OXÍMORA. REVISTA INTERNACIONAL DE ÉTICA Y POLÍTICA
NÚM 20. ENE-JUN 2022. ISSN 2014-7708. PP. 1-37
DOI: 10.1344/oxi.2022.i20.38108

La algoritmización en el mundo del capitalismo de la vigilancia

Algorithmization in the World of Surveillance Capitalism

L'algoritmització en el món del capitalisme de la vigilància

José Antonio Estévez Araujo
Universitat de Barcelona
jestevez@ub.edu

Recibido: 18/01/2022
Aceptado: 25/01/2022

Resumen Las empresas del capitalismo de la vigilancia, como Google o Facebook (y muchísimas otras, menos gigantescas y conocidas) recopilan inmensas cantidades de información sobre nosotros. Sus algoritmos nos clasifican y establecen correlaciones estadísticas a partir de nuestros datos que les permiten predecir y manipular nuestra conducta. Junto con las empresas, los poderes públicos han construido un auténtico "complejo estatal-industrial" de la vigilancia. El uso de los algoritmos plantea cruciales problemas ético-políticos, cuando afectan a los derechos fundamentales, especialmente aquéllos que son capaces de aprender por sí mismos y reprogramarse autónomamente. La irrupción de los algoritmos del capitalismo de la vigilancia en una esfera de la vida transforma su estructura y su lógica de funcionamiento. Como consecuencia se nos está despojando de nuestra identidad y alejándonos de las prácticas democráticas. Tenemos pocos recursos jurídicos para defendernos de esa colonización. Pero eso no significa que debamos resignarnos y aceptar la presente situación. Multitud de personas y organizaciones están desarrollando formas de resistencia al despotismo del capitalismo de la vigilancia. Luchan por la creación de una ciudadanía digital todavía por venir.

Palabras clave Algoritmos, algoritmización, capitalismo de la vigilancia, ciudadanía digital, polarización política, privacidad, redes sociales.

Abstract The companies of surveillance capitalism, such as Google or Facebook (and many, many others, less gigantic and less well known) collect immense amounts of information about us. Their algorithms classify us and establish statistical correlations from our data that allow them to predict and manipulate our behaviour. In conjunction with corporations, the public authorities have built a genuine "state-industrial complex" of surveillance. The use of algorithms raises crucial ethical and political issues when they affect fundamental rights, especially those that are capable of learning by themselves and autonomously reprogramming themselves. The intrusion of surveillance capitalism's algorithms into a sphere of life reshapes its structure and its functioning logic. As a result, we are being stripped of our identity and alienated from democratic practices. We have few legal resources to defend ourselves against this colonisation. But this does not mean that we should resign ourselves and accept the present situation. Many people and organisations are developing forms of resistance to the despotism of surveillance capitalism. They are fighting to create a digital citizenship that is still to come.

Keywords Algorithms, Algorithmization, Surveillance Capitalism, Digital Citizenship, Political Polarisation, Privacy, Social Networks.

Resum Les empreses del capitalisme de la vigilància, com Google o Facebook (i moltíssimes altres, menys gegantesques i conegudes) recopilen immenses quantitats d'informació sobre nosaltres. Els seus algorismes ens classifiquen i estableixen correlacions estadístiques a partir de les nostres dades que els permeten predir i manipular la nostra conducta. Juntament amb les empreses, els poders públics han construït un autèntic "complex estatal-industrial" de la vigilància. L'ús dels algorismes planteja crucials problemes ètic-polítics, quan afecten els drets fonamentals, especialment aquells que són capaços d'aprendre per si mateixos i reprogramar-se autònomament. La irrupció dels algorismes del capitalisme de la vigilància en una esfera de la vida transforma la seva estructura i la seva lògica de funcionament. Com a conseqüència se'ns està despullant de la nostra identitat i allunyant-nos de les pràctiques democràtiques. Tenim pocs recursos jurídics per a defensar-nos d'aquesta colonització. Però això no significa que hàgim de resignar-nos i acceptar la present situació. Multitud de persones i organitzacions estan desenvolupant formes de resistència al despotisme del capitalisme de la vigilància. Lluiten per la creació d'una ciutadania digital encara per arribar.

Paraules clau Algoritmes, algorimització, capitalisme de la vigilància, ciutadania digital, polarització política, privacitat, xarxes socials.

Introducción

No descubro nada nuevo diciendo que el uso de algoritmos se está extendiendo a más y más ámbitos de la vida social y personal y que los dispositivos algorítmicos son cada vez más potentes, tienen la capacidad de gestionar cantidades crecientes de información y de realizar operaciones cada vez más complejas. Pero quizá es menos conocido el hecho de que la "algoritmización" de las diferentes esferas de la vida está provocando cambios estructurales tanto en el ámbito público como privado.

Este texto pretende ser un análisis de dichos cambios estructurales. Para ello, será necesario, en primer lugar, caracterizar el contexto en el que está teniendo lugar la algoritmización: el mundo del capitalismo de la vigilancia. Será preciso también ofrecer algunas nociones básicas acerca del funcionamiento de los algoritmos. Habrá que señalar asimismo qué problemas ético-políticos plantea la utilización de algoritmos en el mundo del capitalismo de la vigilancia, especialmente en el caso de aquellos que son capaces de aprender por sí mismos y tomar decisiones autónomamente.

El análisis de los efectos estructurales de la colonización algorítmica en el mundo del capitalismo de la vigilancia nos permitirá descubrir una serie de cambios profundos que se están produciendo en el ámbito privado y en el público: se está modificando la lógica de nuestras relaciones personales y el funcionamiento de la esfera pública. Estos efectos estructurales son potenciados por la falta de regulación y la consiguiente indefensión jurídica de las personas.

Hay quienes afirman que existe una actitud generalizada de resignación ante esta situación. Pero eso no se ajusta a la verdad. Hay multitud de personas que realizan acciones de autodefensa de sus "derechos digitales" y de organizaciones que desarrollan campañas para que esos derechos sean efectivamente reconocidos y protegidos. Podemos decir que todos ellos están luchando por una ciudadanía digital que está todavía por venir.

Parte 1: Algoritmos, ética y política

1. Relevancia ético-política de las decisiones algorítmicas

En un libro titulado "Cloud Ethics" (Amoore, 2020) expresión que tiene el doble sentido de "ética en o para la nube" y "ética nublada o nubosa", Louise Amoore reflexiona acerca del funcionamiento de diferentes tipos de máquinas inteligentes: coches autónomos, robots médicos, sistemas de vigilancia policial que predicen disturbios, armas letales autónomas... Los diferentes algoritmos que Amoore analiza tienen una característica en común: proporcionan respuestas "accionables" (Amoore, 2020, p. 4). Dicen cosas como "hay una probabilidad muy alta de que este condenado reincida". Y eso se traduce en imponerle una condena de cárcel en lugar de la realización de trabajos comunitarios, en alargar la duración de su pena de prisión, o en negarle la libertad condicional. Lo mismo ocurre con los algoritmos que predicen que "es altamente probable que esta persona incumpla los términos de su visado". La traducción en una acción consiste en negar la entrada al país al alguien que quiere atravesar la frontera. Las decisiones de los algoritmos afectan, pues, a personas concretas, pueden restringir sus derechos o incluso determinar si tienen que morir (como en el caso de los sistemas inteligentes de armas letales, pero también de los coches autónomos).

Si los algoritmos hacen propuestas que afectan directamente a personas concretas, es obvio que su utilización planteará problemas ético-políticos.

El primero de ellos es para qué y cómo se usan esos algoritmos. Lo primero que nos suele venir a la cabeza cuando nos planteamos esa cuestión son las amenazas que las técnicas algorítmicas representan para la libertad, la privacidad o, incluso, la vida. Pero resulta obvio que los algoritmos pueden utilizarse también en beneficio de las personas y como un instrumento de defensa de los derechos humanos.

Así, por ejemplo, se están desarrollando experiencias pioneras que utilizan algoritmos para la investigación de crímenes de guerra con el objetivo de conseguir pruebas que puedan presentarse ante los tribunales. Una de estas tentativas tiene como objetivo investigar si la coalición liderada por Arabia Saudí ha utilizado bombas de racimo, un arma prohibida por el Derecho Internacional, en la guerra de Yemen.

El proyecto está liderado por la universidad británica de Swansea. En 2017 se creó una base de datos para recoger imágenes y vídeos de la guerra extraídos de las redes sociales o aportados por periodistas o miembros de ONG's. Posteriormente se diseñó un sistema de "machine learning" utilizando algoritmos y bases de datos que permitieran al sistema reconocer si en alguna imagen se veía un modelo específico de bomba racimo, la BLU63, fabricada en Estados Unidos. Se pretendía, entre otras

cosas, que el gobierno británico prohibiera la venta de armas a Arabia Saudí y crear evidencias de que la coalición liderada por ese país estaba cometiendo crímenes de guerra[1].

A pesar de que los algoritmos puedan ser utilizados para objetivos loables como ese proyecto, el planteamiento que considera la tecnología como un instrumento moralmente neutro que puede usarte tanto para hacer el bien como el mal, resulta insuficiente de cara a abordar los problemas ético-políticos que plantea la técnica en general y los dispositivos algorítmicos en particular.

Cuando se adopta la perspectiva de la neutralidad de la técnica, es habitual que se presente el desarrollo tecnológico como un proceso que obedece únicamente a la lógica interna de la investigación científica. Ese planteamiento subyace, por ejemplo, a la propuesta de Reglamento que se está discutiendo en la UE sobre los usos de la Inteligencia Artificial: por ejemplo, en la exposición de motivos se señala que "la presente propuesta presenta un enfoque normativo horizontal, equilibrado y proporcionado, para la IA, que se limita a establecer los requisitos mínimos necesarios para subsanar los riesgos y problemas vinculados a la IA, *sin obstaculizar ni impedir indebidamente el desarrollo tecnológico*" (cursivas mías).

En realidad, la tecnología disponible en un momento determinado es fruto de decisiones de política científica adoptadas previamente que han establecido la prioridad de unas líneas de investigación sobre otras. La decisión acerca de qué se va a investigar no tiene carácter técnico, aunque el conocimiento científico tenga un papel crucial a la hora de fundamentar las decisiones que se adopten. Por tanto, el encuentro entre la ética y la técnica se produce en un momento o fase anterior a la de la decisión de para qué y cómo se va a utilizar una determinada tecnología.

Por otro lado, la tecnología puede producir efectos secundarios perjudiciales sea cual sea la forma y el fin para el que se use. La energía atómica es intrínsecamente peligrosa tanto si se utiliza para producir ojivas nucleares como si se usa para generar energía eléctrica (lo que no significa, en absoluto que sea éticamente indiferente utilizarla para uno u otro fin). Los desechos radiactivos constituyen una "basura" enormemente tóxica, extraordinariamente difícil de tratar y con unos efectos contaminantes más duraderos que cualquier institución creada por la humanidad a lo largo de su historia.

2. El capitalismo de la vigilancia

Los problemas ético-políticos que plantean el uso de los algoritmos, el desarrollo tecnocientífico ligado a estas herramientas y el cambio tecnológico que están

[1] Tuve noticia de esta aplicación de los algoritmos en el Congreso "Inteligencia Artificial y Derecho", celebrado en la Facultad de Derecho de la Universidad de Cantabria los días 14 y 15 de octubre. Concretamente, gracias a la ponencia presentada por Manuel Baena Pedrosa titulada "Inteligencia artificial en la persecución de crímenes internacionales". Puede encontrarse información más detallada sobre el proyecto relativo a la guerra de Yemen en un artículo de Karen Hao (Hao, 2020).

propiciando no pueden ser examinados adecuadamente en abstracto, sino que deben ser analizados en un contexto histórico-social definido por la globalización neoliberal, la revolución informática y el surgimiento del llamado "capitalismo de la vigilancia" (Zuboff, 2019).

La globalización neoliberal se gesta junto con la tercera revolución industrial (Capella, 2008), que se basa en el desarrollo de las tecnologías de la información y la comunicación (TIC).

