A DES/PROPÓSITO DE

Teknokultura. Revista de Cultura Digital y Movimientos Sociales
ISSNe: 1549-2230

http://dx.doi.org/10.5209/tekn.66844

EDICIONES COMPLUTENSE

Hacia una privacidad colectiva: repensar las bases teóricas de la distinción público/privado en la economía de la vigilancia

Carlos Fernández Barbudo[1]

Recibido: 5 de diciembre 2019 / Aceptado: 30 de diciembre 2019 Open peer reviews

Resumen. La defensa de la privacidad se ha basado, históricamente, en la protección de la autonomía y dignidad de los individuos. Sin embargo, el reciente desarrollo de la economía de la vigilancia ha hecho que se multipliquen los tipos de tecnologías de seguimiento y los objetivos de observación disponibles. Esta situación está revelando los límites de los mecanismos políticos, jurídicos y sociales con los que las sociedades de raigambre liberal protegían la privacidad; y nos obliga a repensar las amenazas que se vierten sobre la privacidad desde una nueva perspectiva. A tal fin se defenderá que es necesario desarrollar una dimensión colectiva sobre la privacidad, que no esté centrada únicamente en los individuos, como mecanismo para comprender e interrelacionar el conjunto de cambios sociotécnicos que amenazan la dignidad, autonomía política y soberanía digital de los grupos humanos.
Palabras clave: Big Data; datificación; economía de los datos; espacio público; historia conceptual; política de los datos.

[en] Towards a collective privacy: rethinking the theoretical basis of public/private distinction in the surveillance economy

Abstract. The defense of privacy has historically been based on the protection of the autonomy and dignity of individuals. However, the recent development of the surveillance economy has multiplied the types of monitoring technologies and observation targets available. This situation shows the limits of the political, legal and social mechanisms of the liberal societies to protect the privacy, and forces us to rethink these threats from a new perspective. To this end, the aim of this paper is to defend the necessity to develop a collective dimension of privacy, not only focused on individuals, as a mechanism to understand and interrelate the set of socio-technical changes that threaten the dignity, political autonomy and digital sovereignty of human groups.
Keywords: Big Data; conceptual history; data economy; datafication; data politics; public space.

Cómo citar: Fernández Barbudo, C. (2020). Hacia una privacidad colectiva: repensar las bases teóricas de la distinción público/privado en la economía de la vigilancia. *Teknokultura. Revista de Cultura Digital y Movimientos Sociales, 17*(1), 69-76.

1. Introducción

Plantear la necesidad, o simplemente la posibilidad, de desarrollar una mirada colectiva sobre la privacidad podría parecer, y con razón, algo intuitivamente contradictorio cuanto menos. El término privacidad, etimológicamente, hace referencia a un ámbito del individuo que se considera privado y que, por tanto, está en oposición al ámbito de la publicidad, que es donde se desarrollan los asuntos colectivos y, por consiguiente, públicos. De ahí que la expresión privacidad colectiva pueda parecer un oxímoron a simple vista, sin embargo, el objetivo de este texto es defender que esta contradicción es tan sólo aparente y que un estudio en profundidad del concepto de privacidad nos debe llevar a reconocer la existencia de una dimensión colectiva de la misma.

El punto de partida para sostener esta posición radica en que los conceptos sociopolíticos no son estancos o estáticos, al contrario, están abiertos al mundo humano y cambian a lo largo del tiempo en función de múltiples factores (Koselleck, 2004). De este modo, el concepto de privacidad ha experimentado una transformación estructural por acción y efecto de las tecnologías de la información, especialmente por la aparición de las redes de datos y su penetración en todos los ámbitos de la vida social gracias a la multiplicación de los artefactos digitales (véase Fernández Barbudo, 2019). De esta transformación estructural da buena cuenta la amplia bibliografía que se ha de-

[1] Universidad Autónoma de Madrid (España)
E-Mail: cfbarbudo@protonmail.com

sarrollado en las últimas décadas sobre este concepto y que, desde muy diversas disciplinas, pretende comprender qué está cambiando en el mundo para exista una sensación generalizada de que "la privacidad ha muerto" y cómo debería actuarse sobre los desarrollos tecnológicos para que esta situación se revierta.

El caos de la privacidad (Inness, 1992) sería, desde esta perspectiva, la constatación de que el mundo sociotécnico está cambiando y con él los medios intelectuales para comprenderlo y darle sentido. Así, los nuevos miedos, pero también esperanzas, que se experimentan fruto de este cambio nos obligan a mirar cómo son los nuevos fenómenos sociotécnicos que están siendo recogidos bajo el nuevo concepto de privacidad. Sólo de este modo lo que nos parece un oxímoron se podrá revelar como una dimensión más de la vida, un ámbito que precisamente nos cuesta nombrar por las herencias intelectuales con las que aún seguimos intentando comprender un mundo que ya no es como antes.

A tal fin, habrá que comenzar por (1) aclarar cuáles son las herramientas conceptuales que hemos heredado para dar sentido a estos fenómenos, ya que sin esta labor nos resultará más complejo entender cuáles son sus limitaciones. A continuación estaremos en condiciones de (2) mirar a los fenómenos sociotécnicos que han hecho emerger un nuevo ámbito social, el de la economía de la vigilancia, que nos plantea retos diferentes para poder seguir dando sentido a la privacidad tanto en el mundo digital como en lo que podríamos considerar (falsamente) que está fuera de él. Y así, una vez que sepamos cuáles son las cargas del pasado y cómo son las nuevas realidades que se nos escapan, nos será más sencillo (3) establecer las bases para mirar hacia esa dimensión colectiva de la privacidad. Una dimensión que, por la falta de capacidad para nombrarla, actualmente nos aparece contradictoria y parece oculta.

