Privacidad (digital)
(Digital) privacy

Carlos Fernández Barbudo
Universidad Complutense de Madrid
ORCID ID 0000-0003-0508-8032
cfbarbudo@ucm.es

Cita recomendada:

Fernández Barbudo, C. (2019). Privacidad (digital). *Eunomía. Revista en Cultura de la Legalidad*, 17, 276-288.

doi: https://doi.org/10.20318/eunomia.2019.5033

Recibido / received: 28/06/2018
Aceptado / accepted: 05/09/2019

Resumen
El desarrollo de las tecnologías de la información, y en particular Internet, ha supuesto la aparición de nuevas preocupaciones sociales que plantean la imposibilidad de preservar la privacidad —que no la intimidad— de la población en el ámbito digital. Esta contribución aborda, en perspectiva histórica, la formación de un nuevo concepto sociopolítico de privacidad que ha sustituido al de intimidad en el ámbito digital. A tal fin se presentan los principales elementos que diferencian a ambos y cuáles son las transformaciones sociotécnicas fundamentales que han posibilitado este cambio conceptual. El desarrollo del texto llevará a defender la idoneidad de una mirada política sobre la privacidad y finaliza con la presentación de algunas propuestas recientes que abogan por entender la privacidad como un problema colectivo.

Palabras clave
Espacio público, derecho a la privacidad, intimidad, público/privado, ciberespacio.

Abstract
The development of information technologies, and in particular the Internet, has led to the emergence of new social concerns that raise the impossibility of preserving privacy in the digital sphere. This contribution addresses, in historical perspective, the formation of a new socio-political concept of privacy that has replaced the previous one. To this end, the main elements that differentiate both are presented and what are the fundamental sociotechnical transformations that have enabled this conceptual change. The development of the text will lead to defend the suitability of a political view on privacy and ends with the presentation of some recent proposals that advocate understanding privacy as a collective problem.

Keywords
Public space, right to privacy, private life, public/private, cyberspace.

SUMARIO. 1. Introducción: ¿un problema de traducción? 2. El paso de la intimidad a la privacidad. 3. Fase actual: un nuevo concepto. 4. Por una privacidad colectiva: la necesidad de una mirada política. 5. Conclusiones.

1. Introducción: ¿un problema de traducción?

Que el término privacidad pueda considerarse un anglicismo del que es preferible prescindir no es una cuestión pacífica. Los detractores de su uso han argumentado, tradicionalmente, que esta palabra no añade nada sustantivamente diferente a lo que ya se puede expresar mediante el uso del término intimidad. Esta es la razón por la que en la edición a cargo de Benigno Pendás (1995) de uno de los textos más citados sobre el derecho a la privacidad, «The Right to Privacy», se prescinde de la palabra privacidad en favor de la de intimidad. En esta misma línea, el filólogo Díaz Rojo (2002) ha analizado el controvertido uso que se ha hecho del término privacidad en la prensa y como muchos de estos usos eran, en bastantes ocasiones, intercambiables por otros afines y más precisos como vida privada, intimidad o confidencialidad. En definitiva, según sus detractores, la palabra privacidad sería una mala traducción de la voz inglesa *privacy* o, en el mejor de los casos, un neologismo tolerable.

No en vano, si acudimos al Diccionario de la RAE podemos encontrar una definición de privacidad que tiene importantes elementos en común con la de intimidad:

- «Privacidad». f. Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión.
- «Intimidad». f. Zona espiritual íntima y reservada de una persona o de un grupo, especialmente de una familia.

Los defensores del término privacidad, por su parte, argumentan que su uso recoge un significado que va más allá de la intimidad. El ejemplo más claro de este tipo de usos lo encontramos en la exposición de motivos de la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal:

> El progresivo desarrollo de las técnicas de recolección y almacenamiento de datos y de acceso a los mismos ha expuesto a la privacidad, en efecto, a una amenaza potencial antes desconocida. Nótese que se habla de la privacidad y no de la intimidad: Aquella es más amplia que esta, pues en tanto la intimidad protege la esfera en que se desarrollan las facetas más singularmente reservadas de la vida de la persona —el domicilio donde realiza su vida cotidiana, las comunicaciones en las que expresa sus sentimientos, por ejemplo—, la privacidad constituye un conjunto, más amplio, más global, de facetas de su personalidad que, aisladamente consideradas, pueden carecer de significación intrínseca pero que, coherentemente enlazadas entre sí, arrojan como precipitado un retrato de la personalidad del individuo que éste tiene derecho a mantener reservado.

De este modo, la privacidad alude a algo que está más allá de la intimidad pero que comparte con esta una función mediadora entre la publicidad y el secreto, pues reconoce la existencia de algo que debe mantenerse al margen del circuito público de información y que, en consecuencia, debe gozar de confidencialidad.

