y castigar. Este proceso se conoce generalmente como transformación digital, pero no debería permitirse que este término, un tanto neutral, oculte el carácter revolucionario y la motivación política de muchas de esas innovaciones. Es necesario un profundo debate para evaluar críticamente qué papel, si lo hay, deben desempeñar las herramientas de inteligencia artificial (IA) en nuestros sistemas de justicia.

La IA debe reforzar, y no disminuir, las garantías del estado de derecho y la calidad de la justicia a la que tienen acceso todos los ciudadanos. Es también necesario reclamar nuevos derechos superadores de los actuales como la igualdad de oportunidades de acceso a la tecnología (por razones de edad, económicas, de género, etc.); la protección de la integridad personal y a la vida frente a la tecnología; una mejora en la protección de datos y el derecho al olvido en internet; la regulación de la libertad de expresión en entornos virtuales; la explicación, transparencia, trazabilidad, verificabilidad y equidad de los algoritmos y la inteligencia artificial; la igualdad de oportunidades en la economía y el empleo digital; las garantías de los consumidores en el e-commerce; la seguridad de la red (especialmente en lo relacionado con las infraestructuras críticas), etc.

Las administraciones públicas y los gobiernos ampliarán sus dependencias tecnológicas (estadounidense y asiática -principalmente China y Corea del Sur-) aceptando las condiciones impuestas por las grandes tecnológicas en una suerte de lo que he dado en denominar "Gafamcracia", aludiendo al poder de las conocidas como las *big five tech companies*, en este conjunto de empresas tecnológicas encontramos a Google, Apple, Facebook, Amazon y Microsoft (GAFAM), o las BHAT, cuyo acrónimo incluye a grandes compañías asiáticas que han empezado a incursionar de otras formas en la economía mundial (Baidu, Huawei Alibaba, Tencent, Xiaomi). Estas grandes compañías concentran las inversiones en innovación y tecnología más avanzada (poder tecnológico), sus

presupuestos son superiores a algunos países (capacidad de influencia y presión); gastando decenas de millones de dólares en acciones de lobby (en el caso Estadounidense con ventajas financieras y jurídicas -a cambio de soporte e información-; en el caso chino han incrementado la integración de las grandes empresas digitales en la estrategia estatal –al servicio de las ambiciones internacionales del Partido Popular Chino y de la política de control social del régimen-).

No solo el Estado, sino estas Empresas, han conseguido información relevante de millones de ciudadanos de todo el mundo y con ello tienen una gran capacidad para vendernos "lo que todavía no sabemos que nos gustaría y necesitamos", de influir en nuestra propia opinión, y de interferir en las elecciones de un país. También modulan el alcance de la libertad de expresión (incluso a instancia de las autoridades), y en ciertos casos a razón de tecnologías que ellos mismos introducen *exnovo* en el mercado, y presionan para que sean sus estándares éticos (sus propuestas de directrices y normativas) las que se impongan en los mercados desde una visión principalmente mercantilista. Los esfuerzos de la UE por subvertir estos grandes poderes, no resultan inocuos, pero sí con una limitada capacidad.

## 6. Agradecimientos

El presente texto nace en el marco del proyecto PID2019-105841RB-C22, financiado por el MINECO, y del programa de ayudas estructurales para grupos de excelencia de la Xunta de Galicia (GPC-AGAF) (España).

## Referencias


Allport, G.W.; Postman, L. (1947). *The Psychology of Rumor*. New York: Henry Holt.