Una advertencia. El objetivo de este texto no es desvelar algo que esté oculto, al contrario, los fenómenos que aquí aparecerán son bien conocidos entre los especialistas y están suficientemente documentados en la literatura de distintas disciplinas. El objetivo es establecer las bases para una mirada que sepa poner en relación el pasado con el presente y que permita, así, poner en relación problemas que están mucho más relacionados entre sí de lo que intuitivamente podrían parecer. De este modo, las conclusiones tampoco serán tales, porque no se busca desarrollar una propuesta cerrada, sino establecer las bases teóricas que permitan un desarrollo ulterior.

2. El individuo en las raíces de la privacidad

Bajo la palabra "privacidad" se han discutido históricamente cuestiones radicalmente diferentes entre sí pero que, a pesar de las distintas concepciones en juego, comparten un parecido de familia que es el que ha permitido ir labrando una reflexión, con un cierto grado de continuidad, sobre su significado. De este modo, podemos encontrar reflexiones que abarcan desde el carácter prepolítico de relaciones familiares en el mundo premoderno, por estar orientadas a la satisfacción de las necesidades materiales de existencia (Brunner, 1977 [1968]); pasando por otras que se refieren al grado de autonomía del que pueden disfrutar los individuos a la hora de autodeterminar su vida personal y reproductiva (Allen, 1988); hasta discusiones sobre cómo han de ser los mecanismos de salvaguarda ante la opinión pública que deben velar por el buen nombre y honra de las personas públicas (Mill, 2017 [1859]).

La constelación ideológica o el lenguaje paradigmático que ha permitido dotar de esta coherencia interna a las diversas reflexiones sobre la privacidad se enmarca en una de las dicotomías (Bobbio, 1998), o pares conceptuales (Koselleck y Gadamer, 1997), fundamentales para la constitución del pensamiento político moderno, esto es: la dicotomía público/privado. La conceptualización moderna de esta distinción hunde sus raíces en la escisión conceptual entre sociedad civil y Estado, la cual se fraguó en el contexto de formación de un ámbito social nuevo, el de la economía capitalista, que es concebido como una esfera social distinta que se guía, exclusivamente, por sus propias normas (Abellán, 2012). El desarrollo de un ámbito económico autónomo tiene dos prerrequisitos relevantes para la privacidad: por un lado, el reconocimiento de que las relaciones sociales de carácter privado no obedecen a los mismos criterios de funcionamiento que los del ámbito político, ni pueden, en consecuencia, quedar bajo la autoridad política; por otro lado, la conceptualización de un individuo autónomo que goza de diversos ámbitos de agencia en los que no es legítimo interferir, ya sean estos agentes externos otros individuos u organizaciones de carácter privado o público.

Desde estas coordenadas de pensamiento se ha desarrollado la reflexión política, social y académica sobre la privacidad. A su vez, podemos encontrar un desarrollo jurídico muy especializado –pero que ha influido de manera muy importante en otras reflexiones sobre la privacidad– que abarca los problemas relativos a la información que circula públicamente sobre los individuos. Esta privacidad ha sido conceptualizada en el mundo anglosajón como *informational privacy* y en castellano asistimos a una transformación conceptual que se manifiesta en una controvertida tensión entre los términos intimidad y privacidad, no siendo pacífico en qué consisten y en qué se diferencian cada uno de estos conceptos.

No es casual que el Diccionario de la RAE no reconociese el término privacidad hasta el año 2001, ya que hasta hace pocas décadas su uso estaba muy circunscrito al ámbito culto y se refería a la cualidad de lo privado. Sin embargo, la transformación conceptual a la que asistimos ha extendido entre las comunidades de hablantes un significado distinto, el cual trata de recoger la RAE mediante la siguiente definición: «Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión». Esta

definición es muy similar a la que el Diccionario hace del término intimidad («Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia»), no en vano la voz inglesa *privacy* solía ser traducida al castellano por intimidad y cuando la RAE introdujo este nuevo término no faltaron autoridades que cuestionaron la decisión (Díaz Rojo, 2002). Lo interesante de esta polémica, que también tiene su derivada jurídica (véase Toscano, 2017), es que ambos conceptos cumplen una función mediadora entre la publicidad y el secreto, ya que sus usos recogen una asunción social de que existe *algo* que debe mantenerse al margen del circuito público de información y que, en consecuencia, debe gozar de confidencialidad.

De este modo, es posible identificar una corriente mayoritaria que se inscribe en la tradición alemana de las tres esferas, según la cual es posible distinguir tres ámbitos de acción social –íntimo, privado y público– que se diferencian por su relevancia pública, esto es, por el grado de conocimiento e intervención que han de disponer el resto de integrantes de la comunidad sobre lo que una persona o grupo realizan. Esto es lo que permite y da lugar a que se produzcan distintos regímenes de visibilidad en cada una de ellas, ya que existe una estrecha vinculación entre la relevancia pública de los asuntos y el régimen de publicidad del que gocen, no en vano ha de considerarse una precondición de la distinción público-privado el par conceptual público-secreto, tal y como mostró Koselleck (2007 [1959]) en "Crítica y crisis".