2. El paso de la intimidad a la privacidad

Ambos conceptos, por tanto, recogen la necesidad de que los individuos cuenten con mecanismos para mantener un ámbito propio al margen del escrutinio público,

ya provenga este de la sociedad civil o de los poderes públicos. Esta necesidad tiene como fundamento moral la idea, de origen liberal, de que todo individuo cuenta con una dignidad y autonomía personal inalienables (véase Richardson, 2017). Asunto que se encuentra bien consolidado a nivel internacional tanto en la Declaración Universal de Derechos del Hombre de 1948 (art. 12) como en el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (art. 8), y que encuentra en los denominados derechos de la personalidad su necesaria concreción a través de la protección del honor, la propia imagen y la intimidad personal y familiar. La principal diferencia entre ambos conceptos parecería radicar, por tanto, en el papel que desempeñan la informática y las telecomunicaciones en la configuración de las amenazas que se vierten sobre este ámbito, íntimo o privado, que se tiene derecho a mantener en secreto.

Estas amenazas provinieron inicialmente del desarrollo de la informática y, en particular, del creciente uso por parte de las administraciones públicas de las bases de datos. Estas herramientas generaron una fascinación fruto de la eficacia que introdujeron en la gestión, a la vez que una honda preocupación por las capacidades de control sobre la población que inauguraron, ya que la existencia de herramientas que pudieran dar acceso inmediato y unificado a toda la información disponible sobre una persona era materia reservada a las obras de ciencia ficción. En esta línea, la década de 1970 supuso el inicio de la regulación de las bases de datos (véase González Fuster, 2014): el estado alemán de Hesse aprobó la Ley de Protección de Datos de Hesse (*HessischeDatenschutzgesetz*) en 1970, Suecia aprobó la Ley de Datos (*Datalag*) en 1973 y Estados Unidos de América la *Privacy Act* en 1974. Estas normas otorgaban a los afectados diversos derechos, como los de acceso y rectificación, sobre la información que acerca de su persona poseyera la administración (tan solo la sueca lo extendió a organizaciones de derecho privado), y marcaron una gran influencia en el desarrollo legislativo posterior. De este modo, el concepto alemán de Protección de Datos (*Datenschutz*) marcó el proceso europeo que desembocó en el Convenio 108, mientras que en Estados Unidos la capacidad de limitar la adquisición y circulación de información personal se vinculó al concepto de *informational privacy*.

Nótese que en la recepción de estos debates jurídicos en España se ha preferido traducir el término *privacy* por el de intimidad (véase Pérez Luño, 1979), mientras que el término privacidad se utiliza, fundamentalmente, en ámbitos no jurídicos para expresar los problemas que tecnologías como Internet plantean a la intimidad y al respeto por la vida privada de las personas. Por tanto, para entender cómo estos debates no jurídicos han cargado semánticamente la recepción del concepto de privacidad ha de observarse qué temas han marcado el debate de la *privacy* en los desarrollos tecnológicos.

Así, podemos observar que seguridad informática y *computer privacy* han sido tradicionalmente conceptos distintos, pero estrechamente relacionados (véase Yost, 2007). En este sentido, la seguridad informática ha sido históricamente un campo de estudio orientado a la seguridad de estado y las aplicaciones militares, ámbitos dominados por la criptografía y muy cerrados a la discusión pública. No en vano debemos esperar hasta la década de 1990 para asistir al nacimiento de una industria de aplicaciones comerciales de seguridad informática orientada al usuario final. No obstante, fue la criptografía académica, alrededor de la década de 1980, la responsable de abrir al público especializado los problemas de privacidad que la informática podía conllevar. Al respecto cabe destacar la aportación de David Chaum (1985), quien introdujo el anonimato como nueva pieza clave en el diseño de los sistemas criptográficos. Hasta el momento, el problema de la atribución era un

problema de integridad, esto es, orientado a evitar la suplantación de identidad, pero con este giro se introdujo una nueva forma de entender la privacidad como derecho a no ser identificado. El objetivo de este anonimato era sortear el problema del control social y evitar que la vigilancia electrónica conllevase una alteración de la conducta de los ciudadanos, garantizándose, así, que su autonomía y libertad no se vieran afectadas. En efecto, la privacidad ya no aparece aquí como algo relativo exclusivamente a la confidencialidad de las comunicaciones, sino como un problema relativo a la autonomía individual, ya que la falta de seguridad en los sistemas informáticos puede llegar a alterar la voluntad personal: el incremento de interacciones sociales mediadas por ordenadores y de bases de datos que almacenan información personal han hecho que aumente el número de personas en disposición de observar, a través de los múltiples registros electrónicos existentes, las actividades que se realizan cotidianamente; lo cual, argumenta Chaum (1985), puede traducirse en que las personas alteren sus comportamientos al percibir que sus actividades están siendo observadas sin su conocimiento.

