

La configuración invisible del espacio digital: el caso de Facebook¹

The invisible setting of digital space: the Facebook case

Lorena Cano-Orón*, Germán Llorca-Abad**

* Universidad de Valencia, España

** Universidad de Valencia, España

Resumen

La neutralidad en la red no existe. El espacio digital puede ser adaptado de forma automática al perfil de cada usuario. Sin que este tenga que identificarse, las empresas de gestión de contenidos en Internet disponen de suficientes datos de cualquier individuo para poder filtrar los resultados de su búsqueda y *personalizarlos*, sin previo aviso, condicionando así su experiencia en la red. Esta investigación, de carácter exploratorio, aborda en primer lugar la descripción del espacio público digital. En segundo lugar, plantea una tipología de espacios digitales que se definen en función del grado de adaptación de los contenidos al usuario. Finalmente, presenta un análisis de caso de espacio social digital personalizado. Concretamente, el estudio se centra en el caso de Facebook y utiliza como referencia el experimento llevado a cabo por la red social Facebook, que implicó la alteración de los contenidos del *News Feed* de 689.000 personas.

Palabras clave: Personalización, espacio público digital, Burbuja de filtros, Facebook, News Feed, algoritmos.

Abstract

Neutrality does not exist in the Internet. The digital space can be automatically adapted to each user's profile. Internet companies can access even with no permission to our personal data, and can adapt content to it customizing our news feed silently, thus determining our web experience. This exploratory research, firstly addresses the description of the digital public space. Secondly, it proposes a typology of digital spaces that are defined by the degree of adaptation of content to the user. Finally, it presents a case study of personalized digital social space. Specifically, the study focuses on the Facebook case and uses as main reference the experiment conducted by the social network Facebook, which involved altering the contents of the News Feed of 689.000 people.

Keywords: Personalization, digital public space, Filter bubble, Facebook, News Feed, algorithm.

Introducción

Internet tiene un enorme protagonismo en la sociedad actual, tanto en el ámbito laboral como en el personal. La esfera digital se está convirtiendo en el espacio público de referencia, al ser ese lugar de reunión en el que no solo encontramos toda la información que necesitamos, sino donde además realizamos aportaciones personales, precisamente por el carácter interactivo que fomenta la red. La cultura de compartir parece formar parte del ADN digital y refiere a la idea de difundir, para todos los públicos, cualquier

¹ Fuente de financiación: Ministerio Español de Economía y Competitividad y fondos FEDER de la Unión Europea

tipo de información que consideremos relevante, ya sea de tipo general o personal (Castells, 2012; Jarvis, 2012; Shirky, 2012; Han, 2013; Llorca-Abad y Cano-Orón, 2015).

Esta forma de comportamiento resulta positiva por muchos motivos. Por ejemplo, por la liberación de una gran cantidad de información y de conocimiento en la red y las oportunidades de creación y colaboración en grandes proyectos (Jarvis, 2012; Shirky, 2012). No obstante, también supone introducir y producir mucha información sobre uno mismo en la esfera digital; lo que supone una pérdida de privacidad inmediata. Esto es debido a la estructura y el funcionamiento *invisible* de la red, que permite registrar con gran precisión los movimientos virtuales del usuario sin su conocimiento explícito. Las causas que explican esta falta de conciencia sobre lo que sucede son múltiples. Es nuestra huella digital², tanto la activa como la pasiva³, la que nos convierte en personas identificables y potencialmente controlables, sobre todo a partir del avance en las tecnologías de extracción de datos en la red.