El régimen de visibilidad del espacio público que alumbró la Ilustración hacía radicar su legitimidad en el papel emancipador de la crítica pública, la cual operaba mediante el principio del mejor argumento. De este modo, la búsqueda de la verdad mediante la discusión pública convirtió a todas las personas en igual de capaces y eliminó, así, los privilegios estamentales de la vida pública. En este sentido, la visibilidad pública aparece como la condición de posibilidad de la igualdad, ya que los asuntos que se mantienen en secreto quedan al margen del escrutinio público y sólo de este modo se pueden mantener los privilegios de unos sobre otros. Ahora bien, esta igualación social tiende a arrojarlo todo al torbellino de la vida pública, ya que nada, en principio, queda al margen de la crítica pública. Stuart Mill (2017 [1859]) supo captar muy tempranamente el poder social que entrañaba este nuevo régimen de visibilidad pública y entendió que era necesario establecer límites para proteger a aquellos que disienten de las opiniones mayoritarias.

En este sentido, cabe entender la privacidad como un mecanismo de defensa del individuo ante el control social, permitiendo que este pueda establecer un legítimo muro de confidencialidad sobre los asuntos de su vida que no atañen a terceras personas. Atendiendo a la evolución moderna del concepto de privacidad aparece con claridad su carácter esencialmente reactivo, ya que su función de mediación entre la publicidad y el secreto nunca puede establecerse en términos positivos: tan sólo mediante la evolución de las fuentes de injerencia, esto es, de las técnicas para convertir lo secreto en visible, se ha podido ir estableciendo social y jurídicamente el alcance de ese ámbito de la vida personal que se tiene el derecho a mantener fuera de la mirada pública.

Este carácter reactivo se aprecia mejor en la estrecha relación que guarda la privacidad con el desarrollo tecnológico. Así, la libertad de prensa que siguió a la invención de la imprenta conllevó, muy tempranamente, la protección de la vida privada de las personas a través de la prohibición de las calumnias e injurias. La popularización de la cámara fotográfica, en la misma línea, fue la responsable de que se limitase la propiedad y reproducción de fotografías en favor de un derecho a la propia imagen (Whitman, 2004, pp. 1175-1178; Richardson, 2017, p. 3; Smartt, 2014, p. 45). Este mismo esquema se vuelve a repetir en la actualidad con la aparición de Internet y, en particular, desde que la conectividad digital se ha vuelto ubicua y ha hecho que se desdibujen las fronteras entre lo *online* y lo *offline*; asunto que ha permitido que la cuestión de la visibilidad pública de los asuntos íntimos o privados irrumpan en las discusiones sobre la privacidad. La pregunta que cabría formularse, por tanto, es si esta perspectiva que consagra la protección de la vida personal individual sigue siendo adecuada para los cambios sociotécnicos que se están produciendo con la aparición de la economía de la vigilancia.

3. El desarrollo de la economía de la vigilancia

Según datos del Banco Mundial, el número de usuarios de Internet a nivel global pasó del 0,3% en 1993 al 6,8% en 2000, crecimiento que fue mayor en las economías desarrolladas, que pasaron del 1% al 30,6% durante el mismo periodo. Afianzando, así, el papel de las tecnologías de la información en la consolidación de un proceso de globalización político, social y económico sobre el que se ha desarrollado una sociedad altamente digitalizada e interconectada.

Este crecimiento de Internet estaba orientado, por un lado, a mejorar la capacidad organizativa y de gestión de las organizaciones (automatización de las labores de gestión), y, por otro, a fomentar un consumo entre los usuarios finales basado en el comercio electrónico de productos y servicios, suscripciones digitales y la venta de publicidad. De este modo, las empresas del sector de las telecomunicaciones aplicaron a Internet el mismo modelo de negocio que emplean los medios de comunicación de masas, el cual se basa en la retención del público o audiencia en sus medios para así poder vender su espacio publicitario a los anunciantes (Dahlberg y Siapera, 2007).

Sin embargo, el estallido de la burbuja de las *puntocoms* puso en entredicho la viabilidad económica de este modelo de negocio y trajo consigo el declive de uno de los productos estrella de esta etapa económica: los portales de Internet. No obstante, la publi-

cidad y la integración de servicios digitales seguirían siendo dos de los pilares del negocio digital, aunque ahora haciendo un uso más intensivo de las capacidades que la conectividad de red ofrecen en estos ámbitos. De este modo, la publicidad digital dejó de intentar replicar un modelo que estaba bien diseñado para los medios de comunicación de masas y empezó a desarrollar nuevas técnicas para aumentar la precisión con la que se puede diseñar el público objetivo de una campaña publicitaria.

La información disponible sobre los usuarios es el factor que determina la precisión con la que se puede diseñar el público objetivo de un campaña. En función de qué tipo de precisión se pretenda vender a los anunciantes, esta información será tratada para generar un perfil sobre cada usuario acorde con los objetivos perseguidos (Ferraris et al., 2013). De este modo, a las variables ya empleadas en la publicidad tradicional, se suman las disponibles por la especificidad de la conectividad de red, esto es, aquellas que permiten reconstruir el comportamiento de los usuarios durante su actividad en Internet y que dan lugar a un nuevo tipo de publicidad basada en el comportamiento (Goldfarb y Tucker, 2011; Sanje y Senol, 2012).