El desarrollo de las redes de datos, que posteriormente desembocarían en lo que hoy conocemos como Internet, permitió que se establecieran comunicaciones a distancia entre los primeros ordenadores y con ello la *computer privacy* cobró una nueva dimensión. ARPAnet es la más conocida entre las pioneras pero este mismo concepto se desarrolló en paralelo en otros puntos del globo, entre estas primeras redes cabe destacar la francesa CYCLADES (que comenzó a operar en 1975), la inglesa NPL (1973), la canadiense DATAPAC (1976) y la japonesa DDX-1 (1977) (Kim, 2005; Mathison, 1978; Winston, 1998). Estas redes se desarrollaron desde el ámbito académico, con un alto grado experimental, para poner en común recursos científicos almacenados a distancia y no pensando en un hipotético uso generalizado como el que hoy conocemos, de ahí que las medidas de seguridad orientadas a garantizar la confidencialidad de las comunicaciones y evitar accesos no autorizados fuesen muy limitadas. Internet nacería posteriormente como un método para permitir la comunicación entre las redes ya existentes, de ahí que la Red que hoy conocemos haya heredado los problemas de diseño de estas primeras redes en materia de seguridad y confidencialidad. De este modo, al problema iniciado con el desarrollo de las bases de datos se lee sumó, con la capacidad de poner estas máquinas en comunicación remota, el riesgo de que se produjesen accesos no autorizados al contenido de estas bases de datos sobre una red que, además, no estaba diseñada para garantizar la confidencialidad de las comunicaciones que sobre ella se producía. No en vano, el que ha sido el enfoque dominante en este ámbito, el paradigma CIA recogido en la norma ISO 17799, hay que entenderlo desde estas problemáticas, pues sus tres principios rectores (garantizar la Confidencialidad, Integridad y Accesibilidad o disponibilidad de la información) responden a lo que son los tres principales problemas de la arquitectura de Internet. Si su diseño hubiese sido distinto, las preocupaciones de seguridad y privacidad habrían sido diferentes.

3. Fase actual: un nuevo concepto

Cuando Internet se populariza, el problema relativo a las bases de datos experimenta un salto cualitativo. La información personal ya no se circunscribe a la almacenada en una base de datos tradicional custodiada por una organización dada, sino que la propia web se convierte en sí misma en una gran base de datos a la que cualquier usuario puede contribuir. Los motores de búsqueda son los responsables de esta transformación de la web, ya que gracias a su capacidad de indexación hacen que cualquier página web funcione como una entrada en esta

gran base de datos mundial y permiten, a través de su servicio público, que cualquier usuario pueda consultar todo lo indexado sobre una persona con tan sólo introducir su nombre. A este respecto cabe destacar la Sentencia del Tribunal de Justicia de la Unión Europea de 13 de mayo de 2014 contra Google España (asunto C 131/12) en el que se reconoce el conocido como "derecho al olvido", esto es, el derecho de un ciudadano europeo a solicitar a los buscadores web la desindexación (o eliminación de la lista de resultados) de aquellos contenidos sobre su persona que aparezcan a raíz de introducir su nombre completo y que carezcan de interés público (véase Powles, 2015).

Además, los debates y preocupaciones por los peligros que estas tecnologías puedan acarrear para la dignidad y autonomía de las personas cobran importancia social y política, haciendo que se multipliquen las voces que participan en estas discusiones. A partir de este momento es cuando corresponde hacer un análisis sociopolítico del concepto de privacidad, pues gracias a la historia conceptual podemos observar que el surgimiento de este nuevo concepto de privacidad obedece a la formulación colectiva de una experiencia social basada en las transformaciones sociotécnicas acaecidas con el desarrollo de Internet (Abellán, 2007; sobre este enfoque véase Koselleck, 2004). Dicho de otro modo, desde que se populariza la expresión "la privacidad ha muerto" es cuando debemos comprender el concepto de privacidad como expresión de una experiencia sociopolítica colectiva. Aunque parezca contradictorio, la privacidad nace porque se proclama su muerte: nadie diría que la intimidad ha muerto, sino la privacidad, y este es el mejor ejemplo de que son conceptos diferentes que recogen experiencias y proyectan expectativas distintas. De este modo, defiendo que lo específico de la privacidad hay que buscarlo en tres ámbitos distintos, pero estrechamente relacionados entre sí y que desbordan, con creces, el ámbito de la intimidad:

Ciberseguridad

El despliegue de Internet no sólo ha afectado al ámbito de las comunicaciones interpersonales, su penetración en los ámbitos económicos y productivos ha sido tal que podemos afirmar que, en las economías desarrolladas, no existe proceso social que no esté mediado por dispositivos con conexión de datos. De este modo, el número de dispositivos conectados a redes IP alcanzó los 18.000 millones en 2017 y se calcula que lleguen a los 28.500 millones en 2022 (Cisco, 2019). Este crecimiento se debe, entre otros factores, al desarrollo del Internet de las Cosas (*Internet of Things*) (véase Ziegeldorf, Morchon, & Wehrle, 3/2014) y su consiguiente despliegue de dispositivos inteligentes y sensores de distinta índole con conectividad de red.