Angwin, J., Larson, J., Mattu, S., Kirchner, L. (2016, March 23). *Machine Bias. There's software used across the country to predict future criminals. And it's biased against blacks, ProPublica*. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Bhandari, B. (2018, January 2). China's Year in Scams. Despite tougher laws, Chinese citizens continue to get swindled in a surprising variety of ways, *Sixthtone.* https://www.sixthtone.com/news/1001431/chinas-year-in-scams

BBC (2018, April 9). *Cómo Cambridge Analytica analizó la personalidad de millones de usuarios de Facebook.* https://www.youtube.com/watch?v=7831NGClsrM

Bolukbasi, T., Chang, K-W., Zou, J., Saligrama, V., Kalai, A. (2016). Man is to Computer Programmer as Woman is to Homemaker? Debiasing Word Embeddings, *The Conference on Advances in Neural Information Processing Systems 29 (NIPS 2016)*, pp. 4349–435. https://arxiv.org/pdf/1607.06520v1.pdf

Buolamwini, J. (2017). How I'm fighting bias in algorithms, *TED.* https://www.ted.com/talks/joy_buolamwini_how_i_m_fighting_bias_in_algorithms/transcript

Campbell, C. (2019). How China Is Using "Social Credit Scores" to Reward and Punish Its Citizens, *Time.* https://time.com/collection/davos-2019/5502592/china-social-credit-score/

Chen, M. y Grossklags, J. (2020). An Analysis of the Current State of the Consumer Credit Reporting System in China, *Proceedings on Privacy Enhancing Technologies*, 2020 (4), DOI:10.2478/popets-2020-0064

Coglianese, C. y Lehr, D. (2017). Regulating by robot: administrative decision making in the machine-learning era, en *Georgetown Law Journal*, *105* (5), 1147.

Comisión Europea (2018). A multi-dimensional approach to disinformation, *Report of the independent High level Group on fake news and online disinformation.* Luxembourg: Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1

El Mundo (2016, March 28) *Una inteligencia artificial se vuelve racista, antisemita y homófoba en menos de un día en Twitter*. *https://www.elmundo.es/tecnologia/2016/03/28/56f95c2146163fdd268b45d2.html;*

El Mundo (2018, January 16)*. Google soluciona a las bravas su algoritmo ‚racista', que confundía a personas negras con gorilas*. *https://www.elmundo.es/f5/comparte/2018/01/16/5a5dff50468aeb81638b45e7.html*

*El País* (2016, March 25). *Microsoft retira un robot que hizo comentarios racistas en twitter*. *https://elpais.com/tecnologia/2016/03/24/actualidad/1458855274_096966.html*

*El País* (2018, January 14). *Google arregla su algoritmo "racista" borrando a los gorilas*. *https://elpais.com/tecnologia/2018/01/14/actualidad/1515955554_803955.html?id_externo_rsoc=TW_CM*

*El País* (2018b, March 22). *Así fue el atropello moral del Uber sin conductor*. https://elpais.com/elpais/2018/03/22/videos/1521681970_604181.html

Fei, C. (2019). Social Credit System in China, *Panorama. Insights into Asian and European Affairs,* 2/2018. KAS190325 Digital Asia New Sub Project_FA

Fundación Telefónica (2017). *Inteligencia artificial. Las máquinas que aprenden solas.* http://fundaciontelefonica.com/

García, R. M. (2019). Tratamiento de datos personales de las opiniones políticas en el marco electoral: todo en interés público, *Revista de Estudios Políticos*, 183. https://doi.org/10.18042/cepc/rep.183.05

Gutiérrez-Rubí, A. (2016). *Bots para la comunicación Política*. https://www.gutierrez-rubi.es/2016/11/02/bots-en-comunicacion-politica

Harari, Y.N. (2015). *Sapiens. De animales a dioses: Breve historia de la humanidad.* Debate.