Cada una de las revoluciones tecnológicas acaecidas en la historia han proporcionado a los seres humanos nuevas capacidades y poderes. La máquina de vapor creó una fuente de energía cualitativamente nueva, que nos liberó de las limitaciones de la fuerza física, tanto humana como animal. La revolución biotecnológica nos otorgó la potestad demiúrgica de crear vida mediante la ingeniería genética, pero su desarrollo no hubiera sido posible sin la informática. La revolución digital ha proporcionado a la especie humana un poder extraordinario para manejar información que se traduce en la capacidad de transmitir, almacenar y procesar enormes cantidades de información en periodos de tiempo infinitesimales.

La base de ese poder es la digitalización, que consiste en la facultad de crear "objetos digitales". Lo material está hecho de átomos y lo digital, de bits, según la afortunada expresión de Negroponte en un libro tenido por un clásico y titulado "Ser digital" (Negroponte, 1995)[2]. "Bit" es un acrónimo de *binary digit* y se utiliza para designar cada uno de los dígitos que se utilizan en un sistema numérico binario, o sea, el 0 y el 1. Los objetos que pueblan el mundo digital están hechos de información codificada binariamente, es decir que las "cosas" digitales son cadenas de unos y ceros. Estos entes son más leves y fluidos que los materiales y generalmente se mueven en un medio electromagnético.

La información digitalizada se puede almacenar en mucho menos espacio que el papel y transmitir a la velocidad de la luz en grandes cantidades, sin que importe la distancia entre el emisor y el receptor. Nuestro poder de computación nos permite clasificar, ordenar, analizar, agregar y correlacionar enormes cantidades de información con una rapidez inusitada. Todas esas nuevas capacidades han experimentado, además, un crecimiento exponencial durante las últimas tres décadas. Los módems de la época de Negroponte permitían transmitir 28.8 kbit/s. Hoy en día, con la fibra óptica un usuario doméstico dispone de una velocidad 35.000 veces mayor.

El poder de gestionar información que ha proporcionado la revolución digital está muy desigualmente repartido. Si miro a quienes están peor que yo, constato un enorme desequilibrio. La "brecha digital" que existe entre unas personas y otras se ha puesto de relieve con el desarrollo de la enseñanza online durante la pandemia en nuestro país. No es lo mismo que un estudiante disponga de una conexión de

banda ancha a Internet o no cuente con ella. La situación de quienes tienen su propio ordenador es incomparablemente mejor que la de los que han de compartirlo con sus hermanos o con toda la familia. Las desigualdades son mucho mayores si pensamos en los estudiantes del Sur global, que carecen de conexión a la Red en su domicilio (si es que siquiera disponen de un ordenador). Por eso, el acceso universal a Internet es una de las reivindicaciones más extendidas entre las organizaciones de defensa de los derechos digitales.

Si uno mira hacia "arriba", se percibe una enorme concentración de poder. En 2013[3] Google debía tener, calculando por lo bajo, un par de millones de servidores cada uno con una capacidad de al menos 4 terabytes. Eso supone un espacio de almacenamiento 8 millones de veces mayor del que tengo yo ahora, ocho años después, y más del doble del que disponía la Agencia de Seguridad Nacional estadounidense (NSA) por entonces. Google Search realizaba 4 millones y medio de búsquedas por minuto a petición de sus usuarios, lo que pone de manifiesto la enorme capacidad de transmitir y gestionar información que la empresa debía tener. En la actualidad, el poder de Google debe ser mucho mayor.

La materia prima del capitalismo de la vigilancia son los datos acerca de la actividad de los usuarios en internet y en otros ciberespacios como las redes de telefonía digital. Para recolectar el mayor número de datos posible, las plataformas digitales precisan que sus usuarios estén permanentemente conectados y que interactúen constantemente con otros usuarios o con la propia plataforma. La incitación para conectarse e interactuar, así como el análisis de los datos que se recolectan, se llevan a cabo utilizando algoritmos cada vez más sofisticados.

El negocio de las empresas de este sector es un nuevo tipo de publicidad basado en ofertas personalizadas lo que explica la insaciable voracidad de datos de que hacen gala las plataformas digitales. La obtención de beneficios en ese sector ha sido el impulso económico fundamental que ha determinado el desarrollo de las tecnologías digitales.

Las actuales técnicas de análisis de datos permiten prever nuestras reacciones frente a determinados estímulos. Esta capacidad es la que se utiliza para ofrecernos productos o servicios acordes con los gustos e intereses que hemos ido manifestando por medio de nuestra interacción con la plataforma y, en general, a través de nuestra actividad en Internet. Permiten también predecir las circunstancias concretas en las que una oferta resultará más eficaz, incitándonos a consumir un determinado producto.

Las características de la información digitalizada y la enorme concentración del poder para gestionarla es lo que ha hecho posible la creación de los sistemas de

[3] Esas son las únicas cifras que he sido capaz de encontrar y, comparadas con hoy, las diferencias deben ser inconmensurables.

cibercontrol ubicuos y permanentes característicos de las llamadas "sociedades de la vigilancia". La búsqueda del beneficio económico por parte de las empresas del capitalismo de la vigilancia ha sido el motor principal para la construcción de un dispositivo de supervisión total.

3. Internet: del anonimato originario al control total

Un fenómeno paradigmático del tipo de desarrollo tecnológico impulsado por el capitalismo de la vigilancia ha sido la transformación de Internet –que originariamente fue concebido como un espacio de libertad–, en un sistema de rastreo global (Lessig, 2009).

En los años sesenta del pasado siglo se realizaron las primeras experiencias de comunicación entre computadores distantes entre sí, y en los setenta empezaron a surgir las primeras redes informáticas que conectaban ordenadores de diversas universidades. El protocolo TCP/IP posibilitó la interoperabilidad entre las distintas redes existentes en 1981, es decir, permitió que un mensaje pasara de una red física a otra. Su invención dio lugar al nacimiento de Inter-net (entre redes o red de redes).

La arquitectura originaria no exigía saber quién hacía qué en Internet ni dónde lo hacía. Para enviar un correo electrónico o un archivo (las únicas actividades que entonces se realizaban a través de la red) no era necesario informar a los dispositivos de tránsito de la identidad del emisor o del receptor, del contenido del mensaje o del lugar desde dónde se envió. Los mensajes se dividían en paquetes de datos que se expedían por separado. En las intersecciones de la red, los routers encaminaban esos paquetes por la vía que parecía más rápida. Los paquetes llevaban una etiqueta con la dirección IP del remitente y del destinatario. Mostraban también la información necesaria para reconstruir íntegramente el mensaje original. No era preciso revelar el contenido de los paquetes o el tipo de datos (de imagen, de texto, de vídeo…) que transportaban.

Esta arquitectura posibilitaba el anonimato y respondía muy bien a la filosofía libertaria, muy extendida en el mundo de Internet desde sus orígenes. Por ello, resulta paradójico que la "Red" se haya podido convertir en un mecanismo de vigilancia y control total.

La des-anonimización de Internet tuvo lugar durante los años noventa bajo el impulso de las compañías privadas que hacían negocios por medio de la red. Tres agentes fueron decisivos en este proceso: los proveedores de acceso a Internet de pago, las páginas web comerciales y determinadas aplicaciones utilizadas masivamente, como el motor de búsqueda de Google.

Originariamente, las personas tenían acceso a Internet a través de las universidades, lo que limitaba mucho el número de usuarios. En los años noventa surgieron y proliferaron las empresas que ofrecían acceso de pago a Internet, generalmente

vinculadas a las grandes compañías de telecomunicaciones. Los proveedores de acceso a Internet constituyen una plataforma de vigilancia fundamental porque pueden asociar las direcciones IP de sus clientes con su identidad personal, pues son estas empresas las que asignan la IP a sus usuarios. Estos agentes pueden también rastrear la actividad de los dispositivos de sus clientes en la red, porque toda ella se vehicula a través de sus servidores.

Las páginas web comerciales utilizaron mecanismos de identificación y rastreo desde su aparición en los años noventa. Se trata de las llamadas "cookies", algunas de cuyas funcionalidades eran necesarias para que el comercio online fuera posible. Las "galletas" pequeñas piezas de software que las páginas instalan en el ordenador del usuario. Por medio de las cookies el propietario del sitio puede saber si se ha accedido a la web desde ese dispositivo anteriormente y también obtener datos acerca de su navegación por otras páginas. Es un verdadero espía que monitoriza a los internautas sirviéndose de sus propios ordenadores. En el momento en que la Web se convirtió en el centro de la actividad de Internet, especialmente la de carácter comercial, las cookies se transformaron en un mecanismo de vigilancia generalizado. Sus capacidades de inspección se intensificaron con la utilización de webs que exigían estar registrado para poder acceder, pues en ese caso las galletas-espía no se limitaban a rastrear la actividad del ordenador, sino que también podían conocer la identidad del usuario.

También en los años noventa aparecen aplicaciones cuyo objetivo central es la recopilación y procesamiento de datos de los usuarios. El primer ingenio de este tipo fue el motor de búsqueda de Google, que se implantó en 1998. La empresa guardaba un registro de todas las búsquedas llevadas a cabo por sus usuarios y las asociaba a su IP (algo que no descubrieron los estadounidenses hasta el año 2006). Si una persona tenía una cuenta en Google, la compañía podía descubrir también su identidad. Los datos se recogían y utilizaban con fines publicitarios. Google es, fundamentalmente, una agencia de publicidad, y la gran mayoría de sus ingresos proviene de su actividad en ese campo. El servicio que Google proporcionaba a sus clientes era posicionar sus anuncios en los resultados de las búsquedas de manera que sus ofertas se orientaran mejor hacia los deseos y preferencias del usuario puestos de manifiesto en esa y anteriores exploraciones. Se instauró un sistema de "pay per-clic", en virtud del cual las empresas patrocinadas pagaban en función de las veces que su hipervínculo era activado.

Google fue la compañía pionera del capitalismo de la vigilancia y marcó el camino para las que se sumaron posteriormente a ese negocio.

Si las actividades combinadas de los proveedores de acceso a Internet, las páginas web y el motor de búsqueda de Google desanonimizaron la Red durante los años noventa, a partir de la década siguiente, con el desarrollo de la telefonía digital, la vigilancia digital dio un salto cualitativo y pasó a ser ubicua. A partir de ese momento

ya no sólo se supervisa a los usuarios cuando están navegando a través de Internet por medio de un ordenador de sobremesa. El teléfono móvil primero y el smartphone después permitieron que se rastreara su actividad allí donde estuviera. Los "móviles" cuyo uso se generaliza a finales de la década de los noventa, son dispositivos digitales que utilizan una red propia, distinta de Internet. Estos teléfonos ya permitían que las compañías geolocalizasen a sus clientes por medio de las antenas a las que se conectaban los dispositivos. Al guardar los registros, se podían reconstruir los trayectos que esas personas habían recorrido. Las compañías pueden también almacenar los metadatos de las llamadas y, de hecho, lo hacen.

Con el smartphone, que llega la década siguiente, el poder de vigilancia se intensifica. Las capacidades de geolocalización propias de los móviles se mantienen y a ellas se suman los dispositivos GPS. Las Apps "gratuitas" tienen acceso a mucha información almacenada en los teléfonos. Basta con ver los permisos que solicitan para poder instalarlas, los cuales, en muchas ocasiones no tienen ninguna relación con las funcionalidades de la aplicación. También rastrean la actividad de los usuarios y almacenan esos datos. Hoy en día hay aplicaciones que monitorizan nuestro cuerpo, como las que cuentan los pasos que damos, nos guían para seguir una dieta o ejercitarnos, miden los latidos del corazón o supervisan el ciclo menstrual. Con la pandemia, se han desarrollado aplicaciones para rastrear los contactos, algunas realmente invasivas.

4. La vigilancia estatal masiva

Como se ha visto en el apartado anterior, las compañías privadas impulsaron el control de la actividad en el espacio digital desde los noventa. Los estados siguieron su estela de forma sistemática a partir de la década siguiente, como un arma en la llamada "guerra contra el terrorismo" tras los sucesos acaecidos el 11S.