La seguridad y privacidad de este conjunto de dispositivos interconectados ya no afecta, únicamente, a los individuos que los portan, sino que inciden especialmente en los procesos sociales que dependen de ellos. Esta situación no afecta sólo a infraestructuras militares, la penetración de las tecnologías de la información en todos los ámbitos de la vida social permite ahora el acceso remoto a máquinas que controlan procesos estratégicos a diferentes niveles (medios de comunicación, banca, telefonía, energía, salud, etc.) y que hasta el momento no podían más que accederse de manera física y presencial. De ahí que se introduzcan las llamadas ciberamenazas en los planes estratégicos de Protección de Infraestructuras Críticas (Choras, Kozik, Flizikowski, Hołubowicz, & Renk, 2016; véase al respecto Rinaldi, Peerenboom, & Kelly, 2001) y el ciberespacio se plantee como una amenaza para la soberanía y seguridad nacional (Bendrath, 2001; Manjikian, 2010, p. 391), tal y como plantea la recientemente publicada Estrategia Nacional de Ciberseguridad (Departamento de Seguridad Nacional, 2019).

Parte de la responsabilidad de esta situación recae en que en el diseño de estos dispositivos y redes no se han introducido las necesarias consideraciones acerca de su impacto sobre la privacidad. Esta reflexión ha llevado a acuñar el término *Privacy by Design* como un enfoque que pretende revertir dicha situación introduciendo en el proceso de diseño recomendaciones y códigos de buenas prácticas orientados a proteger la privacidad y seguridad de los sistemas, para intentar, de este modo, superar el modelo reactivo que domina en la actualidad (Danezis et al., 2014; véase Langheinrich, 2001).

El Reglamento General de Protección de Datos introduce este concepto de privacidad por diseño (adapto al enfoque de protección de datos) en el art. 25, instando a las organizaciones a aplicar técnicas de seudonimización sobre los datos recopilados, así como a procurar que los datos almacenados sean los mínimos imprescindibles y estén en posesión de la organización únicamente el tiempo necesario para los fines del tratamiento.

Economía de la vigilancia

Tras el estallido de la burbuja de las *puntocoms* en 2001 se inaugura un nuevo periodo en la explotación comercial de Internet. El modelo de negocio que saldrá triunfante de esta crisis tiene como nuevo motor de la economía de Internet la venta de publicidad personalizada. En comparación con la publicidad ofrecida anteriormente por otros medios, especialmente los transmitidos a través de medios de comunicación de masas, la publicidad personalizada supondrá un avance cualitativo para el sector por dos motivos: 1) su capacidad para seleccionar el público objetivo de un anuncio con una elevada precisión y 2) la posibilidad de medir la eficacia de los anuncios en un plazo de tiempo muy reducido (véase Goldfarb, 2013).

La información disponible sobre los usuarios es el factor que determina la precisión con la que se puede seleccionar el público objetivo de un anuncio. En función de con qué fines se acumule esta información y, especialmente, 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 (véase Ferraris, Bosco, Cafiero, D'Angelo, & Suloyeva, 2013). De este modo, a las variables ya empleadas en la publicidad no digital, 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 (véase Beales, 2010; Evans, 2009).

Dicha información se puede obtener por fuentes propias del servicio o través de fuentes externas. Las propias consisten tanto en la información que vierte deliberadamente el usuario de manera activa como aquella que es capturada de manera pasiva por el servicio durante su uso. Captura que únicamente está limitada por la tecnología del dispositivo sobre el que se ejecuta el servicio y el sistema de permisos que establece la aplicación a través de la que se accede al mismo. De ahí que exista un fuerte incentivo económico para que el diseño de los servicios esté orientado a que 1) el usuario vierta la mayor información posible sobre él mismo y 2) lleve a cabo comportamientos de los que se puedan inferir datos significativos para la construcción de su perfil.

El incentivo económico para generar perfiles de comportamiento sobre las personas no se acota al ámbito publicitario. Aunque la economía de la vigilancia encuentra en Internet un punto de inflexión en cuanto a su capacidad para captar y

encontrar un rendimiento a esta información, esta se ha expandido rápidamente a otros sectores gracias a la digitalización del mundo y el auge de dispositivos con capacidad para registrar la actividad humana y transmitir sus datos a distancia (véase Lyon, 2019; Zuboff, 2015). El desarrollo del *Big Data,* y en general la capacidad de computar grandes volúmenes de datos con fines estadísticos, así como los nuevos desarrollos en Inteligencia Artificial, requieren de un gran volumen de información sobre el comportamiento humano para entrenar los modelos matemáticos (algoritmos) que los posibilitan. Esta situación inaugura una nueva etapa en la economía de la vigilancia en la que se producen fuertes presiones por reducir las barreras que, en pos de la privacidad, tratan de limitar la capacidad de control y estudio del comportamiento de las personas (con o sin su consentimiento).