La actividad que llevamos a cabo en la red puede que no tenga valor a simple vista y esa es, precisamente, la causa por la que no recelamos del acceso que las aplicaciones tienen a nuestros datos. Sin embargo, nuestra actividad diaria en la red genera una información que es muy atractiva para empresas y gobiernos. La falta de formación en el modo en el que utilizamos la red implica que, en general, no sabemos gestionar nuestra privacidad en ella. Y nuestros datos y los de nuestros contactos son capturados, cribados y clasificados por entidades a las que no se los habíamos facilitado en primer término. Y es así como las empresas y los gobiernos obtienen *carta blanca* para explotar el Big Data⁴, es decir, el negocio donde la vigilancia y el mercado se fusionan (Han, 2014).

Por supuesto, el objetivo principal de las empresas privadas de la red es obtener el máximo beneficio. En esta misión, el Big Data colma fielmente sus intereses. Gracias a las correlaciones y segmentaciones de población que posibilita, se hace posible clasificar a los usuarios atendiendo a múltiples variables. Y, una vez están clasificados, ¿qué ocurre? ¿Qué trato especial reciben nuestros datos? ¿Qué puede implicar el seguimiento de la población a partir de su comportamiento en la red? Una de las respuestas es que puede utilizarse dicha información para adaptar los contenidos al usuario a partir de un análisis oculto de su perfil. Esta investigación se centra en analizar dicha personalización involuntaria de los espacios públicos virtuales, que se realiza de forma automática, en función del comportamiento digital y de los datos que generamos al interactuar en la red.

² La huella digital define el conjunto de información sobre nosotros mismos que creamos voluntaria e involuntariamente en Internet. Es decir, toda la información que puede encontrarse en la red de una persona o entidad, que ayuda a proyectar una imagen dicho individuo o empresa, en una página web personal, en los perfiles en redes sociales, comentarios en blogs o foros, imágenes, u otro tipo de publicaciones. También por los procesos que realiza el sistema informático de forma invisible, como la navegación de una web, recibir un e-mail, la geolocalización o dispositivo desde el que realizamos la conexión, etc. Estos datos quedan registrados, aunque no todos están a la vista de cualquier usuario, sino que su acceso requiere del trabajo de un profesional y de programas especializados (Madden *et al.*, 2007).

³ La huella digital pasiva se genera sin que el individuo sea consciente de que la información que está proporcionando vaya a ser almacenada. Es un registro, oculto a simple vista, que deriva de nuestro uso de la web y de toda información que alude directamente a nosotros proporcionada por un tercero. La huella digital activa está formada por la información proporcionada por el usuario sobre su persona de forma voluntaria, como la relativa al perfil de una red social (edad, lugar de nacimiento, residencia actual, estudios, trabajo...), fotografías, música, enlaces compartidos, etc. (Madden *et al.*, 2007).

⁴ El Big Data implica un compendio de herramientas de almacenaje y de procesamiento de grandes volúmenes de información que está aumentando su explotación de forma exponencial. Esto es debido a los beneficios que obtienen las empresas al analizar en profundidad los datos de la red, puesto les permite proyectar comportamientos y avanzar decisiones estratégicas en materia publicitaria, comercial y empresarial.

Espacio público digital

Entendemos el espacio público como un lugar de debate e intercambio de ideas acerca de las cuestiones con interés general, que permite la construcción de una opinión pública. Cuando trasladamos esta idea a Internet, podríamos decir que el concepto de esfera pública digital encajaría en todos los portales web de libre acceso que conforman la red y que tienen como objetivo ser una herramienta para que la ciudadanía pueda, en un sentido generoso, comunicarse, compartir, debatir e intercambiar ideas sobre cualquier cuestión; también las de interés general y/o público.