Este nuevo tipo de publicidad digital impulsó el desarrollo de una industria especializada en el seguimiento y registro de las actividades que llevan a cabo los usuarios a través de Internet (véase Cyphers y Gebhart, 2019; Christl, 2017). El objetivo principal de los actores de esta industria es maximizar la información disponible sobre los usuarios, de tal modo que se puedan desarrollar perfiles más precisos sobre los gustos y preferencias de los individuos; ya que cuanto más detallado sea el dossier, mayor valor económico alcanzará.

Podemos afirmar que la economía de la vigilancia nace cuando esta industria del seguimiento se diversifica y comienza a desarrollar nuevas técnicas de vigilancia que ya no están orientadas únicamente a satisfacer las necesidades de la publicidad comportamental. Se trata del momento en el que comienzan a proliferar plataformas digitales que basan su modelo de negocio en ofrecer servicios gratuitos a cambio de que el usuario conceda ser vigilado en sus interacciones digitales, generándose, así, una presión por desarrollar interfaces y ofrecimientos orientados a que los usuarios vuelquen informaciones relevantes para el emergente mercado de los datos, ya sea esto de manera voluntaria o bien mediante el fomento de comportamientos que sean funcionales a la elaboración de los conjuntos de datos (*datasets*).

De este modo, el auge de dispositivos inteligentes como teléfonos, televisiones, altavoces, bombillas, frigoríficos, etc. (IEEE, 2015; Moghaddam, Acar, Ben Burgess, Mathur, Huang, Feamster, Felten, Mittal y Narayanan, 2019; Ren, Dubois, Choffnes, Mandalari, Kolcun y Haddadi, 2019), ha de entenderse dentro de la lógica extractivista de datos en la que se basa la economía de la vigilancia. No basta ya con observar y analizar el comportamiento que llevan a cabo los usuarios a través de Internet, es necesario, además, vigilar las actividades que se producen fuera del ámbito digital para tener una visión más compleja y detallada de los procesos sociales analizados. Esto ha sido posible gracias al desarrollo de las técnicas de Big Data e Inteligencia Artificial, las cuales, a su vez, han permitido la eclosión de un nuevo ámbito de actividad económica orientado a la predicción de los comportamientos humanos. Ámbito que ha contribuido a disparar la demanda de datos, ya que estas técnicas estadísticas requieren una cantidad ingente de información sobre el mundo social para que sus modelos puedan ser aplicables. Extremo que sólo ha sido posible una vez que se ha generalizado la presencia de artefactos digitales en todos los ámbitos de la vida, los cuales permiten que se capturen datos sobre cualquier relación social en la que participen, generándose, así, una digitalización y datificación (*datafication*) del mundo humano sin parangón.

La actual transformación digital de la economía está permitiendo, a su vez, un nuevo empuje en los esfuerzos globales por conocer y cuantificar con mayor precisión el funcionamiento del mundo social, la razón es simple: no es posible gestionar aquello que no se puede observar, y la introducción de la informática en todos los procesos sociales ha permitido que se generen nuevos registros sobre el mundo humano orientados a mejorar la eficiencia en la gestión de los recursos públicos y privados. Esta es la base sobre la que se está conceptualizando la cuarta revolución industrial, a saber: una transformación profunda de los procesos productivos y de gestión posibilitada por las nuevas fuentes de información que tienen a su disposición los responsables de toma de decisiones (*data-driven*). Esta situación no habría sido posible sin el desarrollo y consolidación de una economía de la vigilancia que permite la distribución de recursos informativos (datos) y ordena las demandas de los diversos operadores que participan en ella (productores, intermediarios y consumidores).

En definitiva, esta vigilancia de carácter económico sigue siendo una amenaza para la privacidad de las personas, entendida esta privacidad desde la perspectiva individual, o clásica, que tiene por objetivo proteger un ámbito de autonomía y dignidad personal. Si la excesiva acumulación y procesamiento de información acerca de los individuos ha sido considerado clásicamente una amenaza para las libertades fundamentales, no cabe duda de que esta vigilancia de carácter económico –en particular por su tendencia insaciable a la acumulación de datos– también lo es. Ahora bien, esta nueva forma de vigilancia tiene una serie de especificidades que la alejan, en su naturaleza y funcionamiento, de las formas previas de control y observación: la unidad de análisis no es ya la persona aisladamente considerada, sino el conjunto de datos que los individuos generamos de manera agregada en nuestras interacciones sociales; o dicho de otro modo, se ha pasado de observar personas a observar patrones de datos. De ahí que sea necesario

plantear una nueva forma de comprender la privacidad que se adapte a esta nueva realidad sociotécnica.