Harari, Y.N. (2019, March 6) Los cerebros "hackeados" votan, *Suplemento Ideas de El País.* https://elpais.com/internacional/2019/01/04/actualidad/1546602935_606381.html

Harcourt, B.E., (2010). Risk as a Proxy for Race, en *Criminology and Public Policy, Forthcoming, University of Chicago Law & Economics Oline Working Paper n.535, University of Chicago Public Law Working Paper n.323*. https://ssrn.com/abstract=1677654

Harwell, D. (2018, July 19). The Accent Gap, *The Washington Post*. https://www.washingtonpost.com/graphics/2018/business/alexa-does-not-understand-your-accent

Hay, B. (2016, January 25). Cinq objets connectés pour économiser l'énergie, *La Tribune*. https://www.latribune.fr/entreprises-finance/la-tribune-de-l-energie-avec-erdf/cinq-objets-connectes-pour-economiser-l-energie-545571.html

Hern, A. (2017, November 14). Thirty countries use 'armies of opinion shapers' to manipulate democracy, *The Guardian.* https://www.theguardian.com/technology/2017/nov/14/social-media-influence-election-countries-armies-of-opinion-shapers-manipulate-democracy-fake-news

Holgado González, M. (2017). Publicidad e información sobre elecciones en los medios de comunicación durante la campaña electoral. *Teoría y Realidad Constitucional*, 40, 457-485. DOI: https://doi.org/10.5944/trc.40.2017.20914

Horwitz, J. y Goh, B. (2020, May 26). As Chinese authorities expand use of health tracking apps, privacy concerns grow, *Reuters.* https://www.reuters.com/article/us-health-coronavirus-china-tech-idUSKBN23212V

Human Rights Council of the United Nations. (2019, October 11). *Digital technology, social protection and human rights*, Report, A/74/493. https://undocs.org/A/74/493

Lee, A. (2020, August 9). What is China's social credit system and why is it controversial?, *South China Morning Post.* https://www.scmp.com/economy/china-economy/article/3096090/what-chinas-social-credit-system-and-why-it-controversial

Millar, J. (2016). An Ethics Evaluation Tool for Automating Ethical Decision-Making*, Robots and Self-Driving Cars*, *30*(8), 787-809. https://doi.org/10.1080/08839514.2016.1229919

*Mirror* (2016). *Intelligent robot that remenbers and learns could be scrapped after escaping a lab for a second time.* https://www.mirror.co.uk/news/weird-news/intelligent-robot-remembers-learns-could-8248559

Mistreanu, S. (2018, April 3). Life Inside China's Social Credit Laboratory, Foreign Policy. https://foreignpolicy.com/2018/04/03/life-inside-chinas-social-credit-laboratory/

Montero, S. (2021, March 27). Los algoritmos y sus sesgos de género, raza o clase: así te perjudican en la búsqueda de trabajo o de ayudas sociales, *Público.* https://www.publico.es/ciencias/algoritmos-y-sesgos-genero-raza.html

Mozur, P., Zhong, R. y Krolik, A. (2020, March 1). In Coronavirus Fight, China Gives Citizens a Color Code, With Red Flags, *The New York Times.* https://www.nytimes.com/2020/03/01/business/china-coronavirus-surveillance.html

Needham, K. (2018, March 6). If you get on China's 'blacklist,' you can be banned from travel, *The Sydney Morning Herald.* https://www.smh.com.au/world/asia/big-brother-stops-millions-boarding-planes-trains-in-china-20180306-p4z33u.html

Nowak & Eckel (2012). US Patent no. US20160283485A1. Washington, DC: U.S. Patent and Trademark Office.

Obermeyer, Z.; Powers, B.; Vogeli, C.; Mullainathan, S., (2019, October 25). Dissecting racial bias in an algorithm used to manage the health of populations, *Science* 366, Issue 6464. DOI: 10.1126/science.aax2342. https://science.sciencemag.org/content/366/6464/447

O´Neil, C. (2016). *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*. Crown, Penguin Random House: New York.

Pariser, E. (2011). Cuidado con las burbujas de filtro. *TED.* https://www.ted.com/talks/eli_pariser_beware_online_filter_bubbles?language=es

Pariser, E. (2017). *El filtro burbuja.* Taurus.