Internet se presenta como un espacio de comunicación muy flexible en el que multitud de tipos diferentes de formas de comunicar son posibles. También un espacio de espacios en el que se abre una esfera pública digitalizada, mucho más accesible que aquella que permitían las tecnologías que definían las sociedades *massmediáticas*. Se han multiplicado las voces con acceso a los debates de las cuestiones de interés público, donde los productores de la información no son sólo ya las grandes empresas mediáticas, sino también los ciudadanos. Sin embargo, a pesar de toda la literatura positiva al respecto, existe una brecha digital que matiza cualquier apriorismo. Este espacio público digital excluye, de entrada, a aquellas personas que no tienen un nivel económico, o de conocimientos (Llorca-Abad, 2012), suficiente como para formar parte de estos procesos de comunicación. No hay igualdad de condiciones de acceso y uso, incluso a pesar de la flexibilidad mencionada, la gratuidad de muchas herramientas y la aparente facilidad de uso de la web 2.0. Se trata también de un factor condicionante que la gran mayoría de servicios que son accesibles en la red sean propiedad de empresas privadas. No se trata de criticar a la empresa privada, pero no debe obviarse en el análisis que su objetivo prioritario no es el bien común, sino maximizar beneficios, y este detalle es crucial para entender el funcionamiento de la red. Como subraya boyd (2016), Facebook no es un ente benévolo cuya única misión es facilitar la comunicación entre amigos, Facebook es una empresa, y, de alguna forma tiene que sacar sus beneficios.

El espacio público digital ni es neutro ni todas las personas tienen las mismas posibilidades de servirse de él. En Internet no sólo no se resuelve la desigualdad social, sino que incluso cobran más fuerza otros conflictos, como la circulación de rumores, estafas, acoso, delitos cibernéticos, etc.; que se producen porque el infractor sabe cómo utilizar la red en su propio beneficio. En este sentido, debería promoverse la adquisición de las competencias digitales básicas en todas las personas. Por un lado, esto permitiría la toma de conciencia sobre el funcionamiento real de la comunicación en la red y la supuesta experiencia individualizada que promete y, por otro lado, sobre quién tiene acceso y cómo usa nuestra información.

El nuevo espacio público implica un proceso de individuación digital e individualización física, un aislamiento del medio que nos rodea para contextualizarnos en aquello que solo está ocurriendo o se comunica en lo virtual. A la vez, supone un proceso de supuesta socialización a través de dispositivos de todo tipo que posibilitan un estado de hiperconectividad constante. Y esto supone, desde una perspectiva sociológica, que los límites entre la privacidad y el espacio público digital se diluyan.

Un buen ejemplo de este fenómeno es el que sugiere la frase *si no está publicado, es que no ha ocurrido*, puesto que la hiperconectividad implica a su vez una cierta obsesión por la hipervisibilidad; es decir, una suerte de satisfacción de pulsiones escópicas que se canalizan a través de las tecnologías digitales y las formas de comunicación asociadas. Nosotros y nuestros contactos virtuales tendemos a hacer públicos datos que nos identifican y que forman parte en realidad de nuestra vida íntima. Esta actividad sirve para proyectar

una presencia digital que genera un perfil determinado que se ajusta a un *yo ideal*. La idea subyacente es clara: cuanta más visibilidad mejor, cuantos más *me gusta* o cuantos más comentarios, mejor. El filósofo Byung-Chul Han (2013), en la línea de otros autores (Foucault, 1983; Virilio, 1997)⁵, ha acuñado el concepto de *Sociedad de la Exposición* para describir este fenómeno.

El internauta medio crea una identidad digital a partir de la información que sobre él va introduciendo en la red. Esta información incluye estados de ánimo, pensamientos, lugares en los que se encuentra, fotografías de esos lugares, la música que escucha, los libros que lee, las noticias que enlaza y cualquier tipo de recomendación que haga. También incluye datos sobre sus gustos personales, parte de su biografía, lugar de trabajo y residencia, números de teléfono y correos electrónicos (Brake, 2014). Aunque los usuarios son cada vez más conscientes de su privacidad social y, dependiendo del tipo de público que puede acceder a su publicación⁶, publican un tipo de información u otra (Bazarova y Choi, 2014), se descuida la privacidad instrumental y toda la información queda registrada en la misma plataforma. Y esto es como hacer pública una parte de la intimidad que, a la vez que enriquece el *yo digital*, permanece en Internet sin que sea posible tener un control real sobre quién accede y usa esa información (Brake, 2014; Bazarova y Choi, 2014).