La utilización de formas de vigilancia masiva por parte de los poderes públicos supone un alejamiento de los principios que regulan la actividad policial en un estado de derecho durante los periodos de normalidad. El seguimiento de la policía debe limitarse a las personas sospechosas. Sus aspectos más intrusivos, como el registro domiciliario o la intervención de las comunicaciones deben ser autorizados por un juez. Los agentes deben presentar en el juzgado las pruebas e indicios que tienen en su poder para justificar la vigilancia. Es decir, deben demostrar ante el juez que han recopilado suficientes evidencias para considerar a esa persona concreta como sospechosa.

Las formas de vigilancia masiva, por el contrario, se ejercen de manera indiscriminada y no únicamente sobre determinadas personas. Tratan a todo el mundo como sospechoso o, dicho de otra manera, no vigilan a los sospechosos, sino que los crean (Andrejevic, 2017).

La utilización de cámaras de vigilancia equipadas con sistemas de reconocimiento facial constituye un mecanismo de vigilancia estatal masiva que es objeto de una intensa polémica en la actualidad en Europa. Son profusamente usadas en Gran Bretaña, donde son objeto de una fuerte contestación. En este país pueden instalarse cámaras de ese tipo sobre el techo de las furgonetas de la policía. Se utilizan tanto para identificar a las personas que acuden a un evento deportivo como a quienes participan en manifestaciones de protesta. Estos dispositivos con capacidad de reconocer a las personas utilizando los datos biométricos de sus rostros suscitan varios tipos de problemas: constituye una técnica más invasiva que la de pedir el documento de identidad a todos los que pasan; los viandantes pueden no ser conscientes de que están siendo identificados por la policía; estas cámaras permiten a los agentes asociarnos a todo nuestro historial almacenado en sus bases de datos, por lo que la policía tiene acceso a mucha más información que la contenida en nuestra documentación…

Otro problema que plantean las cámaras de reconocimiento facial, al menos en Gran Bretaña, es cómo se han obtenido las imágenes para llevar a cabo el análisis biométrico de los rostros. Las imágenes provienen de las cámaras de vigilancia que pueblan el país (privadas en su mayoría) y se encuentran por todas partes. También se han extraído de las fotos colgadas en las redes sociales. Es como si les hubieran tomado las huellas digitales a los británicos mientras dormían y sin que se dieran cuenta.

Al smartphone y las cámaras se suma la llamada Internet de las cosas como otro de los mecanismos que hacen posible la "externalización" de la vigilancia digital al mundo material. Ahí encontramos, entre otras cosas, los dispositivos "inteligentes" que pueblan los hogares de manera creciente. Estos aparatos están conectados a Internet o bien se gestionan mediante una App del móvil con conexión a la red. Están equipados con sensores de todo tipo y transmiten grandes cantidades de información sobre nuestros hábitos, gustos y sobre el hogar mismo. Entre ellos se cuentan termostatos, asistentes virtuales como Alexa, aspiradoras robots e incluso camas y ropa.

Así pues, el desarrollo del cibercontrol fue impulsado por las empresas del capitalismo de la vigilancia. Posteriormente, los estados utilizaron los instrumentos y los servicios de las compañías privadas para desarrollar formas de vigilancia masiva. Este proceso produjo hibridaciones público-privadas creando un auténtico "complejo estatal-industrial de la vigilancia" (Hayes, 2012). Hoy en día las empresas privadas realizan multitud de tareas para los estados, tanto en el sector civil como en el militar, como labores de control policial o pruebas forenses y los poderes públicos utilizan los datos recopilados por las compañías para sus fines de vigilancia masiva.

5. El algoritmo, sus clases y sus capacidades

Como se ha señalado en la introducción, este artículo pretende analizar una serie de problemas ético-políticos que plantean los algoritmos, referidos no sólo a la manera como se usan, sino también a las dinámicas que impulsan su desarrollo y a los efectos colaterales que su difusión por todas las esferas de la vida está provocando. Hemos visto ya que el contexto en el que se plantean estas cuestiones está marcado por el llamado "capitalismo de la vigilancia". Pero para entender el contenido y alcance de los problemas que se examinan es necesario tener algunas nociones básicas relativas a la naturaleza y funcionamiento de los algoritmos.

5.1. Pero… ¿qué es un algoritmo?

Esta es una pregunta que raramente se plantea. Generalmente se da por supuesto que todo el mundo sabe la respuesta. Pero cuando alguien tiene el atrevimiento de formular explícitamente la cuestión en un foro en el que puede haberse estado hablando durante horas o incluso días de la regulación del uso de los algoritmos, se encuentra con que los tenidos por expertos no se dan por aludidos o escurren el bulto de manera más o menos afortunada.

Después de indagar acerca del tema durante bastante tiempo y sin haber sido capaz de encontrar una fórmula universalmente aceptada, la concepción que me parece más clara, general y convincente es que un algoritmo es una secuencia de pasos o conjunto de instrucciones que deben seguirse para resolver un determinado problema. Así, una receta de cocina sería un algoritmo que nos permite solucionar la cuestión de cómo hacer, por ejemplo, una buena tortilla de patatas. De acuerdo con esta concepción, los algoritmos son mucho más antiguos que la revolución digital. Pitágoras diseñó algunos muy ingeniosos para resolver problemas geométricos. Pero cuando hablamos de "algoritmos" en la actualidad nos referimos generalmente a los de carácter "computacional", es decir, a secuencias de instrucciones que pueden ser comprendidas y ejecutadas por un ordenador o por un dispositivo complejo que cuenta con un computador entre sus componentes.

5.2. Algoritmos deductivos e inductivos

Cada algoritmo o, al menos, cada uno de los tipos de algoritmos que existen en la actualidad constituyen otros tantos mundos, por lo que resulta difícil afirmar demasiadas cosas que se puedan aplicar sin matices a todos ellos. No podemos explorar aquí todos esos universos. Pero, a efectos del análisis de los problemas ético-políticos que plantean y que constituyen el objeto de este trabajo, es preciso, cuando menos, diferenciar dos grandes clases de algoritmos: los denominaré respectivamente "deductivos" e "inductivos".

Los algoritmos deductivos están constituidos por series finitas de instrucciones o pasos elaborados sobre la base de un modelo matemático que sirve para seleccionar las características y las variables que serán consideradas relevantes. Están

compuestos de series de reglas ordenadas que tienen la estructura sintáctica propia de las sentencias condicionales, es decir: "si se da la situación A, entonces realiza la operación B". La secuencia de pasos a seguir para solucionar el problema es diseñada de principio a fin por un programador. El ordenador se limita a seguir las instrucciones de manera análoga a como lo hace con buena parte del software que utilizamos habitualmente en casa o en el trabajo.

Los algoritmos "inductivos" son muy diferentes. En su libro, Louise Amoore (Amoore, 2020) se centra en particular en los algoritmos utilizados en un tipo de máquinas virtuales dotadas de inteligencia artificial llamadas "redes neuronales". Estos mecanismos se diferencian de los que se sirven de algoritmos "deductivos" en dos aspectos cruciales: a) son capaces de aprender y de reprogramarse autónomamente; b) los resultados a los que llegan pueden ser imprevisibles e inexplicables incluso para los programadores que los diseñaron.

La autora insiste repetidamente en su libro acerca del diferente carácter de ambos tipos de algoritmos:

> La representación de los algoritmos como una cadena lógica pasa por alto el grado en que los algoritmos se modifican a sí mismos en y a través de sus relaciones iterativas no lineales con los datos de entrada. (Amoore, 2020, p. 11)

O bien:

> Entiendo que la escritura del algoritmo excede sustancialmente la escritura del código fuente y se extiende a la escritura iterativa, la edición y la reescritura producto de nuevos conjuntos de datos, de seres humanos y de otros algoritmos. (Amoore, 2020, p. 43)

5.3. ¿Qué pueden hacer los algoritmos?

Los algoritmos son capaces de realizar muchos tipos de operaciones diferentes. Para los propósitos de este texto nos interesan especialmente sus capacidades de reconocimiento, clasificación, establecimiento de correlaciones estadísticas, aprendizaje y reprogramación.

Los algoritmos pueden reconocer objetos o personas a partir de datos digitalizados proporcionados por diversos tipos de sensores o depositados en distintas clases de "bancos". Por ejemplo, la cámara de un smartphone puede seleccionar los rostros humanos que aparecen en la escena que estamos enfocando cuando queremos sacar una fotografía. Es decir, puede distinguir las caras de otros tipos de elementos y proceder a encuadrarlas. Es capaz de realizar esta operación de reconocimiento porque ha aprendido cuál es el conjunto de patrones que caracterizan una faz humana.

Un algoritmo no sólo es capaz de reconocer un rostro en una escena o imagen, sino también identificar a la persona a quien pertenece. Es lo que hacen los llamados "sistemas de reconocimiento facial" utilizados por la policía de diversos países y de los que hemos hablado más arriba. Estos sistemas se sirven de sofisticadas cámaras de vigilancia y bancos de datos –en los que se han recopilado numerosas imágenes de "personas de interés", cuando no de toda la población– para conocer la identidad de quien participa en una protesta o de alguien que deambula por un aeropuerto.

Los algoritmos pueden determinar si un objeto o una persona pertenecen a una determinada clase. Lo hacen examinando si posee los atributos que definen el conjunto de que se trate. Por ejemplo, son capaces de decidir si las características de un mensaje de correo electrónico permiten o aconsejan clasificarlo como "spam".

Los conjuntos son definidos originariamente por el programador o diseñador del algoritmo. Este puede hacerlo proporcionando datos estructurados al dispositivo clasificados en categorías mediante, por ejemplo, una hoja de cálculo. También tiene la posibilidad de definir las diferentes clases de cosas o personas etiquetando imágenes, textos, sonidos, o cualquier otro tipo de archivo digital. Poner etiquetas es una tarea larga y engorrosa, especialmente cuando se utilizan grandes bases de datos. Por eso las plataformas a veces engañan a sus usuarios para que realicen ese trabajo de forma gratuita. Así, cuando identificamos unas letras distorsionadas o la imagen de un barco para probar a Captcha que somos seres humanos, estamos también etiquetando textos e imágenes para alimentar a los algoritmos de reconocimiento de Google.

Para que un algoritmo sea capaz de reconocer y clasificar personas y cosas tiene que poseer la capacidad de aprender. Todos los algoritmos se programan, pero a algunos también hay que "entrenarlos".

Se les puede enseñar de diversas maneras. Por ejemplo, utilizando los datos etiquetados que hemos mencionado para que aprendan a clasificar cosas o personas. Los algoritmos que tienen que realizar operaciones de reconocimiento visual son entrenados mostrándoles una gran cantidad de imágenes. Si deben reconocer números escritos a mano, se utiliza una base de imágenes de dígitos manuscritos (las hay disponibles en Internet) para que aprendan a identificar patrones. Eso les permitirá reconocer si el número rotulado en el papel es un 1, un 7 o un 9. Si se trata de un sistema de reconocimiento facial habrá que realizar el entrenamiento mostrándole imágenes de rostros humanos extraídas de documentos oficiales o de las redes sociales.

Una vez finalizado el periodo de instrucción, algunos tipos de algoritmos son capaces de seguir aprendiendo "por su cuenta". Mientras operan, detectan nuevas características relevantes y perfeccionan sus clasificaciones afinando, por ejemplo, su capacidad de identificar qué mensajes son correo basura. También crean nuevos conjuntos de cosas o personas identificando nuevos atributos que resultan

adecuados para clasificarlas, de cara a resolver los problemas para los que deben ofrecer soluciones.

Los algoritmos pueden establecer correlaciones estadísticas entre conjuntos de personas o cosas. Es decir, pueden calcular la probabilidad de que, si una persona pertenece al conjunto A, forme parte también del conjunto B. Formulado de otra manera: pueden calcular qué grado de posibilidad hay de que alguien que pertenece al conjunto A, tenga, por ejemplo, los gustos que caracterizan a las personas del conjunto B o de que un objeto que tenga los atributos que definen el conjunto C, tenga también los que son característicos de la clase D.