Pardo, P. (2010, December 29). Las máquinas que controlan la economía, *El Mundo*. https://www.elmundo.es/elmundo/2010/12/29/internacional/1293605644.html

Pascua,, F.A. (2019). Un nuevo capítulo en la tutela del derecho a la protección de datos personales: los datos de contenido político. comentario a la sentencia del tribunal constitucional 76/2019, de 29 de mayo, en el recurso de inconstitucionalidad núm. 1405-2019, *Revista de las Cortes Generales,* 106. https://doi.org/10.33426/rcg/2019/106/1411

Peytibi, X. (2012). La segmentación electoral, *Más poder local*, 13. http://www.maspoderlocal.es/files/articulos/110-F508305df1101350763999-articulo-1.pdf

Perc, M.; Ozer, M.; y Hojnik, J. (2019). Social and juristic challenges of artificialintelligence, *Palgrave Commun*, *5*(61): https://doi.org/10.1057/s41599-019-0278-x

Proyecto Carabela (2019). http://carabela.prhlt.upv.es/es

*Público* (2017). ¿Qué fue de Tay, el robot de Microsoft que se volvió nazi y machista?. https://acortar.link/EVRCYq

Punset, E. (2008). *Por qué somos como somos*. Aguilar.

Ramírez-Bustamante, N.; Páez, A. (2021). Análisis jurídico de la discriminación algorítmica en los procesos de selecciónlaboral, *SSRN*. http://dx.doi.org/10.2139/ssrn.3765741

Ricoy-Casas, R.M. (2019). Inteligencia artificial y políticas públicas en la UE, Valcárcel, P.; Fernández, R.; Bonorino. P.R. (Dirs.), *Derecho, desarrollo y nuevas tecnologías,* Aranzadi Thomson Reuters, ISBN 9788413087184, 187-234.

Sunstein, C. (2003). *República.com: Internet, democracia y libertad (Estado y Sociedad).* Estado y Sociedad. Ediciones Paidós.

Tatman, R. (2016, July 12). Google's speech recognition has a gender bias. https://makingnoiseandhearingthings.com/2016/07/12/googles-speech-recognition-has-a-gender-bias/

Tatman, R. (2017, April 4). Gender and Dialect Bias in YouTube's Automatic Captions, *Proceedings of the First Workshop on Ethics in Natural Language Processing.* http://www.aclweb.org/anthology/W17-1606

*The Economist* (2016, December 17). *China invents the digital totalitarian state. The worrying implications of its social-credit project.* https://www.economist.com/briefing/2016/12/17/china-invents-the-digital-totalitarian-state

*The Guardian* (2016, March 24). *Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter.* https://

www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter

*The Guardian* (2018, May 29). *Computer learns to detect skin cancer more accurately than doctors.*

*The Washington Post* (2016, June 30). *The brave escape and untimely demise of one Russian robot.* https://www.washingtonpost.com/news/the-switch/wp/2016/06/30/the-brave-escape-and-untimely-demise-of-one-russian-robot/

Thomas, N. (2019, November 11). AI sensor keep fuel flowing at Europe´s largest refinery, *Financial Times*. https://www.ft.com/content/bfbac636-ee8b-11e9-a55a-30afa498db1b

Victoria, M. y Nadal, S. (2020, December 8). Los algoritmos que permiten recuperar idiomas perdidos. Un sistema de inteligencia artificial desarrollado por el MIT pretende descifrar lenguas desaparecidas y conocer más sobre las personas que las hablaron, *El País*. https://elpais.com/retina/2020/12/07/innovacion/1607359036_565608.html

Zuboff, S. (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Publicafairsbook.

Zuckerberg, M. (2018, November 15). *A Blueprint for Content Governance and Enforcement, Menlo Park: Facebook.*https://m.facebook.com/nt/screen/?params=%7B%22note_id%22%3A751449002072082%7D&path=%2Fnotes%2Fnote%2F&refsrc=deprecated&_rdr