Esta difusión de datos contribuye a una pérdida de intimidad (Tello, 2013). Gracias a los avances tecnológicos en el rastreo de información, se han multiplicado las posibilidades de intrusión de terceros en nuestras vidas privadas y de vigilancia de nuestra actividad. Sin ir más lejos, Facebook monitoriza la actividad de los usuarios fuera de su red gracias a la incorporación por parte de terceros del botón 'me gusta' en sus páginas web. El potencial de esta recogida es muy significativo, pues "it can easily link the browsing behavior of its users to their real world identities, social network interactions, offline purchases, and highly sensitive data such as medical information, religion, and sexual and political preferences" (Acar *et al.* 2015: 2). Es por ello que algunas voces (Rheingold, 2004 y Tremblay, 2006) reclaman desde hace tiempo un refuerzo mayor en la protección de nuestra información personal. Un reciente estudio⁷, realizado por miembros de las Universidades de Cambridge y Stanford, ha demostrado que a partir del análisis automatizado de los *me gusta* de Facebook, se obtiene un perfil de la personalidad de las personas mucho más exacto del que puedan tener sus amigos, familiares o incluso parejas sentimentales. Es decir, sólo con los *me gusta* que una persona marca en la red social, un algoritmo es capaz de realizar un perfil psicológico⁸ más fidedigno

⁵ Esta preocupación ha sido estudiada por varios autores a lo largo de los años. Desde Guy Debord en *La sociedad del espectáculo* (2002) o Paul Virilio en *Un paisaje de acontecimientos* (1997), hasta incluso Michel Foucault en *Vigilar y Castigar* (1983), que inciden en la idea de la exposición de la vida íntima de las personas fomentado también por el placer de observar al otro.

⁶ Cuando hablamos de un tipo de público, hacemos referencia a la idea de *contextos sociales colapsados*, es decir, a la descripción de la audiencia en Internet como unos usuarios conectados entre ellos pero pertenecientes a diferentes esferas sociales, las cuales en un plano offline condicionarían el modo de actuación del usuario (Marder *et al.*, 2012; Marwick y Boyd, 2010).

⁷ El estudio realizado por Youyou, Kosinski y Stillwell (2015) utilizó una muestra de 86.220 usuarios voluntarios de Facebook. Los autores emplearon una aplicación, diseñada *ad hoc* para la investigación, que ha demostrado que un programa con acceso a los datos del usuario, generados a partir de su actividad en Facebook, puede definir, con mayor precisión que un humano, rasgos de personalidad de un usuario (gustos, intereses, preferencias, actitudes, etc.). Entre los resultados, destaca que con 150 *me gusta* la precisión de la aplicación para definir rasgos de personalidad de un usuario es igual o superior a la de un familiar; y con 300 *me gusta* llega a superar a una pareja. Si tenemos en cuenta que la media de *me gusta* de Facebook de un usuario es de 227, podemos afirmar que Facebook tiene suficiente capacidad como para conocer, a un nivel muy alto, la forma de actuar de cualquier usuario medio.

⁸ Algunas aplicaciones como <http://appliedmagicsauce.com> de la Universidad de Cambridge permiten construir un perfil psicológico del usuario a partir de la información disponible en las redes sociales en las que tiene una cuenta. Los resultados que ofrece no superan en ocasiones lo anecdótico, pero nos indican la proximidad de herramientas de análisis cada vez más precisas.

del que pudieran realizar sus conocidos reales (Youyou, Kosinski & Stillwell, 2015).