Los algoritmos pueden calcular estas correlaciones estadísticas entre diversos conjuntos de atributos guiados por una hipótesis formulada por el programador o el usuario. Pero pueden también descubrir por sí mismos correspondencias inéditas y sorprendentes sin necesidad de partir de una hipótesis. Esta capacidad resulta especialmente útil en los análisis de grandes bancos de datos como los que se designan por medio de la expresión "big data".

5.4. Factores de imprevisibilidad

Denomino "factores de imprevisibilidad" a las capacidades que sustraen el funcionamiento del algoritmo al control del programador que lo creó o del técnico que lo utiliza. Me refiero a las facultades que les permiten llegar a resultados imposibles de ser previstos, e incluso explicados, por estos expertos. Se trata de una de las características de los algoritmos que hemos denominado "inductivos" y que hacen necesario diferenciarlos de los meramente "deductivos".

El aprendizaje no dirigido, la capacidad de detectar rasgos relevantes para crear nuevas clases de cosas, el poder de descubrir correlaciones estadísticas inéditas, todo ello unido a las facultades de reconocimiento y clasificación de personas y objetos, permiten que un algoritmo sea capaz de reprogramarse por sí mismo en función de sus propios hallazgos, y se convierta en un ente que tome sus propias decisiones. La autonomía de estos algoritmos inductivos exige que nos planteemos los problemas ético-políticos que suscita su uso de forma muy distinta a como lo hacemos en el caso de los algoritmos deductivos.

5.5. Las redes neuronales artificiales

Las redes neuronales artificiales constituyen los algoritmos inductivos con capacidad de adoptar decisiones autónomas más relevantes en la actualidad. Merece la pena dedicar un poco de tiempo a analizar en qué consisten.

Las llamadas "redes neuronales" son máquinas virtuales compuestas de "neuronas artificiales" conectadas entre sí. Las neuronas que integran la red tienen unas características funcionales similares a las que se encuentran en el cerebro humano. Pueden captar y emitir señales eléctricas. También cuentan con la capacidad de calibrar la importancia relativa de una señal atribuyéndole un determinado "peso".

Tienen asimismo un "umbral de activación" que determina cuándo emitirán una señal como reacción a un impulso concreto.

Las neuronas están distribuidas en diversas capas, dos de las cuales son "externas" y el resto se suelen caracterizar como "ocultas". La primera capa externa es la de "entrada". Las neuronas que la integran reciben los estímulos de "fuera": de los bancos de datos, de los sensores... La otra capa externa es la de "salida". El output que proporciona esa capa consiste en la solución óptima al problema planteado y su probabilidad de éxito. Cada neurona de una capa está conectada con todas las de la siguiente. Las diferentes capas actúan como una especie de filtros. La red parte de una gran cantidad inicial de información, de variables y de posibilidades. Cada una de las capas ocultas va descartando unas soluciones y optando por otras. La de salida está diseñada para ofrecer una solución única. Como dice Amoore, la red neuronal lleva a cabo una "condensación" (Amoore, 2020, p. 99) desde la multiplicidad hasta la unidad. Es decir, toma innumerables decisiones entre posibles alternativas, en base a parámetros que ella misma establece a partir de su capacidad de aprendizaje autónomo. Una red neuronal puede tener numerosas capas ocultas. En cada capa puede haber una gran cantidad de neuronas. Hay redes que contienen millones de ellas. A mayor cantidad de capas y neuronas más complejos serán los problemas que podrá resolver la red.

6. Problemas ético-políticos que plantea la utilización de algoritmos

El uso de los algoritmos en el mundo del capitalismo de la vigilancia plantea una serie de problemas ético-políticos. Estos pueden ser distintos o tener diferentes posibilidades de ser solucionados según se trate de algoritmos deductivos o inductivos. Analizaremos los más importantes y para centrarnos a continuación en la cuestión de cómo tratan los algoritmos a las personas.

6.1. Los algoritmos inductivos no fundamentan sus decisiones

Los algoritmos inductivos (especialmente las redes neuronales artificiales) realizan ponderaciones al igual que hacen los jueces. En caso de conflicto, los órganos judiciales determinan qué derecho, principio o bien jurídico debe prevalecer. Las premisas y criterios utilizados para la ponderación pueden tener carácter no sólo jurídico, sino también ético o político. Los argumentos esgrimidos en las sentencias de los tribunales constitucionales para establecer que un derecho fundamental prevalece sobre otro ponen claramente de manifiesto esto último.

Louise Amoore hace uso específicamente del término "ponderación" al referirse al modo como los algoritmos inductivos, especialmente las redes neuronales artificiales, razonan:

> La disposición de las proposiciones hace que un resultado aparentemente óptimo surja de la ponderación diferencial de los caminos alternativos a través de las capas de un algoritmo (Amoore, 2020, p. 13).

La diferencia entre los algoritmos y los jueces es que éstos últimos tienen que fundamentar sus sentencias. El juez ha de especificar qué hechos considera efectivamente acaecidos y en base a qué pruebas. Ha de exponer los fundamentos normativos que le han llevado a dictar su fallo en relación con los hechos juzgados. El algoritmo nos da una solución y una probabilidad de éxito que sería equivalente al "fallo". Pero el usuario del algoritmo o el destinatario de sus decisiones suelen desconocer cómo ha llegado el algoritmo a esa conclusión. Acceder al "código fuente" no proporciona un conocimiento suficiente de los factores que se han tenido en cuenta ni de las valoraciones que se han llevado a cabo en el caso de los algoritmos que hemos denominado "inductivos". No nos dirá qué pesos y umbrales de activación han utilizado las neuronas. Desconoceremos de dónde han extraído la información y por qué han seleccionado unos rasgos de los datos en lugar de otros.

El algoritmo nos ofrece una solución a un problema y su probabilidad de éxito (p. ej. un 90%). En su proceso de razonamiento, el algoritmo se encuentra con innumerables bifurcaciones. En diversos momentos puede haber escogido uno u otro camino basándose en una probabilidad menor (p. ej. del 60%). La probabilidad que da a su propuesta final oculta el grado de incertidumbre al que se ha enfrentado a la hora de realizar las opciones previas que finalmente le han conducido a proponer esa solución. Las decisiones de los algoritmos no están, por consiguiente, fundamentadas. No se exponen las premisas, valoraciones y opciones que han conducido a su output. Las decisiones de los jueces son siempre recurribles por los afectados. Las de los algoritmos, no.

Resulta dudoso si se pueden reconstruir todos los pasos que ha dado un algoritmo inductivo, por ejemplo, una red neuronal, para proponer una solución y calcular sus probabilidades de éxito. En ocasiones se utiliza la expresión "caja negra" para referirse al problema que plantean los algoritmos cuyos procesos son indescifrables. Otras veces se señala que abrir las tripas del algoritmo supone enfrentarse a una cantidad de datos tal que resulta imposible que puedan ser revisados por los seres humanos. Esta circunstancia aumenta las razones para considerar que las decisiones algorítmicas pueden ser arbitrarias: no sólo resulta imposible fundamentar sus decisiones en reglas preestablecidas, sino que parece que, en bastantes casos, tampoco pueden descifrarse sus razonamientos a posteriori. Si esas decisiones afectan a la libertad o la vida de personas concretas e identificables, la posibilidad de justificar su puesta en práctica (su "accionamiento") queda puesta en cuestión de modo radical.

6.2. Algoritmos y sesgos discriminatorios

Los sesgos discriminatorios constituyen uno de los problemas que más preocupan a quienes tratan el tema de la regulación de los algoritmos.

La distinción entre discriminación directa y discriminación indirecta utilizada en el ámbito jurídico resulta de utilidad para analizar el problema de los sesgos algorítmicos. La discriminación directa se da cuando la ley establece explícitamente tratos diferentes para las personas debido a su raza, género, ideología, religión… sin que exista una justificación razonable para ello. La discriminación indirecta tiene lugar cuando la ley no establece explícitamente distinciones basadas en el género o la raza, por ejemplo, pero el resultado estadístico de su aplicación se traduce en un trato perjudicial para las personas negras o para las mujeres.

En el caso de los algoritmos deductivos, los sesgos discriminatorios pueden evitarse o corregirse técnicamente con relativa facilidad si la discriminación es directa. En el caso de que el código contenga instrucciones que explícitamente establezcan diferencias de trato no justificadas entre hombres y mujeres o entre personas blancas y negras, será necesario eliminar o modificar dichas reglas reprogramando el algoritmo.

Cuando se constata que el algoritmo genera formas de discriminación indirecta, la cosa resulta un poco más complicada. Si su aplicación discrimina estadísticamente a las personas de raza negra o a las mujeres, entonces habrá que descubrir cuál es la instrucción que introduce ese sesgo. El problema puede ser producto, por ejemplo, de un paso del programa que obliga a tener en cuenta el tipo de barrio donde vive una persona a la hora de determinar su grado de solvencia económica. Si se da la circunstancia que en los barrios más pobres habita un mayor número de personas negras, el resultado de la utilización del algoritmo puede ser indirectamente discriminatorio para los afrodescendientes. Pero, en cualquier caso, localizar el defecto puede resultar una tarea bastante laboriosa.

Un algoritmo capaz de aprender autónomamente y de reprogramarse a sí mismo puede también discriminar indirectamente a las personas en función de su raza, género u otras “categorías sospechosas”. El sesgo puede constatarse analizando estadísticamente los resultados que va produciendo. Pero en el caso de estos algoritmos que hemos denominado “inductivos”, es muy difícil evitar o corregir sus tendencias discriminatorias. Los técnicos pueden modificar determinados parámetros del algoritmo, pero no pueden prever con exactitud cómo modificará eso los resultados que éste proporcione.

Amoore cuenta que: “como me explicó un informático, una red neuronal como AlexNet, con seis u ocho capas ocultas, es demasiado compleja para que el propio diseñador del algoritmo pueda delimitar las probabilidades condicionales que aprende. ‘Puedo ajustar la ponderación en esa capa’, explica, ‘y sé que esto cambiará la salida, pero no puedo decir exactamente cómo’. Al igual que con el diseño de

AlexNet, los informáticos trabajan con la naturaleza esencialmente experimental e incógnita del algoritmo (Amoore, 2020, p. 74).

7. ¿Cómo tratan los algoritmos a las personas?

Los algoritmos tratan a las personas como conjuntos de atributos. Las consideran como elementos de diversos conjuntos que, en ocasiones, el propio algoritmo ha creado para clasificarlas. Facebook tiene incluidos a cada uno de sus usuarios en cientos de conjuntos diferentes. La persona como singularidad única e irrepetible no existe para el algoritmo. Los seres humanos resultan intercambiables. Una vez establecido que en dos personas confluyen los mismos atributos, es indiferente tratar con una, con la otra o con ambas.

Uno de los ámbitos más sensibles donde se está expandiendo la utilización de algoritmos es el sistema punitivo de los estados. Ya se usan profusamente en Estados Unidos: sirven, entre otras cosas, para distribuir las patrullas de la policía por los diferentes barrios, detectar cuándo se cometen delitos con armas de fuego, identificar sospechosos… y también para determinar si se concede o no la libertad condicional a un preso, si se suspende la ejecución de una pena y, en algunos estados, se utilizan para fijar la propia duración de las condenas de cárcel. Estos últimos algoritmos "calculan" la peligrosidad del acusado o del reo, es decir el riesgo, de que reincida o de que viole la condicional.

No se trata de un fenómeno exclusivamente estadounidense. En España, se utilizan también procedimientos y mecanismos algorítmicos para diversos fines. Viogen es un algoritmo que se utiliza para predecir la posibilidad de reincidencia en los casos de violencia de género y sirve de base para la adopción de medidas preventivas, como las órdenes de alejamiento. La administración catalana utiliza un algoritmo para predecir el riesgo de reincidencia de los presos que se utiliza para decidir la concesión o no de la libertad condicional. Un sistema denominado "Veripol" es usado por la policía nacional para identificar denuncias falsas interpuestas por los particulares[4].