Impacto en la configuración del espacio público digital

La economía de la vigilancia no sólo posibilitó el desarrollo de la publicidad personalizada en Internet sino que aupó, en general, el fenómeno de la personalización de contenidos en la web. Internet ha sido vista tradicionalmente como una herramienta que permite que los usuarios sorteen las limitaciones geográficas a la hora de establecer contactos entre personas afines, de modo que puedan encontrar una mayor diversidad de opiniones o cosmovisiones de las que tendrían a disposición en su comunidad local y construir, así, públicos con un alto grado de homogeneidad a pesar de su dispersión geográfica. Sin embargo, dada la multiplicidad de voces disponibles en el espacio público digital, la capacidad de un usuario para encontrar aquel público que maximice sus afinidades electivas sería muy reducida de no ser por la personalización de contenidos.

Esta personalización persigue un doble objetivo: 1) que la publicidad mostrada goce de una mayor efectividad, gracias a que las posibilidades para definir el público objetivo de una campaña se vuelven mucho más precisas, y 2) que los usuarios pasen un mayor tiempo en cada uno de los servicios, ya que la personalización permite que los usuarios encuentren con mayor rapidez y facilidad aquellos contenidos en los que están interesados e incluso pueden descubrir nuevos contenidos que, gracias a la agregación de reacciones de usuarios similares, desconocía pero coinciden con las preferencias manifestadas a través del uso del servicio.

Una personalización que, además, tiene el efecto de reunir a los usuarios en función de sus diferencias particulares, generando, de este modo, públicos que se encuentran expuestos a unos niveles muy bajos de pluralidad. Esta situación obliga a replantear el carácter público de la web personalizada, pues la premisa de la máxima visibilidad (Arendt, 1958/2003) queda aquí en entredicho, ya que lo que ahí se exponga deja de ser visible por todos, o lo que es lo mismo: su publicidad deja de ser común para convertirse en particular. Efectivamente, el principio de visibilidad general de lo público queda ciertamente suspendido por efecto de la personalización, ya que el todos de cada público varía y el carácter común de la exposición pública se disuelve, especialmente por el carácter individual de la articulación de cada espacio público digital. Correspondería, entonces, hablar de mundos comunes, en plural, que se dan sobre articulaciones efímeras de carácter semipúblico, pues un mundo común sin casi pluralidad se parece más a un ámbito privado que a uno propiamente público.

4. Por una privacidad colectiva: la necesidad de una mirada política

Previamente al auge de los debates sobre la privacidad, que dató en la irrupción de la informática y las telecomunicaciones, la palabra privacidad en el castellano de España era un cultismo que se refería a la calidad de lo privado, del mismo modo que publicidad lo es de público, y que en ocasiones se utilizaba de manera muy similar al de ámbito privado o íntimo (véase Béjar, 1990). Esta línea que pensó la privacidad desde lo privado y no tanto desde lo íntimo, o como un derecho a disfrutar de una vida privada, produjo interesantes reflexiones desde la filosofía y la sociología. A este respecto cabe destacar el trabajo de E. Garzón Valdés (1998) y su distinción entre lo íntimo, lo privado y lo público que permita establecer criterios morales para una legítima intervención de terceros en cada uno de estos ámbitos.

Esta perspectiva sobre la privacidad está muy influenciada por la filosofía alemana, en la que se desarrolló la teoría de las tres esferas, y de la que J. Habermas es una de sus máximos exponentes. En este sentido, Habermas (1990/2009) plantea una relación de lo privado con lo público que resulta muy fructífera para entender el carácter no individualista de la privacidad, pues es en este ámbito en el que se producen las relaciones sociales (privadas) con relevancia pública y que desembocan en la creación de un espacio público en el que se acaba forjando la opinión pública.

La línea que inaugura Habermas puede actualizarse desde el punto clave que entiende el problema planteado en este texto como un asunto relativo a la visibilidad del ámbito privado y, por tanto, que afecta a cómo se estructura el espacio público. Este asunto de la visibilidad de lo privado es lo que ha sufrido una transformación estructural con el desarrollo de las tecnologías de la información, pues lo que hace público y secreto ya no solo se refiere a aquello que podíamos localizar en el ámbito privado, sino también (y sobre todo) en el ámbito íntimo.

Dicho de otro modo, hay una mirada posible sobre la privacidad que se refiere a cómo se produce y reproduce el secreto, y más concretamente a cómo se estructura la visibilidad personal. Esta mirada dista de la dominante en otros ámbitos que abordan la necesidad de desarrollar instrumentos para garantizar el derecho a la intimidad o privacidad, esto es, proteger el ámbito de la vida privada e íntima. Estas perspectivas dan por supuesta la existencia de un ámbito a proteger y se centran en el desarrollo de instrumentos para defenderla. Ahora bien, esos instrumentos solo se pueden desarrollar desde la constatación de hechos sociales que la ponen en cuestión. Nunca antes se dibuja el ámbito privado o íntimo, únicamente se hace esto a partir de sus amenazas; o lo que es lo mismo: solo es posible dibujar el ámbito privado e íntimo desde sus contornos, desde las cosas que la amenazan y por tanto nos obligan a tomar partido y decidir: el ámbito llega hasta aquí. Y esta toma de partido por definir hasta dónde llega es política. De ahí la necesidad de una mirada política a la privacidad, pues las pugnas por definirla y las amenazas que se engloban en las discusiones sobre la privacidad, son las que están dibujando los contornos de ese ámbito privado y/o íntimo.