En la conclusión de su trabajo, los autores reparan en los posibles usos que podría tener en el futuro este conocimiento tan afinado de la personalidad de los usuarios. Además de lo que ya se hace, como la personalización de los mensajes publicitarios, destaca el cruce de información sobre la personalidad y la idoneidad del puesto de trabajo. También aventuran que en un futuro “people might abandon their own psychological judgments and rely on computers when making important life decisions, such as choosing activities, career paths, or even romantic partners” (Youyou, Kosinski & Stillwell, 2015: 4). Un futuro que no queda tan lejos. A principios de 2015, la Universidad de Santa Clara en California, lanzó una *app* para ayudar a tomar decisiones éticas⁹. Más allá de lo anecdótico, coincidimos en la preocupación de los autores sobre la necesidad de implementar el control de la huella digital de los usuarios: “knowledge of people’s personalities can also be used to manipulate and influence them” (Youyou, Kosinski & Stillwell, 2015: 4).

El potencial peligro de estos usos no es sólo la gran capacidad de vigilancia que posibilita la estructura de la red, sino también el control sobre lo que piensa el usuario que puede llegar ejercerse sobre él. Cuando estas empresas utilizan los datos generados por el usuario para elaborar un perfil o un patrón de conducta, esta información puede utilizarse para alterar su visión del espacio público, ordenándola según una combinación de intereses del usuario y de la empresa, atendiendo a las características que crean convenientes. De ser así, estaríamos hablando de un control ideológico, de un control mental, que es inconsciente para el usuario.

Personalización y posibles consecuencias

El uso de motores de búsqueda implica, de entrada, *prescindir* de la mayor parte de información contenida en la red, puesto que dichos motores establecen una *selección* a partir de los criterios introducidos. Atendiendo a la variable de acceso a la red, Fornas (2003) distingue tres tipos de Internet: la *Internet global*, que es la información libre a la que podemos tener acceso a través de buscadores y protocolos de internet. La *Internet invisible o profunda*, que es 500 veces mayor que la Internet global (Bergman, 2001)¹⁰, que es la información que no está indexada por los buscadores de forma automática. Se trata de una red también libre a la que podemos acceder desde cualquier ordenador, pero debemos conocer la dirección la URL. La *Internet oscura* es el conjunto de redes restringidas, servidores y redes privadas (hosts), cuya utilización sólo es posible con una autorización o con softwares específicos (Gehl, 2016).

Esta distinción prueba que el acceso a la información de la web es restringido. Asimismo, la búsqueda de información se realiza principalmente de forma individualizada, o personalizada, lo que implica también una limitación al tipo de información a la que se accede. Aquí, entendemos personalización como una forma de filtraje de la información (Bozdog, 2013), un ajuste o modificación de los aspectos de la web que están expuestos al usuario para adecuarse a sus gustos y necesidades (Wu *et al.*, 2003). Por este motivo, la visualización de un espacio público en la red es siempre en función de una acción individual, asociada a un uso también individualizado de datos (Steichen *et al.*, 2012). En última instancia, los resultados de estas

⁹ El acceso a la web se hace a través de la siguiente URL: <http://goo.gl/7uvsPc>

¹⁰ Para profundizar en el conocimiento de esta parte de Internet, referenciamos el artículo de Bergman (2001).

búsquedas y acciones pueden ser involuntarios. Tal y como hemos sugerido, las empresas proveedoras de acceso y servicios a la web pueden utilizar la información personal de cada usuario para presentar una información *más allá* de su voluntad consciente. En otras palabras, los resultados de las búsquedas de información están condicionados por la estructura de metadatos y funcionamiento de la web.

Resultados de búsqueda *no deseados*. Personalización involuntaria¹¹

La digitalización de la información ha permitido que ingentes cantidades de datos puedan almacenarse, transmitirse y procesarse fácilmente. En este sentido, es relativamente sencillo para las empresas de gestión de datos y tráfico web introducir un sesgo en la información a la que accedemos. Este sesgo se elabora a partir del análisis de la información personal que hemos *cedido* a partir de nuestra actividad web. Así, el acceso a través de diferentes modos al espacio público digital es, en realidad, el acceso a unos entornos cuyo contenido ha sido *diseñado* sin el consentimiento explícito del usuario. Los motores de búsqueda de la web, y algunas redes sociales como Facebook, elaboran perfiles de usuario a partir de las distintas variables sobre las que el usuario no tiene ningún control.