Uno de los problemas que plantea la algoritmización del proceso punitivo es el de la opacidad de los propios algoritmos. En Estados Unidos, los mecanismos de vigilancia policial o los instrumentos forenses son proporcionados por empresas privadas que se niegan a desvelar cómo funcionan sus algoritmos amparándose en los derechos de propiedad intelectual y la defensa frente a su copia por parte de sus competidores. Abogados, activistas y organizaciones luchan para que se desvelen los algoritmos que se utilizan en el proceso punitivo, especialmente los que se usan

[4] Esta información ha sido extraída de un artículo titulado "Cómo los algoritmos perpetúan la desigualdad en España", escrito por Laura Aragó y publicado en *La Vanguardia* el 26 de octubre de 2021. *https://www.lavanguardia.com/tecnologia/20211026/7814332/como-algoritmos-perpetuan-desigualdad-espana.html*

para la obtención de pruebas. Los acusados tienen derecho a conocer las pruebas que existen contra ellos, cómo se han obtenido y qué fiabilidad tienen. Se han dictado ya algunas sentencias judiciales que establecen la obligación de proporcionar esta información. Pero el desvelamiento del código fuente y de los modelos matemáticos que utilizan los algoritmos no resulta siempre suficiente para saber cómo toman sus "decisiones".

Como hemos dicho, en el sistema penal estadounidense, se utilizan algoritmos para calcular la peligrosidad del acusado: el riesgo de que reincida o de que viole la condicional. La determinación estadística de la peligrosidad es un método que castiga a las personas, no por sus actos, sino por lo que pueden llegar a hacer en el futuro. Maqueda ha caracterizado este fenómeno como una deriva "actuarialista" del derecho penal (Maqueda Abreu, 2021).

Pero, además de esta consideración de la "peligrosidad" como motivo para un castigo, hay otro aspecto de esta tendencia que resulta también muy preocupante. El riesgo de que una persona realice un acto dañoso en el futuro no se determina sólo en función de su trayectoria personal, sino también en base a lo que han hecho otros sujetos en el pasado. Se le castiga no sólo por su conducta pasada, sino también por la de otros.

Los bancos de datos proporcionan información acerca de un enorme número de casos acaecidos en el pasado. Los algoritmos establecen correlaciones estadísticas entre determinados atributos (o combinaciones de atributos) y el peligro de reincidencia o de violación de la condicional. Por ejemplo, el algoritmo puede descubrir una alta correlación estadística entre habitar en una determinada zona o formar parte de una familia monoparental y ser reincidente. Con ello, el sujeto al que se castiga es hecho responsable de hechos pasados en los que no ha tenido participación alguna.

Tratar a los seres humanos como meros centros de imputación de atributos conduce fácilmente a instrumentalizarlas. Instrumentalizar a una persona significa utilizarla como medio para alcanzar un determinado fin que es ajeno a sus intereses o derechos, cosa que puede causarle algún tipo de perjuicio. Los objetivos que se persiguen cuando se utiliza a la persona como un simple medio responden a los intereses de sujetos distintos a los de quien resulta mediatizado.

Los algoritmos tienen como función resolver un problema de forma eficaz, proporcionando la mejor solución posible. Esto significa que, en principio, la lógica instrumental rige tanto su diseño como su funcionamiento. El principio de eficacia y la lógica instrumental pueden atemperarse mediante la introducción de instrucciones éticamente motivadas. Pero si no se crean cortapisas de este tipo, los algoritmos utilizarán a las personas como simples medios para alcanzar sus fines.

Los casos de instrumentalización de las personas por parte de los algoritmos son frecuentes. En el ámbito del comercio electrónico, se dan muchos supuestos que

no parecen ser justificables como formas legítimas de competencia. Los algoritmos utilizados por las empresas que comercializan productos a través de Internet tienen acceso a muchos datos de los consumidores obtenidos de diversas fuentes, como las redes sociales. Este conocimiento les permite segmentar el mercado y hacer el tipo de ofertas que resulte más provechosa para la empresa y tenga la probabilidad mayor de ser aceptada por los clientes de un determinado espectro.

Esta estrategia comercial es "legítima", en principio, en una economía capitalista. Pero resulta frecuente que se crucen ciertas "líneas rojas" lo que suscita dudas ético-jurídicas acerca del modo de proceder de los algoritmos.

La primera es que el usuario puede no saber qué datos se han facilitado al algoritmo ni de dónde o cómo se han obtenido. La segunda es que el algoritmo suele ser "opaco". Al desconocer su funcionamiento, el consumidor no puede saber por qué se le hace una determinada oferta. La tercera línea que se puede traspasar conduce a prácticas claramente abusivas. El algoritmo puede disponer de datos que le permiten saber que el consumidor se encuentra en una situación de desamparo y "aprovecharse" de esa circunstancia para ofrecerle determinados productos o servicios. Por ejemplo, puede proponerle que suscriba un seguro de vida aprovechando el impacto psicológico producido por la muerte de un amigo o un familiar. Un algoritmo puede también presentar una oferta de provisión de acceso a Internet a un precio más alto que la media "aprovechándose" de que el destinatario es una persona de avanzada edad y que, por tanto, no es previsible que compare su propuesta con otras que pueden resultar más ventajosas.

Hemos analizado los problemas ético-políticos que plantea el uso de algoritmos en el mundo del capitalismo de la vigilancia. También hemos visto cómo los algoritmos instrumentalizan a los seres humanos. Pasaremos ahora a ver los efectos estructurales de la algoritmización.

Parte 2: La algoritmización del mundo

La proliferación del uso de algoritmos en el mundo del capitalismo de la vigilancia puede que acabe resultando comparable con la extensión de la burocracia a todos los ámbitos institucionales tanto públicos como privados. Weber resaltó la eficiencia, inigualable en su tiempo, de la organización burocrática. La burocracia podía utilizarse tanto para organizar un ejército como un hospital o una empresa de automóviles. Parecía un simple medio técnico para alcanzar un fin. La utilización ética de la organización burocrática dependería del objetivo al que sirviera. No obstante, poco a poco, se fueron manifestando las consecuencias estructurales de la burocratización del mundo. La organización burocrática carecía de mecanismos adecuados de retroalimentación. Su rigidez no le permitía adaptarse a las circunstancias

cambiantes. La forma burocrática de tratar a las personas fue representada extraordinariamente bien por Kafka en sus novelas.

La burocratización es un aspecto específico de un proceso más general, que se ha denominado "juridificación". El derecho, como la burocracia, es un instrumento que puede utilizarse para fines diversos, buenos o malos éticamente. Puede ser un medio de opresión o una fuente de garantías frente al poder. Pero, en cualquier caso, cuando el derecho irrumpe en un nuevo escenario o esfera de la vida, cambia su lógica de funcionamiento con independencia de los fines para los que se utilice.

Pensemos, por ejemplo, en un proceso de divorcio en el que los padres pleiteen por la custodia de sus hijos. El juez adoptará una decisión que determinará con quién van a vivir los niños. Pero eso no resuelve necesariamente el conflicto. Al contrario, el proceso judicial probablemente lo agravará e incrementará el enconamiento de los padres. Destrozará los mecanismos de funcionamiento propios de las relaciones familiares sustituyéndolos por planes estratégicos dirigidos a ganar el pleito. Esto lastrará el futuro de las relaciones entre la expareja y entre padres e hijos, cuyas relaciones seguirán estando colonizadas por el derecho durante muchos años.

8. La algoritmización de las relaciones personales

Cuando el capitalismo de la vigilancia y sus algoritmos invaden una esfera de la vida cambian también su lógica de funcionamiento.

Los algoritmos han colonizado nuestras relaciones personales especialmente por medio de las redes sociales: algunos de sus aspectos esenciales se han visto alterados o modificados como consecuencia de la lógica algorítmica combinada con los intereses del capitalismo de la vigilancia.

En primer lugar, los algoritmos del capitalismo de la vigilancia modifican la lógica de las relaciones personales porque reconfiguran la propia identidad de las personas. los algoritmos del capitalismo de la vigilancia crean una identidad digital para nosotros y nos inducen a que nos parezcamos cada vez más a ella. Las empresas del "capitalismo de la vigilancia" han desarrollado la capacidad de agrupar todos los rastros digitales que hemos ido dejando en Internet y de fabricar un dosier exhaustivo sobre nosotros mismos, nuestras actividades y nuestros gustos. Este proceso construye un "gemelo digital" del usuario(Rossignaud, Maria Pia & De Kerckhove, 2020), es decir, nos dota de una identidad construida heterónomamente a la que se nos incita a amoldarnos.

Esto da sentido a la reivindicación del "derecho a nuestra propia identidad" contenido en una "Declaración de derechos en el ciberespacio" elaborada por el periodista J. Jarvis que publicó en su blog y, luego en *The Guardian*. En este manifiesto dice que tenemos derecho a nuestra propia identidad y que ésta no es algo tan simple como nuestro nombre, sino que se compone también de nuestro discurso,

creaciones, acciones y conexiones. Jarvis señala que el control que tengamos sobre nuestros datos y sobre nuestras identidades conforma el derecho a la privacidad[5].

Una de las operaciones características de los algoritmos es la clasificación de personas y cosas en base a sus atributos. Las operaciones algorítmicas tienden a reforzar en nosotros los rasgos en virtud de los cuales nos han incluido en determinados conjuntos o clases. Así, si hemos sido incluidos dentro de la categoría de personas a las que les gustan los "golden retriever", recibiremos múltiples informaciones relacionadas con esa raza de perros y se nos harán sugerencias de gentes o grupos con los que podemos contactar para compartir nuestra afición. Y, desde luego, se nos enviará mucha publicidad personalizada relacionada con ello. Como dice D'Ancona en su libro sobre la posverdad: "Justamente ese es el cometido de los algoritmos: ponernos en contacto con las cosas que nos gustan, o podrían gustarnos" (D'Ancona, 2019, p. 47).

Este bombardeo es muy probable que tienda a reforzar nuestra afición y a encerrarnos en un mundo que gira en torno a esa raza canina. Puede, incluso, crear esa afición en nosotros. Muchas veces no está claro por qué un algoritmo clasifica a alguien en una determinada categoría. Esa opacidad hace que resulte muy difícil o imposible saber por qué se nos envía una determinada información o se nos hace una determinada oferta. Es posible que nosotros ni siquiera supiésemos de la existencia de los golden retriever y que el algoritmo los haya incluido entre nuestras aficiones en base a algún tipo de inferencia indirecta. Igual no hacemos caso, pero igual resulta que nos hacemos unos entusiastas admiradores de esos inteligentes animales.

En segundo lugar, los algoritmos del capitalismo de la vigilancia nos hacen perder una serie de habilidades fundamentales para las relaciones sociales.

Las empresas del capitalismo de la vigilancia persiguen que estemos conectados durante el mayor tiempo posible y que esa conexión sea activa: que interactuemos a través de la plataforma. Los algoritmos se utilizan para predecir qué mensajes o notificaciones despertarán nuestra curiosidad y nos llevarán a conectarnos y/o interactuar en las plataformas. Facebook manda constantemente mensajes acerca de las actividades de nuestros "amigos" que pueden interesarnos, para incitarnos a que nos conectemos. Y, en cuanto abrimos la página principal de la plataforma, Facebook nos pregunta qué estamos pensando ahora para que lo transmitamos mediante un mensaje en nuestro muro.

La mengua de nuestra capacidad para conversar es una de las habilidades sociales que se han visto más afectadas por la conectividad permanente según Sherry Turkle (Turkle, 2020). Turkle fue la primera psicóloga que se ocupó de la manera

5 J. Jarvis, "A Bill of Rights in Cyberspace," *@BuzzMachine*, 27 Marzo 2010, *http://bzzm.ch/I92sZv*

como cambia nuestra forma de ser cuando interactuamos con un ordenador. Se trata de una auténtica pionera pues en fecha tan temprana como 1984 escribió un libro titulado "El otro yo" (Turkle, 1984), que ahora es de obligada referencia.