4. Viejos ropajes para nuevos problemas: la necesidad de una perspectiva colectiva

La poca literatura existente que aboga por una perspectiva colectiva de la privacidad suele poner como ejemplo clásico de los límites de la perspectiva individualista dos situaciones prototípicas. La primera, y posiblemente más intuitiva, es aquella en la que se producen filtraciones sobre la vida de uno a través de la información que otros deciden hacer pública (véase Sarigol, García y Schweitzer, 2014). La segunda situación, aunque menos intuitiva, está estrechamente relacionada con la anterior. No se trata ya de la información que otros, por descuido o voluntariamente, distribuyan sobre uno sino aquella información que es posible deducir a partir de los datos que otros están suministrando, a saber, los denominados datos emergentes. Por ejemplo, una persona o grupo puede estar guardando con celo ciertas informaciones referidas a su salud o hábitos de vida pero siendo más descuidados a la hora de compartir datos sobre otros aspectos de su actividad cotidiana como preferencias musicales, literarias o de ocio nocturno. El problema aquí radica en que a partir del estudio agregado de diversas fuentes de información es posible identificar variables *proxy* que permiten deducir la información ocultada a partir de las que sí se suministra. Esto es posible gracias a que otros grupos o personas están comunicando tanto las informaciones que otros pretende ocultar como las que sí se están haciendo públicas, por lo que es posible identificar un conjunto de variables compartidas que hacen de puente (*proxy*) entre aquello que sí se revela y lo que se oculta. No es necesario que haya una relación causal entre ambas, lo que permite el estudio agregado de fuentes diversas de información es establecer correlaciones estadísticas entre datos que intuitivamente nada tendrían que ver entre sí y, por tanto, desvelar aquello que se pretendía mantener oculto.

Habría que, por tanto, atender a la existencia de una dimensión colectiva sobre la privacidad que trasciende el ámbito individual de decisión. Esta dimensión tiene su fundamento no tanto en la naturaleza del bien jurídico a proteger –el derecho a mantener en secreto ciertos aspectos de la vida privada de las personas–, como en el funcionamiento de las tecnologías implicadas en la vigilancia. En este sentido, Taylor et al (2017) han argumentado que las técnicas estadísticas asociadas al *Big Data* no están orientadas al tratamiento de información que permita identificar personas (esto es, datos personales), sino información relativa a grupos o unidades de análisis agregadas (datos sociales). De este modo, al ser objeto de tratamiento estadístico los datos agregados de diversos individuos que comparten unas características determinadas, ya sean estas demográficas, de intereses o relativas al comportamiento, de nada sirve que uno o pocos individuos decidan oponerse al tratamiento de su información: mientras siga siendo posible adscribirlos al grupo estudiado, las consecuencias sobre su privacidad seguirán siendo las mismas.

El grupo, en tanto que agregado de individuos que comparten determinados rasgos, es el que es objeto de vigilancia y por tanto el que debe tener la capacidad de autodeterminarse informativamente. Esto plantea un serio reto teórico: la literatura y doctrina que ha abordado el derecho de autodeterminación informativa como mecanismo para adaptar la protección de la vida privada e íntima al ámbito digital (derecho a la privacidad), la ha fundamentado filosóficamente en el iusnaturalismo de corte individual (Richardson, 2017). De ahí que la tarea pendiente sea llevar este razonamiento al plano colectivo y desarrollar una perspectiva no individualista sobre la privacidad, lo cual puede lograrse sin renunciar a sus pilares, a saber, la protección de la autonomía y dignidad en el ámbito digital; solo que ahora esa autonomía y dignidad que hay que proteger ya no es individual, sino grupal.

Esta privacidad colectiva debe, por tanto, extrapolar la protección de la autonomía y dignidad personal a la escala grupal, lo cual debe pasar por introducir en la reflexión teórica, al menos, las siguientes tres dimensiones:

4.1. Discriminación y sesgos en el análisis de datos

Bajo las etiquetas de Big Data o Inteligencia Artificial encontramos diversas técnicas de tratamiento automatizado de elevados volúmenes de datos con el fin de descubrir patrones de comportamiento entre los individuos o fenómenos estudiados. Esto ha dado lugar a una industria del dato orientada a la predicción de fenómenos sociales con diversos fines, a saber: mejorar los procesos organizativos, optimizar las rutas logísticas, anticipar picos de demanda en los servicios, etc. Pero también otros cuya ética es más dudosa, por ejemplo: deducir la orientación sexual de una persona a través del reconocimiento facial (Wang y Kosinski, 2018), detectar enfermedades genéticas a partir del rostro de un paciente (Gurovich, Hanani, Bar, et al., 2019), inferir el grado de criminalidad de una persona por su rostro (Wu y Zhang, 2016), predecir en qué zonas se producirán más crímenes, calcular la probabilidad de que un preso llegue a ser reincidente o de que un denunciante esté mintiendo en su declaración, etc. (Suresh y Guttag, 2019; Kleinberg, Ludwig, Mullainathan y Sunstein, 2019; Ricaurte, 2019; Tayebi y Glasser, 2016; Hardyns y Rummens, 2017; Cui, 2016; Skeem y Lowenkamp, 2016; Fass, Heilbrun, DeMatteo y Fretz, 2008; Babuta, 2018).

Estas herramientas predictivas utilizan lo que se conoce como aprendizaje automático, esto es: una amplia familia de técnicas estadísticas que emplean diversos conjuntos de datos (*data sets*) para entrenar los modelos matemáticos en aras de perfeccionar sus capacidades de anticipación (véase Marsland, 2015). Esto quiere decir que, por sí mismas, estás

técnicas no garantizan un conocimiento que se adecue a los estándares científicos: en función de cómo sea diseñado e implementado el modelo, y dependiendo de qué tipo de datos están disponibles para el entrenamiento, los resultados podrían variar significativamente.