Este tipo de personalización no tiene porqué estar relacionada únicamente con los perfiles que se hayan creado, sino que en ocasiones tiene en cuenta otras variables como la localización desde donde se está consultando la información. La idea de que Internet nos conecta con todo el mundo por igual, sin filtros y que ofrece una información plural, creando un espacio democrático, sencillamente, no es real y es una interpretación ideológica interesada. La esfera pública digital está adaptada a cada usuario, es decir, pierde su característica de pública o general para pasar a ser muy individual. Como afirma Eli Pariser (2011), se trata de un universo único de información para cada uno de nosotros, una "burbuja filtrada" que altera la forma en la que (per)recibimos la información¹².

Podría denominarse también personalización implícita o pasiva, puesto que se recrea una perspectiva del espacio público digital adaptada para el usuario sin que éste lo haya pedido. Algunos ejemplos sobre cómo se lleva a cabo este tipo de personalización son las recomendaciones basadas en el historial del usuario, o en su comportamiento en una red social; la adecuación de los contenidos basados en su posición geográfica, o la ordenación jerárquica de los contenidos atendiendo al número de visitas o *me gusta*. En el caso de los *me gusta* se trataría de un sesgo basado en la popularidad (Thurman y Schifferes, 2012)¹³.

Google ofrece resultados distintos para cada usuario aún cuando la búsqueda se haya realizado a partir de las mismas palabras clave. Esto es debido a que "Google usa varias 'señales' para personalizar búsquedas, incluyendo la localización, palabras clave de búsquedas previas y contactos recientes en un usuario de red

¹¹ Una cuestión relacionada directamente con este tipo de personalización, pero que excede los límites de este trabajo, es la personalización de los anuncios en Internet a partir de datos personales de los usuarios y el análisis de big data. Un tema que cada vez se investiga más, sobre todo por empresas cuya economía se sustenta principalmente en ello, porque está más que demostrada su efectividad (Li, 2015; Köster et al., 2015).

¹² Pariser (2011: 9 y 10) destaca tres características de este tipo de personalización involuntaria: En primer lugar, la soledad o singularidad de la burbuja; ya que cada visión está adecuada al usuario específicamente. En segundo lugar, la invisibilidad; porque, como hemos comentado anteriormente, no somos conscientes del nivel de adaptación de los contenidos. Y, en tercer lugar, la no-elección de estar en la burbuja.

¹³ Un concepto similar al que estamos abordando en este artículo es la 'ilusión de conocimiento' (Müller et al., 2016) que se genera al estar expuesto a una abundancia de noticias dentro de una burbuja mediática, es decir, sesgada bien sea por el idioma desde el que se consultan, la zona geográfica o la selección de información de determinadas cabeceras mediáticas. El usuario se siente informado porque ha estado expuesto a una agenda mediática determinada.

social” (Bozdag, 2013: 211). De esta manera Google puede predecir qué es relevante para el usuario, utilizando filtros que sesgan la información para ofrecerle los resultados que, según la propia Google, más le interesan al usuario (Bozdag, 2013).

Por su parte, Facebook tiene en cuenta para jerarquizar la información que le muestra al usuario variables como la interacción entre los usuarios (los *me gusta* que han marcado, los contenidos que han compartido, los comentarios en las fotografías o en los posts, etc.). La empresa identifica esta información como signo de interés de un usuario en otro y, como consecuencia, prioriza las novedades de estos contactos en la sección principal de la plataforma. Si no se mantiene ningún tipo de interacción con un contacto, su información permanecerá oculta del *News Feed* del usuario de manera automática e involuntaria (Bozdag, 2013). No obstante, hay que señalar que este algoritmo no obedece a parámetros estáticos, es dinámico, invisible y se adapta a las características de cada usuario (Tufekci, 2015; Bucher, 2012). Asimismo, la empresa continúa investigando y cambiando las variables que le hacen al algoritmo detectar ese interés del usuario (en el último apartado profundizamos en esta cuestión).