La conversación es una interacción que tiene lugar cara a cara, durante la cual puede observarse el lenguaje corporal del interlocutor. Las conversaciones se llevan a cabo "en tiempo real", es decir, que nuestras reacciones han de ser respuestas prontas. No podemos actuar como jugadores de ajedrez que se toman media hora para decidir cuál va a ser su siguiente jugada.

Pero a través de las redes sociales no se conversa, sino que se chatea. A lo largo de su libro Turkle va desgranando las diferencias entre la comunicación producto de la conversación y la actividad consistente en el envío y recepción de mensajes de texto a través de las redes sociales. La interacción mediante mensajes de texto no se realiza "en tiempo real". Existe la posibilidad de tomarse un tiempo, calcular cuál es la mejor respuesta, de editar y corregir el mensaje, de decidir en qué momento enviarlo…En un mundo en que se destaca como un importante valor que las interacciones se lleven a cabo en tiempo real, resulta que muchos estudios demuestran que los jóvenes consideran que es un gran alivio poder interactuar de forma diferida.

El chateo hace que se pierdan todos los elementos comunicativos que proporciona la presencia física del otro. Se pierden todas las facetas del lenguaje corporal, la posibilidad de mirarse a los ojos, las reacciones que provoca en nosotros el aspecto o la actitud de nuestro interlocutor… Turkle no es contraria a la interacción digital. Lo que le preocupa son los efectos perturbadores que la hiperconectividad está teniendo sobre nuestra capacidad de conversar.

9. La algoritmización de la esfera pública

Aparte de colonizar las relaciones personales, los algoritmos del capitalismo de la vigilancia han irrumpido en lo que Habermas bautizó como "esfera pública" (Öffentlichkeit). Tres claras manifestaciones de las transformaciones inducidas por esta colonización son: a) la modificación del comportamiento electoral de los ciudadanos; b) el distanciamiento de "lo público" que provoca en los usuarios; c) el fomento de la polarización política.

9.1. Manipulación de la conducta electoral

Los manejos de Cambridge Analytica vienen a nuestra mente inmediatamente cuando hablamos de la manipulación de los electores utilizando datos extraídos de las redes sociales. La medida en que la empresa consiguió cambiar los resultados no está clara, pero la dimensión de su influencia puede percibirse en los "experimentos" que llevó a cabo Facebook a principios de la pasada década. Estos pusieron de manifiesto que el porcentaje de la población sobre la que realmente se influye fue pequeño, pero la cantidad bruta de personas influenciadas fue grande (Zuboff, 2019).

Uno de los experimentos se practicó sobre 61 millones de usuarios (sin que ellos lo supieran), más o menos la misma cifra de votantes que tuvo Trump en 2016. En él se trataba de determinar la capacidad de influir en el grado de participación en unas elecciones, concretamente en la votación para las presidenciales estadounidenses de 2010. Los resultados fueron publicados en 2012 en la revista *Nature* (Bond *et al.*, 2012). De acuerdo con el estudio Facebook consiguió incrementar la participación en las elecciones en 340.000 votantes. Esa cifra representa sólo un 0'5% de la "muestra", pero puede resultar determinante en votaciones en las que la opinión pública está muy dividida.

Por otro lado, no sólo hay que tener en cuenta el número total de personas influidas. Las modificaciones de la conducta electoral pueden resultar clave si se dirigen a grupos de electores específicos. Estos pueden dar un vuelco a los resultados en distritos electorales cruciales, como podría suceder en las elecciones presidenciales norteamericanas. Hay que tener en cuenta que el experimento de Facebook se realizó sin utilizar publicidad personalizada ni se orientó a grupos específicos de usuarios.

9.2. El efecto "burbuja y la polarización política

La publicidad "personalizada" es el negocio que está en la base del capitalismo de la vigilancia y su insaciable voracidad de datos. Captar nuestra atención durante el mayor tiempo posible es la estrategia de las redes sociales. Lo que le interesa a Facebook o a Google es que nos mantengamos interactuando en sus plataformas para, así, recabar el mayor número de datos acerca de nosotros.

Hubo un momento, en 2009 en que el buscador de Google dejó de ser el mismo para todos y se convirtió en una miríada de herramientas adaptadas a los gustos e intereses de cada usuario. Las búsquedas dejaron de estar reguladas por criterios de relevancia objetiva y se pasó a posicionar los resultados en base a lo que los algoritmos consideraban que cada usuario preferiría. Distintas personas obtendrían resultados diferentes, aunque realizasen una consulta idéntica. Fue el inicio de la "personalización"(Pariser, 2011, pp. 5 ss.).

En el caso de Facebook la personalización consiste en que nos presenta primero los posts o los links compartidos que el algoritmo cree que se ajustarán más a nuestros gustos y creencias y que, por tanto, despertarán más nuestro interés. Los otros quedarán relegados al fondo de la lista, por lo que es muy probable que no lleguemos nunca a verlos si tenemos 100 o 200 amigos en esa red social.

La personalización de la información que recibimos produce un efecto burbuja. Es como si nos encontrásemos dentro de una esfera cuyo interior fuera un espejo de modo que únicamente viésemos nuestro propio reflejo.

Internet no ha supuesto una desintermediación de la información, como a veces se afirma. Lo que ha ocurrido es que los intermediarios han cambiado. Antes, las

noticias que nos llegaban venían determinadas por editores profesionales de grandes medios. Los nuevos "editores" son muchas veces invisibles y, entre ellos, los algoritmos del capitalismo de la vigilancia tienen una influencia extraordinaria en la determinación de la información que se nos va a ofrecer.

Actualmente un gran porcentaje de la población se informa principal o exclusivamente por medio de las redes sociales. En el año 2018 el porcentaje de la población estadounidense que se informaba a través de las redes superó al de los lectores de periódicos. Este hecho confiere una enorme trascendencia a los mecanismos de personalización que se utilizan para escoger la información que se ofrece a los usuarios y a los algoritmos que se utilizan para la selección.

El efecto burbuja y sus consecuencias fueron analizados exhaustivamente por primera vez en un libro que constituye hoy en día una referencia obligada: *El filtro burbuja: cómo la web decide lo que leemos y lo que pensamos* escrito por, Eli Pariser y publicado originariamente en inglés el año 2011 (Pariser, 2011) y traducido al castellano en 2017 (Pariser, 2017).

Estas son algunas de sus conclusiones:

1) La burbuja-filtro fomenta la rigidez y el dogmatismo tanto en la esfera pública, como en los demás ámbitos de nuestra existencia.

Las opiniones que se nos presentan son afines a las nuestras y los hechos de los que se nos informa tienden a reafirmar nuestras creencias. La burbuja-filtro refuerza nuestra tendencia (¿natural?) a no replantearnos nuestros presupuestos, esquemas de percepción o sistemas conceptuales, es decir, las "casillas" por medio de las cuales asimilamos nuevas informaciones. También puede disminuir o anular la conciencia de estar utilizando una rejilla de ese tipo cuando percibimos o analizamos la realidad. Consolida nuestros pre-juicios y disminuye o anula la conciencia de que los tenemos.

2) La burbuja nos distancia de "lo público" pues da preeminencia a aquello que nos gusta, nos entretiene o nos afecta directamente y nos aleja de los problemas sociales importantes o los invisibiliza.

3) El filtro disminuye cualitativamente nuestro "capital social", es decir, las relaciones con personas externas a los grupos de que formamos parte. Esta menor variedad debilita nuestra capacidad de preocuparnos por intereses distintos de los nuestros o de los miembros de nuestros grupos. Y la capacidad de preocuparse de los intereses ajenos es la base de la virtud cívica que nos lleva a participar en lo público.

4) Tener una base de hechos común y conocer las opiniones de los otros son requisitos mínimos para que sea posible cualquier tipo de diálogo. Sin embargo, al limitar nuestras posibilidades de conocer y tomar en consideración opiniones e informaciones el filtro inserta a los usuarios en diferentes "realidades paralelas".

Los algoritmos combinan la personalización con otro criterio o filtro: la popularidad o volumen de tráfico en Internet de la información o tema, privilegiando los que tienen "tendencias virales". El plus que se otorga a las informaciones con potencial de viralidad da como resultado que se prioricen cosas que atraen nuestra atención a primera vista, que son estadísticamente muy vulgares, escandalosas o inverosímiles. Los temas importantes, pero complejos quedan relegados, aunque entren dentro de la gama de los intereses del usuario.

El maridaje entre personalización y viralidad fomenta la polarización política de la población. La polarización consiste en dividir a la población en dos bandos contrapuestos intolerantes el uno con el otro. Genera una dinámica amigo/enemigo: si no estás conmigo, estás contra mí. Esa dinámica hace que el diálogo resulte imposible y que no se puedan mantener posturas neutrales o ponderadas sin recibir ataques de un lado, del otro, o de ambos.

El plus de viralidad de la burbuja-filtro favorece la difusión de los contenidos más extremistas, provocadores o insultantes en el debate político que se lleva a cabo en la red. La razón de esto es que los contenidos que provocan reacciones emocionales más intensas, como rabia, ansiedad o entusiasmo son los más vistos y los que más se comparten. La burbuja filtro traslada el debate político al mundo de las emociones.

Las revelaciones de Frances Haugen y los documentos que las avalan han puesto claramente de manifiesto que Facebook fomenta la polarización de manera culposa (por negligencia) e, incluso, dolosa (intencionalmente). La política de inversiones de la compañía va dirigida sobre todo a contratar más programadores o perfeccionar los mecanismos maximizadores de beneficios. Se deja de lado la formación de moderadores o supervisores de contenido o la mejora del funcionamiento de los mecanismos automatizados de control de contenidos. Esto produce efectos especialmente perniciosos en países pobres con lenguas minoritarias. Pero Facebook no sólo fomenta la polarización por negligencia, sino también de forma activa al privilegiar los contenidos altamente emotivos. Persigue, con ello, atraer la atención de los usuarios, mantenerlos más tiempo conectados y multiplicar sus interacciones. Según Haugen, existen también algunos millones de usuarios VIP a los que Facebook no aplica controles de contenido por lo que pueden difundir cualquier tipo de opiniones o informaciones a través de la red.

Los efectos polarizadores de las burbujas-filtro de las redes sociales influyen a su vez en la dinámica de los demás medios de comunicación. La obsesión por el tráfico en Internet ha llevado a muchos medios digitales a utilizar la popularidad (o potencial de viralidad) como criterio determinante a la hora de decidir qué contenidos ofrecen y cuáles no. Los medios de comunicación rigurosos pueden verse arrastrados hacia el sensacionalismo y amplificar, con ello, la polarización.

En un libro recientemente publicado, Chris Bail defiende la tesis de que las redes sociales crean la apariencia de una "falsa" polarización porque presentan las opiniones de los "otros" (republicanos o demócratas en su caso) como mucho más radicales y contrapuestas de lo que son realmente. Esta "falsa polarización" es provocada por el hecho de que los extremistas son los más activos participantes en la discusión política de las redes. Aunque constituyen una porción pequeña del total de usuarios, son los que generan el porcentaje mayor de mensajes políticos. La radicalización de la discusión hace huir a los moderados de este tipo de debates (Bail, 2021).

Los planteamientos de Bail resultan muy discutibles por diversos motivos.

La evidencia empírica en que se basan las tesis del libro es absolutamente insuficiente. En última instancia, las conclusiones se fundamentan en entrevistas en profundidad hechas a cuarenta norteamericanos durante la primera mitad del mandato de Trump. De una muestra tan pequeña en un periodo tan convulso resulta difícil pensar que pueda extraerse algún tipo de conclusión general sobre el efecto de las redes sociales en la polarización política.

El autor comete graves errores a la hora de analizar cómo se crea nuestra identidad digital en Internet. Considera que esa identidad es el resultado de nuestra interacción con otros a través de las plataformas. Cree que nuestra identidad digital se basa exclusivamente en la información que transmitimos de modo voluntario a través de las redes. Así, por ejemplo, dice: "Nadie que lea mis tweets puede saber qué estoy viendo en Netflix" (Bail, 2021, p. 106).