Debido a que estas técnicas están siendo utilizadas en ámbitos que pueden afectar directamente a la autonomía y dignidad de las personas, durante los últimos años se ha desarrollado un amplio campo de estudio enfocado a introducir principios éticos y de transparencia en el desarrollo de los mismos. Esto es importante porque dependiendo del uso que se den a estas técnicas se podrían estar introduciendo sesgos raciales, de género e ideológicos en los resultados de los modelos predictivos y con ello se podría estar colaborando a la estigmatización de colectivos ya discriminados e, incluso, se podría estar sometiendo a procesos de decisiones automatizadas, en base al historial de comportamientos de un grupo, a individuos que no guardan, necesariamente, ningún tipo de relación con el patrón de comportamientos del grupo al que han sido adscritos.

4.2. Autonomía política

La vigilancia sistemática de las preferencias ideológicas y los comportamientos políticos, aunque sean agregados, de grupos de votantes inaugura nuevos riesgos de cara al funcionamiento de la esfera pública digital. Esto es especialmente severo por las oportunidades que se abren a los distintos actores políticos para influir en la opinión pública, diseminar la desinformación o alterar el comportamiento electoral de los votantes.

De este modo, la autonomía política de los electores se puede ver alterada por diversas técnicas que no existían hasta la aparición de las plataformas digitales que vehiculan la esfera pública digital. Por ejemplo, diversos estudios (Sánchez, 2018; Tambini, Labo, Goodman y Moore, 2017; Barocas, 2012) han documentado el uso de campañas publicitarias hipersegmentadas (*microtargeting*) para impactar en distintos grupos de votantes de manera personalizada. El objetivo de estas técnicas es adaptar los mensajes políticos a los miedos e intereses particulares de cada colectivo y así aumentar la eficacia de los mismos, normalmente para dirigir su compartimiento hacia el objetivo marcado (votar a un candidato o desmovilizar el voto del adversario). El fenómeno de la desinformación está estrechamente relacionado con esto (Bradshaw y Howard, 2019; Bendiek y Schulze, 2019; Canadian Security Intelligence Service, 2018), ya que el proceso de personalización que ha experimentado la web con el desarrollo de las plataformas digitales ha permitido la creación de burbujas informativas en las que los bulos se reproducen y aumentan su repercusión con facilidad; por lo que diseminar la desinformación resulta relativamente sencillo con un estudio adecuado de los comportamientos mediáticos de los grupos que participan en estas burbujas.

A pesar de que estas técnicas han podido desarrollarse gracias al desarrollo de técnicas de vigilancia masiva de individuos, de nuevo nos encontramos con que la privacidad que se ve afectada por estas técnicas no es solo la del individuo tomado aisladamente, sino la autonomía de los colectivos que son diseñados como públicos objetivos de las campañas orientadas a alterar su comportamiento político. De ahí la necesidad de introducir en el análisis sobre la privacidad no solo aquello que se refiere a la observación de comportamientos, componente fundamental de la vigilancia, sino también las consecuencias políticas que esta vigilancia tiene sobre los comportamientos colectivos.

4.3. Soberanía digital

Al ampliar el foco sobre las consecuencias que la vigilancia tiene en la autonomía de los grupos humanos nos aparece una cuestión fundamental: la soberanía digital. Efectivamente, a la ya clásica carrera por liderar el sector de la computación mediante el desarrollo de superordenadores que aventajen a sus rivales en capacidad de cómputo, se le ha sumado en estos años la carrera por liderar el sector de la Inteligencia Artificial. Ambas competiciones no se entienden únicamente por su relevancia económica o tecnológica, más bien la inversión pública que las sustentan se explica mejor desde la derivada militar –especialmente por su relación con el dominio criptográfico– y por su papel en la pugna global por la soberanía digital.

Esta pugna se está desarrollando paralelamente en dos ámbitos diferentes. Por un lado, la ya mentada carrera por liderar el sector de la computación y la IA obedece a la necesidad de desarrollar el conocimiento técnico suficiente para procesar volúmenes elevados de información sin depender de empresas que estén bajo jurisdicciones extranjeras. Por otro lado, como ya se ha explicado antes, los modelos de aprendizaje automatizado en los que se basa el actual estadio de la IA requieren de un volumen de datos muy alto que no resulta fácil acumular y que, en la actualidad, están bajo la custodia de las principales plataformas digitales (estadounidenses). De ahí la presión por desarrollar legislaciones que obliguen a que los datos se almacenen en territorios que estén bajo la misma jurisdicción que la nacionalidad de sus generadores.

¿Cuál es el objetivo de lograr la soberanía digital en materia de datos y de su capacidad para procesarlos? Si para hablar de la dimensión económica de los datos es necesario comprender el papel que juegan en lo que se ha denominado cuarta revolución industrial, al llevarlo al plano político hemos de comprender que la lógica de los datos sigue siendo la misma, sólo que desde un plano de acción distinto: la capacidad de observación. La economía de la vigilancia ha generado un ámbito sociotécnico nuevo desde el que se puede observar, comprender y analizar el comportamiento de las sociedades a una escala nunca antes disponible. Privar a las comunidades políticas de esta posibilidad

para autocomprenderse supondría limitar la capacidad de acción de las mismas y, por ende, de su soberanía. Además, tampoco debe pasarse por alto la dimensión geopolítica en cuestión, ya que la capacidad de observar el funcionamiento de las sociedades a través de los datos permite a los detentores de los mismos obtener una posición de superioridad en el tablero global.