Esta mirada política permite entender que los problemas que se plantean actualmente a la privacidad no son de orden individual sino colectivo, ya que las situaciones descritas en la sección anterior no afectan al individuo considerado aisladamente sino a una serie de fenómenos socioeconómicos que afectan a la sociedad en su conjunto. Actualmente pueden encontrarse algunos trabajos que abordan los problemas de privacidad desde una perspectiva grupal (véase Taylor, Floridi, & van der Sloot, 2017), argumentando que las técnicas estadísticas asociados 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).

El problema no es solo que, en materia de privacidad, las decisiones de otros me afecten a mí o que las decisiones que se tomen sobre otros tengan repercusiones sobre uno (véase Sarigol, Garcia, & Schweitzer, 2014). El nudo gordiano radica en el actual paradigma de atribución de derechos individuales del enfoque de protección de datos y, especialmente, en el pilar del consentimiento informado. Actualmente, la cantidad de actores involucrados en la recolección, tratamiento y compra-venta de datos personales es tan elevada que resulta prácticamente imposible que los titulares de derechos puedan otorgar un consentimiento realmente informado, especialmente atendiendo a las consecuencias y fines de los diversos tratamientos a los que se pueden ver sometidos (Mundie, 2014). Tras esta situación se puede observar una desigual relación de poder entre las partes involucradas en el consentimiento, de tal modo que la capacidad de los titulares para oponerse efectivamente al mismo queda en entredicho.

Habría, por tanto, que 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 uno—, como en el funcionamiento de las tecnologías implicadas en la vigilancia. Por un lado, al ser objeto de tratamiento estadístico los datos agregados de diversos individuos que comparten unas características determinadas, ya sean estas demográficas, en función de sus intereses o según el comportamiento que desarrollen, 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 consiguiente el que debe tener la capacidad de otorgar el consentimiento. Por otro lado, cabe argumentar que la eficacia de la oposición a nivel individual resulta muy limitada, por dos motivos fundamentales. El primero se refiere a que la vigilancia sobre una persona puede operar a través de la información que suministran otros, intencionadamente o no, sobre actividades, lugares o intereses que son compartidos, de modo que resulte trivial extrapolar ese conocimiento al individuo opositor. El segundo consiste en que, dado el volumen de actores que intervienen en la economía de la vigilancia, resulta poco operativo que los individuos tengan que estar constantemente mostrando o no su consentimiento, lo cual implica el severo riesgo de que los usuarios acaben aceptando cualquier situación por mero hartazgo.

Resuelta conveniente, en consecuencia, pensar una aproximación colectiva a la privacidad que entienda la desigual relación de poder existente y dote de herramientas de negociación colectiva a los titulares para garantizar la privacidad en el ámbito digital, como ha planteado A. Mantelero (2017). Esto podría pasar por transferir la capacidad de otorgar consentimiento a organizaciones que representen los intereses de privacidad colectivos, de tal modo que la decisión pueda ser realmente informada y en un contexto de negociación en el que pueda darse un reequilibrio de poder. Esto llevaría, muy posiblemente, a que la explotación de datos fuese remunerada y se produjese, al estilo de lo que ocurre con las asociaciones que gestionan los derechos de los autores, un reparto colectivo de los intereses generados por explotación de datos personales. Conviene no confundir esta propuesta con la literatura que defiende entender los datos personales como una

propiedad y aplicar, en consecuencia, la aproximación de propiedad intelectual y una solución mercantilista a la cuestión (véase Ritter & Mayer, 2018).

Si se pudiesen establecer cauces de negociación colectiva, al estilo de las presentes en las relaciones laborales, entre representantes de las diversas industrias interesadas en el tratamiento de datos personales y representantes de los consumidores o asociaciones en defensa de los derechos civiles en Internet, se podría desarrollar una perspectiva de gestión colectiva de la privacidad. Esto podría tener diversas ventajas frente al paradigma individualista actual. En primer lugar, permitiría entender que tras la explotación de los datos personales hay una relación económica que se desarrolla en un contexto asimétrico y con intereses contrapuestos entre generadores y explotadores de datos. A partir de ahí se podrían desarrollar mecanismos para: 1) acordar tarifas que habiliten la recolección y tratamiento de ciertos tipos de datos; 2) gestionar colectivamente los ingresos derivados de la explotación de estos datos; 3) establecer mecanismos de auditoría e inspección sobre los acuerdos de cesión y tratamiento, de tal manera que se garanticen su cumplimiento; y 4) limitar el alcance de los datos recopilados de acuerdo a los fines acordados (minimización de datos).