Bail habla de Twitter porque es la plataforma que utilizó para su investigación, pero en el libro extrapola sus conclusiones a todas las redes sociales. Parece ignorar que las empresas del capitalismo de la vigilancia obtienen muchos datos nuestros sin que lo sepamos, sean éstos fruto de nuestra interacción con la plataforma (p. ej. qué navegador o qué modelo de ordenador estamos usando), o provenientes de otras fuentes. Tampoco toma en consideración que las plataformas fabrican unos "gemelos digitales" que conforman nuestra identidad digital.

Como ya se ha dicho, Bail basa sus conclusiones en una serie de historias personales recogidas por medio de entrevistas en profundidad. En su libro utiliza constantemente episodios de esas vivencias para reforzar la fuerza de convicción de sus argumentos. Resulta legítimo, pues, contar anécdotas personales para criticarle.

Una anécdota especialmente ilustrativa la cuenta Pariser en su libro sobre el efecto burbuja.

Resulta que un buen día sus amigos conservadores desaparecieron de su cuenta de Facebook. No es que hubieran decidido dejar de seguirle en masa, sino que la plataforma relegó sus posts al fondo de la lista hasta el punto de hacerlos prácticamente invisibles. Los algoritmos habían clasificado al autor como una persona progresista. Consideraron que no le interesarían las opiniones de personas

conservadoras. La invisibilidad de estos mensajes no tenía nada que ver con el mayor activismo de los usuarios radicales, ni con la huida de los moderados provocada por el radicalismo de las posturas que se adoptaban (Pariser, 2011, p. 8). Este episodio contradice frontalmente las conclusiones de Bail.

Parte 3: Hacia una ciudadanía digital

Hemos analizado los problemas ético-políticos que plantea el uso de los algoritmos en el mundo del capitalismo de la vigilancia. También hemos visto los efectos estructurales que la algoritmización tiene tanto en la esfera privada como en la pública. Se ha señalado repetidamente que la materia prima de las empresas del capitalismo de la vigilancia son los datos sobre las características y la actividad de las personas y que se han desarrollado numerosos mecanismos para obtenerlos con el consentimiento de éstas o sin él. De ello se infiere que la garantía efectiva del derecho a la privacidad es algo que se contrapone frontalmente a los intereses de esas empresas.

La resignación frente al uso que hacen las plataformas de sus capacidades de monitorización de las conductas es una actitud bastante frecuente entre los usuarios. Se han publicado estudios que hablan de la llamada "paradoja de la privacidad": esta expresión se refiere al fenómeno de que las personas, cuando se les pregunta, dicen valorar mucho su privacidad, pero en su comportamiento práctico ceden sus datos personales a cambio de muy poco o no adoptan medidas para proteger su intimidad digital[6]. Un autor llamado Firmin DeBrabander llega a afirmar, en un libro titulado "La vida después de la privacidad", que el principal peligro que amenaza a la intimidad son los propios ciudadanos por aceptar que les controlen a cambio de disfrutar de las nuevas tecnologías (DeBrabander, 2020).

Ese tipo de afirmaciones confunden el efecto con la causa. Con independencia de lo extendida que esté la actitud de resignación, el conformismo no es la causa del problema. Es la indefensión jurídica de los usuarios lo que provoca la resignación y no la resignación la que causa la indefensión. Por otro lado, este tipo de afirmaciones no tienen en cuenta el intenso activismo actual en defensa de los derechos "digitales". Se han llevado y se están llevando a cabo multitud de acciones de resistencia. Existen muchas formas de acción directa digital y también campañas de movilización y concienciación emprendidas por organizaciones activistas.

[6] Aunque las inconsistencias entre lo que dicen los usuarios y lo que hacen en la práctica ya habían sido documentadas previamente, la expresión "paradoja de la privacidad" fue utilizada por primera vez en un artículo publicado en 2007 (Norberg, Horne and Horne, 2007). Hay también autores que han sostenido que la paradoja de la privacidad es solamente un "mito" (Solove, 2021).

10. La indefensión jurídica de los usuarios

El negocio de la recopilación y procesamiento de datos surge en el contexto de la globalización neoliberal. La filosofía del neoliberalismo considera que el mercado es el mecanismo más eficiente de distribución de los recursos y que la regulación debe dejarse a sus "leyes" y a sus instrumentos jurídicos idiosincrásicos, que son la propiedad privada y el contrato. El neoliberalismo también promueve la privatización. Bienes y servicios que antes eran considerados "fuera del comercio" se convierten en mercancías, En este contexto marcado por la privatización y mercantilización, los datos digitalizados se convierten en mercancías y fuente de beneficios.

En el capitalismo de la vigilancia, las obligaciones y los derechos de las empresas y sus usuarios se establecen fundamentalmente mediante contratos privados. La protección de los datos personales, por ejemplo, se hace depender del consentimiento informado, en base a un sistema denominado "notice and consent" (información y aceptación). La empresa tiene el deber de informar al usuario acerca de los datos que va a recoger, a quién se los va a ceder, cómo se van a procesar… y el cliente puede decidir aceptarlos o no "libremente".

Para el liberalismo y las leyes civiles el consentimiento es libre siempre que no haya habido violencia, amenaza o engaño. Pero esa visión contractual no tiene en cuenta otras formas de interferencia en la libertad como puede ser la existencia de una relación de dominación entre las partes.

El mecanismo de *notice and consent* es una forma de regulación inadecuada, debido a las asimetrías de poder entre los usuarios de servicios digitales y las empresas. Los particulares no pueden negociar las cláusulas de los contratos, sino que su única opción es "o lo tomas o lo dejas". Si alguien pretendiera conocer con exactitud todas las "políticas de privacidad" de las aplicaciones que instala o las páginas que utiliza, necesitaría algo así como dedicar a esa tarea cuatro meses al año a jornada completa. Las empresas proporcionan la información, pero ésta resulta inabarcable y en buena medida incomprensible para los usuarios.

Por ello, debería crearse una regulación estatal fuerte que compense esa desigualdad (como ocurre –u ocurría– en el caso del derecho laboral) imponiendo coercitivamente limitaciones a las compañías que recolectan datos personales y que no puedan ser modificadas ni siquiera con el consentimiento de los usuarios.

El Reglamento general de protección de datos de la Unión Europea ha supuesto un avance en la regulación que ha servido de punto de referencia para los activistas estadounidenses. Pero hay que tener en cuenta sus limitaciones, derivadas de que el objetivo principal de esta norma es facilitar el intercambio de datos entre las empresas de los diversos países de la UE, homogeneizando la normativa en toda la Unión y no la preservación de la privacidad de los usuarios (v. Gonzalo Suárez, 2019).

11. Actos de ciudadanía en el mundo digital

La ciudadanía no se concibe aquí únicamente como un estatus, sino también una actividad. Esta dimensión activa incluye los que Isin denomina "actos de ciudadanía". Los actos de ciudadanía son acciones de reivindicación de derechos que no han sido efectivamente reconocidos y los pueden llevar a cabo tanto las personas que tienen el estatus de ciudadanos como las que carecen de él.

Como se ha señalado, la tesis que considera la resignación como el principal peligro para la privacidad no tiene en cuenta la gran cantidad de acciones de resistencia contra su violación que se llevan a cabo en Internet y desconoce que hay multitud de organizaciones que actúan en defensa de los derechos digitales de las personas.

En la actualidad se están desarrollando multitud de campañas de movilización y concienciación emprendidas por organizaciones activistas para conseguir que usuarios y ciudadanos en general dejen de estar desprotegidos frente a las empresas del capitalismo de la vigilancia. También se llevan a cabo diversas formas de acción directa que se utilizan como mecanismos de autodefensa.

Las diferentes formas como las personas se defienden de las intrusiones del capitalismo de la vigilancia pueden ser agrupadas en tres categorías: ocultación, ofuscación y filtración.

11.1. Ocultación

La expansión de la vigilancia intrusiva y su ubicuidad han dado lugar a muchas formas de acción directa dirigidas a impedir o dificultar la vigilancia ocultándose del vigilante o confundiéndolo.

La forma más antigua de acción directa consistió en el uso de la criptografía para "hacerse invisible" en Internet y es una de las estrategias preferidas del "hacktivism" o activismo hacker. Los hackers han sido y son, fundamentalmente, programadores: se dedican a escribir códigos. Se suele distinguir a los hackers de sombrero negro (*black hat*) de los de sombrero blanco (*white hat*). Los hacktivistas se incluyen en la segunda categoría y se caracterizan porque sus acciones tienen una motivación política o social. En un libro reciente de Maureen Webb, titulado "Coding Democracy: How Hackers are Disrupting Power, Surveillance, and Authoritarianism" [Codificar la democracia: cómo los hackers están trastocando el poder, la vigilancia y el autoritarismo] (Webb, 2020) se puede encontrar abundante información sobre la historia del hacktivismo.

El movimiento fue impulsado por una serie de personas que previeron muy tempranamente que Internet se iba a convertir en un sistema de vigilancia total (Bartlett, 2017). La opción por la acción directa queda claramente puesta de manifiesto en la siguiente cita:

> Por una fracción de la inversión de tiempo, dinero y esfuerzo que me tomaría tratar de convencer al estado de que abrogue el espionaje y todas las formas de censura, puedo enseñarle a cada libertario que esté interesado en cómo usar la criptografía para abrogarlo unilateralmente[7].

Los primeros hackers pretendían restaurar el anonimato originario de Internet. Desarrollaron, entre otros instrumentos el sistema de cifrado de doble llave. Con él quienes envían un mensaje encriptado usan una clave puesta a disposición de los usuarios por el destinatario (llave pública). Éste descifra los mensajes por medio de una clave que solo él conoce (llave privada). No se produce, por tanto, ningún envío de claves que sirvan para descifrar el mensaje y que pueda ser interceptado. El mensaje se puede encriptar con la llave pública, pero sólo puede descifrarse mediante la clave privada. Ni siquiera quienes envían los mensajes podrían desencriptarlos.

Los hackers han participado también en el "proyecto Tor", que desarrolló un navegador que permite circular de manera anónima por la red. Tanto el navegador como el sistema de cifrado de doble llave siguen utilizándose profusamente en la actualidad.

11.2. Ofuscación

Otro conjunto de formas de acción directa son las llamadas tácticas de "ofuscación". El objetivo de la ofuscación es confundir al que vigila cuando uno no puede ocultarse de él. Consiste en usar señuelos para que no pueda distinguir lo que es verdad de lo que no. Se trata de tácticas análogas a las que utilizan los jets para burlar a los misiles que les rastrean: los pilotos lanzan un montón de "señuelos" cuyo objetivo es confundir al misil dificultando la identificación del avión y su trayectoria (Brunton and Nissenbaum, 2015).

Hay modos de ofuscación que afectan a la geolocalización que se realiza por medio del móvil o de las aplicaciones que activan su GPS. La geolocalización permite determinar dónde está el usuario y registrar sus itinerarios (algo que hacen aplicaciones como Google Maps). El software que se ha diseñado para confundir al rastreador envía información sobre varias trayectorias simultáneamente, sin especificar qué camino se está siguiendo realmente. Al usuario le sigue siendo útil una aplicación como Google Maps, porque sabe dónde está y a dónde se dirige, pero la compañía no puede detectar su posición ni su trayecto.

Otro tipo de ofuscación se aplica a las búsquedas realizadas por motores como el de Google. El mecanismo para confundir al buscador consiste en hacer una lista de cosas en las que el usuario no está interesado y utilizar un software que se encarga

[7] La cita ha sido extraída de una conferencia pronunciada en 1987 por el matemático Chuck Hamill (Hammill, 1987), El texto de la conferencia ha sido consultado en https://nakamotoinstitute.org/static/docs/from-crossbows-to-cryptography.pdf

automáticamente de hacer búsquedas sobre esos temas. Con ello, se distorsiona la información que se utiliza para perfilar al usuario.

11.3. Filtraciones

En su libro sobre el hacktivismo, Webb menciona un documento que considera como un manifiesto hacker del siglo XXI. Dice lo siguiente:

> El manifiesto 'Privacidad para los débiles, transparencia para los poderosos' es ahora omnipresente en los círculos de hackers. Es breve (…) como debe ser un manifiesto para el siglo XXI. No he podido descubrir quién es el autor. Parece haber surgido del colectivo sin líder (Webb, 2020, p. 68).