5. Conclusión

La privacidad ha sido abordada históricamente como un asunto relativo a la protección del ámbito íntimo e individual frente a las injerencias ilegítimas que pudieran provenir del exterior. A pesar de las diferentes concepciones que se pueden encontrar en la literatura, existe un núcleo conceptual que se ha mantenido a lo largo del tiempo con cierta estabilidad y que proviene, precisamente, de uno de los pares conceptuales que más han marcado el pensamiento político occidental: la distinción público/privado. Así, el lenguaje paradigmático de la privacidad se ha movido en un entramado ideológico que le permitía operar como un regulador de los límites, siempre volátiles, entre lo que se considera público y lo que se entiende que no debe concernir a nadie más que al individuo. Esta es la razón por la que en su núcleo conceptual se encuentran dos de las cuestiones claves de la tradición política de raigambre liberal, a saber, la autonomía y la dignidad de la persona. No en vano el pensamiento sobre la privacidad está fundamentalmente orientado a garantizar estos dos atributos inalienables del individuo.

Ahora bien, según han ido evolucionando los fenómenos sociotécnicos que podían poner en cuestión estos atributos del individuo, así ha ido transformándose el concepto de privacidad. Esta es la razón por la que en la tercera sección haya sido abordado el desarrollo de la economía de la vigilancia, pues su aparición es actualmente el principal motor de cambio del concepto de privacidad. De este modo, para comprender y dar sentido a la privacidad en el mundo actual ha de observarse cómo son y qué consecuencias sociales tienen estas nuevas formas de vigilancia. Aquí se ha defendido que para lograr este objetivo es necesario introducir un nuevo nivel de análisis en la privacidad que no se centre exclusivamente en el individuo.

El principal obstáculo para desarrollar teóricamente esta privacidad colectiva radica en que no resulta sencillo extrapolar los dos principales pilares de la privacidad, la autonomía y dignidad, del plano individual al colectivo. No al menos sin pensar cómo se relacionan ambas en el contexto de la economía de la vigilancia, de ahí que hayan sido expuestas las tres dimensiones que, de manera fundamental, tendremos que seguir explorando para construir este puente teórico. El objetivo no es otro que mostrar que la privacidad es un bien social que no sólo asiste a los individuos o grupos, sino a la sociedad en su conjunto, y que de su evolución depende cómo se reproduzca en el futuro la distinción público/privado, o lo que es lo mismo, cómo serán las bases culturales para delimitar hasta dónde puede llegar el control y la automatización de la vida.

6. Referencias

Abellán, J. (2012). Diferenciación conceptual entre Estado y sociedad. En *Política* (pp. 233-238). Madrid: Alianza Editorial.

Allen, A. L. (1988). *Uneasy Access: Privacy for Women in a Free Society*. Totowa, N.J: Rowman & Littlefield.

Babuta, A. (2018). Innocent Until Predicted Guilty? Artificial Intelligence and Police Decision-Making. *Royal United Services Institute*, *38*(2), 1-4.

Barocas, S. (2012). The price of precision: voter microtargeting and its potential harms to the democratic process. En *PLEAD '12 Proceedings of the first edition workshop on Politics, elections and data* (pp. 31-36). New York: ACM.

Bendiek, A. y Schulze, M. (2019). Disinformation and Elections to the European Parliament. *SWP Comments* k. Recuperado de https://www.swp-berlin.org/10.18449/2019C16/

Bobbio, N. (1998). La gran dicotomía: público/privado. En *Estado, Gobierno y Sociedad* (pp. 11-38). México: Fondo de Cultura Económica.

Bradshaw, S. y Howard, P. N. (2019). *The Global Disinformation Order. 2019 Global Inventory of Organised Social Media Manipulation*. Oxford: Oxford Internet Institute.

Brunner, O. (1977). La "casa grande" y la "oeconomica" de la Vieja Europa. En *Nuevos caminos de la historia social y constitucional* (pp. 87-123). Buenos Aires: Alfa (Original publicado en 1968).

Canadian Security Intelligence Service (2018). *Who said what? The Security Challenges of Modern Disinformation* (No. 2018-02-01). Ottawa: World Watch Expert Notes.

Christl, W. (2017). *Corporate Surveillance in Everyday Life*. Vienna: Cracked Lab – Institute for Critical Digital Culture. Recuperado de http://crackedlabs.org

Cui, G. (2016). Evidence-Based Sentencing and the Taint of Dangerousness. *The Yale Law Journal*, *125*, 315-322.

Cyphers, B. y Gebhart, G. (2019). *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*. San Francisco: Electronic Frontier Foundation. Recuperado de https://www.eff.org/wp/behind-the-one-way-mirror

Dahlberg, L. y Siapera, E. (2007). Introduction: Tracing Radical Democracy and the Internet. En L. Dahlberg & E. Siapera (Eds.), *Radical democracy and the Internet. Interrogating theory and practice* (pp. 1-16). New York: Palgrave Macmillan.

Díaz Rojo, J. A. (2002). Privacidad: ¿neologismo o barbarismo? *Espéculo*, (21). Recuperado de https://webs.ucm.es/info/especulo/numero21/privaci.html

Fass, T. L., Heilbrun, K., DeMatteo, D. y Fretz, R. (2008). The LSI-R and the Compas. *Criminal Justice and Behavior*, *35*(9), 1095-1108.