Esta gestión colectiva permitiría, además, garantizar que no se produjesen asimetrías de privacidad entre los usuarios. En efecto, la tendencia actual en sectores como el de las financias y la actividad aseguradora es la de desarrollar productos que permitan obtener descuentos en los seguros o recomendaciones crediticias a cambio de la instalación de aplicaciones de seguimiento en los *smartphones* de los clientes. De este modo, a través del estudio de la actividad física del individuo, gracias a los datos proporcionados por los sensores del terminal, o el análisis de los movimientos de su cuenta bancaria, a través de aplicaciones ofrecen información en tiempo real sobre los movimientos en la cuenta o interfaces de gestión de su actividad económica; estas empresas obtienen información directa del individuo que son utilizadas para analizar más eficazmente los riesgos que presenta (véase Christl, 2017). En consecuencia, la asimetría de esta relación económica produce una asimetría de privacidad, ya que oponerse a esta clase de vigilancia conlleva un coste económico que, a largo plazo, acabará convirtiendo a la privacidad en un bien de pago.

5. Conclusión

La distinción público/privado ha sido históricamente un tema central en la filosofía política occidental, ya que sobre esta oposición se ha desarrollado el criterio básico para delimitar qué cuestiones son materia de deliberación pública y cuáles deben mantenerse al margen del escrutinio público. No en vano, delimitar el alcance de estos ámbitos ha sido una cuestión altamente controvertida, razón por la que Norberto Bobbio (1998) calificó este par conceptual como una de las «grandes dicotomías» de la historia del pensamiento político y social.

En este contexto, el concepto de privacidad ha ido variando históricamente en función de los problemas que socialmente han marcado la discusión sobre los límites del ámbito privado y, en consecuencia, sobre el alcance legítimo que el secreto debe tener para garantizar que las cuestiones relativas a este ámbito quedasen al margen del escrutinio público, ya fuese este público entendido en el sentido mediático (el que se desarrolla en la esfera pública) o en el sentido político (que opera a través de las administraciones públicas).

El desarrollo de las tecnologías de la información y, en particular, el surgimiento de la informática en conjunción con las redes de datos han supuesto la aparición de nuevas preocupaciones sociales relativas a la imposibilidad de preservar el debido secreto que asiste al ámbito privado. Aquí han sido expuestos tres de los principales temas en los que se basan estos temores, aunque la lista podría ampliarse: cómo el desarrollo de Internet y el crecimiento de los dispositivos interconectados plantean riesgos de ciberseguridad que trascienden el ámbito individual; el desarrollo de una economía de la vigilancia orientada al control sistemático del comportamiento y los afectos de la población; y el proceso de personalización del espacio público digital que hace mermar el principio de visibilidad general de lo público.

Debido a la especificidad de estas nuevas preocupaciones sociotécnicas, y los conflictos políticos que a ellas van asociadas, podemos afirmar que nos encontramos ante un nuevo concepto de privacidad (véase Fernández Barbudo, 2019). A diferencia de lo que ocurría con el de intimidad, este nuevo concepto ya no tiene al individuo en su núcleo fundamental, sino que pone el énfasis en cómo se estructura la visibilidad personal de manera agregada, esto es: cómo se produce y reproduce digitalmente el secreto del ámbito privado e íntimo y, por tanto, cómo se establece la distinción público/privado. De ahí que sea necesario continuar desarrollando una mirada política que comprenda la privacidad como un asunto colectivo antes que individual y, que atienda a las condiciones estructurales que han posibilitado esta transformación sociotécnica.

Bibliografía

Abellán, J. (2007). En torno al objeto de la «historia de los conceptos» de Reinhart Koselleck. En E. Bocardo Crespo (Ed.), *El Giro Contextual: Cinco ensayos de Quentin Skinner, y seis comentarios* (pp. 215–248). Madrid, España: Tecnos.

Arendt, H. (2003). *La condición humana*. Buenos Aires, Argentina: Paidós. (Original publicado en 1958).

Beales, H. (2010). *The value of behavioral targeting*. Washington, Estados Unidos de América: Network Advertising Initiative. Disponible en: https://www.networkadvertising.org/pdfs/Beales_NAI_Study.pdf

Bendrath, R. (2001). The Cyberwar Debate: Perception And Politics In Us Critical Infrastructure Protection. *Information Security*, *7*, pp. 80–103.

Béjar, H. (1990). *El ámbito íntimo. Privacidad, individualismo y modernidad*. Madrid, España: Alianza.

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

Chaum, D. (1985). Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, *28*(10), pp. 1030–1044. doi: http://doi.org/10.1145/4372.4373

Choras, M., Kozik, R., Flizikowski, A., Hołubowicz, W., & Renk, R. (2016). Cyber Threats Impacting Critical Infrastructures. En R. Setola, V. Rosato, E. Kyriakides, & E. Rome (Eds.), *Managing the Complexity of Critical Infrastructures* (pp. 139–162). Cham, Suiza: Springer.

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

Cisco. (2019). *Cisco Visual Networking Index: Forecast and Trends, 2017–2022*. *White Papers*. San José, Estados Unidos de América.

Danezis, G., Domingo-Ferrer, J., Hansen, M., Hoepman, J.-H., Le Metayer, D., Tirtea, R., & Schiffner, S. (2014). *Privacy and Data Protection by Design–from policy to engineering*. Heraklion, Grecia: European Union Agency for Network and Information Security.