Este tipo de sesgos son realizados de forma automática mediante algoritmos que acaban tomando decisiones subjetivas, en las que no hay una respuesta correcta, como seleccionar la información que le puede interesar a alguien. Este tipo de algoritmos, invisibles al ojo humano, juegan un papel de editor de la información que consume el usuario: filtran, destacan, suprimen y en última instancia determinan la información que le interesa. Los principales efectos negativos de estas lógicas reguladoras son la falta de visibilidad, la asimetría de la información y la influencia oculta. Aunque como señala Tufekci (2015), el principal problema no es que influyan en esferas sociales e interpersonales, sino que también actúan en esferas políticas y cívicas. Desde el contexto académico, las principales preocupaciones que se destacan cuando se aborda este tema son los efectos del sesgo, la discriminación, la justicia, la distribución de la visibilidad, la vigilancia y la responsabilidad (Ziewitz, 2016).

Desde que Pariser (2011) publicó su teoría sobre la burbuja de filtros, esta característica ha recibido atención por los medios, la industria y la academia. Este mecanismo es principalmente criticado por la limitación de la autonomía del usuario y su capacidad de elección y por la reducción de la calidad de la información y capacidad de deliberación. Ante esta situación, varios desarrolladores han creado herramientas capaces de romper la burbuja de filtros¹⁴. Como explica Bozdag y van den Hoven (2015), algunas les dan al usuario el control completo para incluso aumentar el filtrado y otras modifican los resultados de búsqueda para asegurar la diversidad, aunque sin notificar al usuario. No obstante, también muchos activistas recomiendan prácticas quizá tediosas para el usuario pero efectivas, como eliminar el historial de búsqueda, borrar las cookies, usar el modo de búsqueda de incógnito o realizar búsquedas desinteresadas con el objetivo de ‘marear’ al algoritmo. (Bozdag y van den Hoven, 2015)

¹⁴ Ejemplos de este tipo de software son: *Balancer*, que tiene como misión informar al usuario de sus hábitos de lectura y los sesgos que realiza, realizando un seguimiento de su historial; *Scoopinion*, un plugin que realiza un seguimiento de los portales de noticias que visita el usuario y le devuelve un informe para que sea consciente; o, *Bobble*, permite al usuario comparar los resultados de búsqueda de Google con otros perfiles de usuario según la geografía (Bozdag y van den Hoven, 2015).

Personalización solo voluntaria

La personalización voluntaria de los contenidos a los que el usuario accede a través de la red podría entenderse en términos de construcción del espacio público propio, es decir, la configuración deliberada de las fuentes de información online que se usan. "El proceso de personalización al que puede llegar el usuario en Internet es máximo, puesto que parte de la máxima selección posible (...) y, además, cuenta con casi total libertad para ir moviéndose de un espacio a otro en busca de la información que más le interese" (López García, 2005: 49).

Ejemplos de esta clase de personalización, que también podríamos denominarla como personalización activa debido a la decisión libre y decidida del usuario de ejercer este tipo de caracterización de su espacio, son los *newsletters* que los usuarios solicitan marcando las áreas de interés de las que quiere recibir información de forma periódica. También se considera personalización activa o explícita cuando el usuario decide *customizar* la página principal de las webs de noticias con las secciones y periodistas con los que prefiere informarse, o las aplicaciones móviles o *widgets* que permiten filtrar la recepción de noticias atendiendo a las preferencias que el usuario le ha añadido, como pueda ser la localización, los temas de interés, etc. (Thurman y Schifferes, 2012).