El lema "privacidad para los débiles, transparencia para los poderosos" es utilizado profusamente en un libro publicado por Assange en 2012, titulado "Cypherpunks: la libertad y el futuro de Internet" (Assange *et al.*, 2012), que contiene, incluso, un capítulo dedicado a esa especie de principio de la ética hacker.

Assange cumplió el segundo mandato del principio –que exige transparencia para los poderosos–, por medio de WikiLeaks, una plataforma que creó y dirigió. WikiLeaks incitaba a filtrar documentos secretos garantizando el anonimato de quienes lo hacían y ofrecía una plataforma para su difusión. El desvelamiento de secretos es una forma de denunciar lo que ocurre tras las bambalinas del poder, pero también es una manera de presionar, a los gobiernos y a las empresas, para disuadirles de realizar acciones secretas de carácter ilegal o inmoral. Es una especie de advertencia de que todos los trapos sucios serán sacados a la luz, pues se cuenta con los medios necesarios para hacerlo.

WikiLeaks ha difundido toneladas de documentos "confidenciales" desde su fundación en 2006. El último *leak* se produjo en noviembre de 2019 y en él se destapaban las prácticas de corrupción de una multinacional pesquera que tiene su sede en Islandia: Samherji.

El siguiente gran hito de la historia reciente de las filtraciones tuvo lugar en 2013 con las revelaciones de Snowden, que no utilizó la plataforma de Assange porque no quería difundir documentos "en bruto", sino ofrecer una información ordenada y sistematizada. Ésta fue publicada en los periódicos *The Guardian y The Washington Post* para lo que Snowden contó con la inestimable ayuda del periodista Glenn Greenwald. El libro en el que el redactor cuenta las peripecias de la filtración es tan apasionante como un thriller (Greenwald, 2014). Las revelaciones de Snowden pormenorizaban las prácticas de vigilancia ilegal por parte de la NSA que, entre otras cosas, almacenaba y procesaba millones de "metadatos"[8] referentes a las

[8] El "dato" en este caso es el contenido de la conversación telefónica; los datos sobre ese dato o metadatos son informaciones acerca del momento y duración de la llamada, los interlocutores que participaron en la misma o el lugar desde donde se hizo y en el que se recibió.

llamadas de móvil que realizaban los norteamericanos y que la compañía Verizón fue obligada a proporcionarles (Greenwald, 2013). Esas filtraciones se acomodan perfectamente a la exigencia de obligar a los poderosos a que sean transparentes.

Con posterioridad se desvelaron los manejos de Cambridge Analytica (CA) en la campaña del Brexit y en las elecciones que llevaron a Trump a la presidencia en 2016. Esta empresa manipuló a los votantes mediante el uso de estrategias personalizadas en las que utilizaban datos de los votantes obtenidos a través de las redes sociales. Christopher Wylie, exdirector de investigación de Cambridge Analytica (CA), se convirtió en un informante en 2018 y proporcionó documentos al periódico *The Guardian* sobre la explotación de la información facilitada por Facebook a su empresa. Los entresijos de la "segunda" campaña a favor del "leave" (salida de la UE), organizada por Dominic Cummings, son puestos al descubierto en un documental dramatizado titulado *Brexit: The Uncivil War*, dirigido por Toby Haynes en 2019.

Más recientemente, las filtraciones de Frances Haugen han desvelado la responsabilidad de Facebook en la difusión de mensajes extremistas que fomentan la polarización de la población. Sus revelaciones han provocado la mayor crisis en la historia de la compañía.

11.4. Organizaciones y campañas de defensa de los derechos digitales

Aparte de las diferentes formas de acción directa, existen multitud de organizaciones que luchan por los derechos digitales mediante campañas de información, estudios de investigación, denuncias, pleitos judiciales, litigios estratégicos[9] o participando en el diseño de las políticas de protección de datos (advocacy). Una de estas organizaciones se llama *Electronic Privacy Information Center* (EPIC). Fue fundada en el año 1994 y forma parte de esa primera hornada de activistas que se dieron cuenta de que Internet podía convertirse en un mecanismo de vigilancia. Realiza actividades de investigación, difusión, litigación y *advocacy*. En su página web *https://epic.org/* puede obtenerse información acerca de las campañas que está llevando a cabo actualmente y los temas de los que se ocupa.

Privacy International (https://privacyinternational.org/) tiene un lenguaje más radical que EPIC. Una de sus campañas más importantes se desató durante el desarrollo del *Street View* de Google, que ahora podemos usar mediante *Google Maps* y que nos permite ver imágenes de la calle o del portal que estamos buscando. Estas fotografías se realizaban desde un vehículo equipado con una cámara que filmaba los edificios y la propia calle. Esta actividad generó rechazo en personas que se preguntaban por qué podían difundirse imágenes de las viviendas sin el consentimiento

[9] Los litigios estratégicos se entablan no solamente para ganar un caso objeto, sino también para establecer un precedente.

de sus dueños, o por qué se mostraban sus rostros (lo segundo se solucionó mediante la pixelación de las caras). Pero lo más grave es que Google recopilaba información de las redes wifi de los domicilios por donde pasaba el vehículo. La compañía "hackeaba", contraseñas, mensajes y todo lo que cayera en sus manos.

La Electronic Frontier Foundation (https://www.eff.org/es) es una de las organizaciones señeras en este campo y surge directamente del movimiento de los hackers. Uno de los temas de los que se ha ocupado son los peligros que la vigilancia pandémica ha supuesto y supone para la protección de los datos personales. Estos riesgos tienen que ver especialmente con los mecanismos que se utilizan para rastrear los movimientos y contactos de la población.

Estas tres organizaciones son únicamente tres ejemplos de la miríada de entidades que están luchando actualmente en defensa de la privacidad.

12. Convertirse en ciudadanos digitales

Comparto la opinión de Engin Isin y Evelyn Ruppert quienes consideran que todas estas acciones y campañas son actos de ciudadanía que contribuyen a dar nacimiento a una ciudadanía digital que aún no es efectiva. Los autores señalan que la investigación que llevan a cabo en su libro "Being digital citizens" –que se podría traducir como "Convertirse en ciudadanos digitales– (Isin and Ruppert, 2020) estudia "(...) los actos de las personas que exigen derechos digitales y de datos y que resisten y subvierten las desposesiones y apropiaciones de los estados y las corporaciones"(Isin and Ruppert, 2020, p. ix) y consideran que "Lo que los ciudadanos emergentes están haciendo realidad al promulgar sus derechos atravesando las fronteras estatales y nacionales es precisamente la figura de un ciudadano digital que está por venir"(Isin and Ruppert, 2020, p. 167).

Los debates acerca de la protección de datos, los usos de la inteligencia artificial, el poder y la práctica de las empresas del capitalismo de la vigilancia o la mejor forma de regular su actividad están ya muy presentes en la esfera pública. Pero las propuestas y discusiones de quienes se ocupan de la regulación algorítmica (ética o jurídica) desde el ámbito académico o institucional son, a veces, poco inteligentes. Cuando tratan de temas como los sesgos o la opacidad de los algoritmos, esos debates no suelen tener en cuenta las características de los algoritmos capaces de aprender y decidir por sí mismos. El único problema que se suele discutir respecto de éstos es el de quién tiene la responsabilidad ética y jurídica en el caso de que un dispositivo dotado de capacidad de decisión autónoma cause daños debido a un error.

Como hemos señalado más arriba, el desarrollo tecnológico está fuertemente determinado por decisiones económicas y políticas. Lo hemos visto ejemplificado en el caso del proceso de desanonimización de Internet. Esto hace necesario desvelar y revelar las decisiones políticas y económicas que se ocultan tras el progreso

tecnológico, cuando éste se es presentado como un proceso regido únicamente por la lógica de la investigación científica y el saber de los expertos.

Los ciudadanos deben poder participar en las decisiones que determinan el desarrollo tecnológico. Pero el conocimiento que la mayoría de las personas tiene sobre el mundo digital es ínfimo en comparación con lo que saben del mundo físico o material. Una "educación para la ciudadanía digital" debería realizar una tarea de alfabetización que permita tener un conocimiento básico de las características y funcionamiento del mundo digital. Este texto ha pretendido ser una pequeña contribución a esa tarea.

Bibliografía

Amoore, L. (2020) *Cloud ethics*. Duke University Press.

Assange, J. *et al.* (2012) *Cypherpunks: Freedom and the Future of the Internet*. OR books New York.

Bail, C. (2021) *Breaking the Social Media Prism*. Princeton University Press.

Bartlett, J. (2017) *La red oculta*. Paidos México.

Bond, R. M. *et al.* (2012) 'A 61-million-person experiment in social influence and political mobilization', *Nature*, 489(7415), pp. 295–298. doi: 10.1038/nature11421.

Brunton, F. and Nissenbaum, H. (2015) *Obfuscation: A user's guide for privacy and protest*. Mit Press.

Capella, J.-R. (2008) *Fruta Prohibida. Una aproximación histórico-teorética al estudio del derecho y del estado*. 5ª. Madrid: Trotta.

D'Ancona, M. (2019) *Posverdad: La nueva guerra en torno a la verdad y cómo contraatacar*. Alianza Editorial (El Libro De Bolsillo - Ciencias Sociales). Available at: https://books.google.es/books?id=oVu-DwAAQBAJ.

DeBrabander, F. (2020) *Life After Privacy: Reclaiming Democracy in a Surveillance Society*. Cambridge University Press.

Greenwald, G. (2014) *Snowden. Sin un lugar donde esconderse*. B de Books.

Greenwald, G. (no date) *NSA collecting phone records of millions of Verizon customers daily*, *The Guardian*. Available at: http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

Hammill, C. (1987) 'From Crossbows to Cryptography: Techno-Thwarting the State', in *Given at the Future of Freedom Conference*.

Hao, K. (2020) 'Human rights activists want to use AI to help prove war crimes in court', *MIT Technology Review*. Available at: https://www.technologyreview.com/2020/06/25/1004466/ai-could-help-human-rights-activists-prove-war-crimes/.

Hayes, B. (2012) 'The surveillance-industrial complex', in *Routledge handbook of surveillance studies*. Routledge London, New-York, pp. 167–175.

Isin, E. F. and Ruppert, E. S. (2020) *Being digital citizens*. Rowman & Littlefield Publishers.

Lessig, L. (2009) *El Código 2.0*. Madrid: Traficantes de Sueños, 2009. Available at: https://libros.metabiblioteca.org/handle/001/145.

Maqueda Abreu, M. L. (2021) 'Los "ismos" de la globalización penal', in Estevez Araujo, J. A. (ed.) *El derecho ya no es lo que era: las transformaciones jurídicas en la globalización neoliberal*. Madrid: Trotta, pp. 305–334.

Negroponte, N. (1995) *Being Digital*. New York: Alfred A. Knopf, Inc.,.

Norberg, P. A., Horne, D. R. and Horne, D. A. (2007) 'The privacy paradox: Personal information disclosure intentions versus behaviors', *Journal of consumer affairs*, 41(1), pp. 100–126.

Pariser, E. (2011) *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin.

Pariser, E. (2017) *El filtro burbuja: Cómo la web decide lo que leemos y lo que pensamos*. Barcelona: Taurus.

Rossignaud, Maria Pia & De Kerckhove, D. (2020) *Oltre Orwell. Il gemello digitale*. Castelvecchi.

Solove, D. J. (2021) 'The myth of the privacy paradox', *Geo. Wash. L. Rev.*, 89, pp. 1–42.

Turkle, S. (1984) 'The second self: computers and the human spirit'. Simon \& Schuster, Inc.

Turkle, S. (2020) *En defensa de la conversación: el poder de la conversación en la era digital*. Ático de los Libros.

Webb, M. (2020) *Coding Democracy: How Hackers are Disrupting Power, Surveillance, and Authoritarianism*. MIT Press.

Zuboff, S. (2019) *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile books.