Departamento de Seguridad Nacional. (2019). *Estrategia Nacional de Ciberseguridad*. Madrid, España: Ministerio de la Presidencia.

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

Evans, D. (2009). The online advertising industry: Economics, evolution, and privacy. *Journal of Economic Perspectives*, *23*(3), pp. 37–60.

Fernández Barbudo, C. (2019). El nuevo concepto de privacidad: la transformación estructural de la visibilidad. *Revista De Estudios Políticos*, (185), pp. 139–167. doi: http://doi.org/10.18042/cepc/rep.185.05

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

Garzón Valdés, E. (1998). Privacidad y publicidad. *DOXA, Cuadernos De Filosofía Del Derecho*, *1*(21), pp. 223–244.

Goldfarb, A. (2013). What is Different About Online Advertising? *Review of Industrial Organization*, *44*(2), pp. 115–129. doi: http://doi.org/10.1007/s11151-013-9399-3

González Fuster, G. (2014). The Emergence of Personal Data Protection as a Fundamental Right of the EU. Cham, Suiza: Springer.

Habermas, J. (2009). *Historia y critica de la opinión pública*. Barcelona, España: Gustavo Gili. (Original publicado en 1990).

Kim, B.-K. (2005). *Internationalizing the Internet*. Cheltenham, Reino Unido: Edward Elgar Publishing.

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

Langheinrich, M. (2001). Privacy by Design—Principles of Privacy-Aware Ubiquitous Systems. En G. D. Abowd, B. Brumitt, & S. Shafer (Eds.), *Ubicomp 2001: Ubiquitous Computing*, (pp. 273–291). Berlin, Alemania: Heidelberg: Springer Berlin Heidelberg.

Lyon, D. (2019). Surveillance Capitalism, Surveillance Culture and Data Politics. En D. Bigo, I. E, & E. Ruppert (Eds.), *Data Politics. Worlds, Subjects, Rights*, (pp. 64–78). Nueva York, Estados Unidos de América: Routledge.

Manjikian, M. M. (2010). From Global Village to Virtual Battlespace: The Colonizing of the Internet and the Extension of Realpolitik. *International Studies Quarterly*, *54*(2), 381–401. doi: http://doi.org/10.1111/j.1468-2478.2010.00592.x

Mantelero, A. (2017). From Group Privacy to Collective Privacy: Towards a New Dimension of Privacy and Data Protection in the Big Data Era. En L. Taylor, L. Floridi, & B. van der Sloot (Eds.), *Group Privacy: New Challenges of Data Technologies* (pp. 139–158). Cham, Suiza: Springer International Publishing.

Mathison, S. L. (1978). Commercial, legal, and International Aspects of Packet Communications. *Proceedings of the IEEE*, *66*(11), pp. 1527–1539.

Mundie, C. (2014). Privacy Pragmatism. Focus on Data Use, Not Data Collection. *Foreign Affairs*, *93*(2), pp. 28–38.

Pérez Luño, A.-E. (1979). La protección de la intimidad frente a la informática en la Constitución Española de 1978. *Revista De Estudios Políticos*, (9), pp. 59–72.

Powles, J. (2015). The Case That Won't Be Forgotten. *Loyola University Chicago Law Journal*, *47*, pp. 583–615.

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

Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems*, *21*(6), pp. 11–25.

Ritter, J., & Mayer, A. (2018). Regulating data as property: a new construct for moving forward. *Duke Law Technology Review*, *16*(1), pp. 220–277.

Sarigol, E., Garcia, D., & Schweitzer, F. (2014). Online privacy as a collective phenomenon. En *Proceedings of the second ACM conference on Online social networks* (pp. 95–106). Nueva York, Estados Unidos de América: ACM Press. DOI http://doi.org/10.1145/2660460.2660470

Taylor, L., Floridi, L., & van der Sloot, B. (Eds.). (2017). *Group Privacy*. Cham, Suiza: Springer International Publishing. doi: http://doi.org/https://doi.org/10.1007/978-3-319-46608-8

Warren, S. D., & Brandeis, L. D. (1995). *El derecho a la intimidad*. (B. Pendás y P. Baselga, Eds.). Madrid, España: Civitas.

Winston, B. (1998). *Media Technology and Society. A History: From the Telegraph to the Internet.* Nueva York, Estados Unidos de América: Routledge.

Yost, J. R. (2007). A History Of Computer Security Standards. En K. de Leeuw & J. Bergstra (Eds.), *The History of Information Security A Comprehensive Handbook* (pp. 595–621). Ámsterdam, Países Bajos: Elsevier.

Ziegeldorf, J. H., Morchon, O. G., &Wehrle, K. (2014). Privacy in the Internet of Things: threats and challenges. *Security and Communication Networks*, *7*(12), 2728–2742. DOI http://doi.org/10.1002/sec.795

Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, *30*(1), pp. 75–89. doi: http://doi.org/10.1057/jit.2015.5.