Fernández Barbudo, C. (2019). El nuevo concepto de privacidad: la transformación estructural de la visibilidad. *Revista De Estudios Políticos*, *185*, 139-167.

Ferraris, V., Bosco, F., Cafiero, G., D'Angelo, E. y Suloyeva, Y. (2013). *Defining Profiling*. PROFILING. Fundamental Rights and Citizenship Programme of the European Union. Recuperado de www.proling-project.eu

Goldfarb, A. y Tucker, C. E. (2011). Online advertising, behavioral targeting, and privacy. *Communications of the ACM*, *54*(5), 25-27.

Gurovich, Y., Hanani, Y., Bar, O., Nadav, G., Fleischer, N. y Gelbman, D. (2019). Identifying facial phenotypes of genetic disorders using deep learning. *Nature Medicine*, *25*(1), 60-64.

Hardyns, W. y Rummens, A. (2017). Predictive Policing as a New Tool for Law Enforcement? Recent Developments and Challenges. *European Journal on Criminal Policy and Research*, *24*(3), 1-18.

IEEE (2015). *Internet of Things (IoT) Ecosystem Study*. Piscataway: IEEE. Recuperado de http://standards.ieee.org/innovate/iot/study.html

Inness, J. C. (1992). Privacy, intimacy, and isolation. New York: Oxford University Press.

Kleinberg, J., Ludwig, J., Mullainathan, S. y Sunstein, C. R. (2019). Discrimination in the Age of Algorithms. *SSRN Electronic Journal*. Recuperado de https://ssrn.com/abstract=3329669

Koselleck, R. (2004). Historia de los conceptos y conceptos de historia. *Ayer*, *1*(53), 27-45.

Koselleck, R. (2007). *Crítica y Crisis*. Madrid: Trotta, Universidad Autónoma de Madrid (Original publicado en 1959).

Koselleck, R. y Gadamer, H.-G. (1997). *Historia y hermenéutica*. Barcelona: Paidós I.C.E./U.A.B.

Marsland, S. (2015). *Machine Learning. An Algorithmic Perspective*. Boca Raton: Champan & Hall.

Mill, J. S. (2017). *Sobre la libertad*. Madrid: Biblioteca Nueva (Original publicado en 1859).

Moghaddam, H. M., Acar, G., Ben Burgess, Mathur, A., Huang, D. Y., Feamster y N. (2019). *Watching You Watch: The Tracking Ecosystem of Over-the-Top TV Streaming Devices*. ACM SIGSAC Conference on Computer and Communications Security, Londres.

Ren, J., Dubois, D. J., Choffnes, D., Mandalari, A. M., Kolcun, R. y Haddadi, H. (2019). *Information Exposure From Consumer IoT Devices: A Multidimensional, Network-Informed Measurement Approach*. IMC '19, Amsterdam.

Ricaurte, P. (2019). Data Epistemologies, Coloniality of Power, and Resistance:. *Television & New Media*, *20*(4), 350-365.

Richardson, M. (2017). *The Right to Privacy. Origins and Influence of a Nineteenth-Century Idea*. Cambridge: Cambridge University Press.

Sánchez, S. A. (2018). La esfera pública en la era de la hipermediación algorítmica: noticias falsas, desinformación y la mercantilización de la conducta. *Hipertext.Net: Revista Académica Sobre Documentación Digital Y Comunicación Interactiva*, *17*, 74-82.

Sanje, G. y Senol, I. (2012). The Importance of Online Behavioral Advertising for Online Retailers. *International Journal of Business and Social Science*, *3*(18), 114-121.

Sarigol, E., Garcia, D. y Schweitzer, F. (2014). Online privacy as a collective phenomenon. En *Proceedings of the second ACM conference on Online social networks* (pp. 95-106). New York: ACM Press.

Skeem, J. L. y Lowenkamp, C. T. (2016). Risk, Race, And Recidivism: Predictive Bias And Disparate Impact. *Criminology*, *54*(4), 680-712.

Smartt, U. (2014). *Media and Entertainment Law.* London: Routledge.

Suresh, H. y Guttag, J. V. (2019). *A Framework for Understanding Unintended Consequences of Machine Learning*. arXiv. Recuperado de https://arxiv.org/abs/1901.10002v1

Tambini, D., Labo, S., Goodman, E. y Moore, M. (2017). *The new political campaigning*. *Media Policy Brief*. London: Media Policy Project, London School of Economics and Political Science.

Tayebi, M. A. y Glasser, U. (2016). *Social Network Analysis in Predictive Policing. Concepts, Models and Methods*. Génova: Springer.

Taylor, L., Floridi, L. y van der Sloot, B. (Eds.). (2017). *Group Privacy*. Cham: Springer International Publishing.

Toscano, M. (2017). Sobre el concepto de privacidad: la relación entre privacidad e intimidad. *Isegoría*, *57*, 533-20.

Wang, Y. y Kosinski, M. (2018). Deep neural networks are more accurate than humans at detecting sexual orientation from facial images. *Journal of Personality and Social Psychology*, *114*(2), 246-257.

Whitman, J. Q. (2004). The Two Western Cultures of Privacy: Dignity versus Liberty. *The Yale Law Journal*, *113*(6), 1151-1222.

Wu, X. y Zhang, X. (2016). *Automated Inference on Criminality using Face Images*. arXiv. Recuperado de https://arxiv.org/abs/1611.04135v2