Según Cass Sunstein (2003), la posibilidad de poder personalizar el espacio público de acuerdo a los gustos e intereses de los usuarios puede suponer un peligro para la concepción de esfera pública que se forma, al no estar expuesto al conjunto de la sociedad. El hecho de que sea posible estar en contacto con solo aquello que se quiere ver, leer y escuchar, dejando a un lado aquellas opiniones y temas que no interesan pueden suponer un gran problema para la construcción de una sociedad democrática común. Sunstein (2003) sostiene además que este tipo de acciones provoca la polarización del espacio público y la radicalización de las ideologías. Cuando el individuo no está expuesto a la variedad tanto social como informacional, cualquier tipo de debate será siempre con ideas afines que reforzarán sus creencias y su visión social acabará reduciéndose a una postura extrema debido a la falta de contacto con la diversidad. Esta tendencia pone al civismo democrático en peligro en la nueva sociedad red, ya que "la revolución cognitiva atribuida a Internet puede devenir en auténtica involución cognitiva si finalmente las únicas fuentes de información del mundo son las que extraemos del ciberespacio o del espacio audiovisual tras haber seleccionado estrictamente el tipo de información que previamente deseábamos recibir" (Gozálvez, 2011: 1).

El nuevo espacio digital conlleva, además de indudables beneficios, varios peligros potenciales, sobre todo desde la perspectiva de la privacidad. La satisfacción de la pulsión escópica de los usuarios en los entornos digitales, les otorga más visibilidad y protagonismo, pero también un mayor grado de vulnerabilidad respecto a la protección de su privacidad e intimidad. Mediante el rastro o huella digital que dejan los usuarios de Internet, las *cookies* y otros programas araña y las distintas metodologías de extracción de datos, la vigilancia líquida de la que hablan Bauman y Lyon (2013) se hace plenamente plausible. Y desde una perspectiva cognitiva, hay que tener en cuenta las consecuencias que podría llegar a tener la personalización voluntaria del espacio público digital, ya que una visión sesgada del mundo puede traer peligros que no son precisamente nuevos.

Personalización de espacios en redes sociales: el caso de Facebook

Es poco frecuente que compañías como Google o Facebook hablen del modo en el que analizan y usan el Big Data acumulado en sus servidores, relativo a la información personal de los usuarios. Menos frecuente aún es que hagan público un estudio acerca de las investigaciones que llevan a cabo en la manipulación de los *News Feed* de sus entornos de uso¹⁵. En junio de 2014 se daba a conocer el experimento llevado a cabo por Facebook consistente en la alteración invisible del *News Feed* de 689.003 usuarios. Dicha alteración, supuso la priorización de contenidos positivos o negativos en los *News Feed* de estos usuarios y estaba encaminada a determinar si era posible llevar a cabo un contagio emocional a gran escala. Los resultados, estudiados por Kramer, Guillory y Hancock (2014), no ofrecen lugar a dudas: fue posible y se demostró así la capacidad de manipulación sobre los contenidos¹⁶.

Tal y como señalan los autores del análisis en el planteamiento inicial, el estudio de la transferencia emocional de una persona a otra está bien documentado en la literatura psicológica y en diferentes experimentos de laboratorio llevados a cabo desde hace algunas décadas. La novedad de esta aproximación radica, entre otras, en la enorme escala del experimento y la total falta de conciencia por parte de los sujetos de estar siendo sometidos a un estudio. El factor de mediación tecnológica, así como de otros condicionantes que tendremos en cuenta más adelante, no debe ser menospreciado.

Las variaciones en el comportamiento de los sujetos del experimento son claras: "The results show emotional contagion. [...] For people who had positive content reduced in their News Feed, a larger percentage of words in people's status updates were negative and a smaller percentage were positive. When negativity was reduced, the opposite pattern occurred" (Kramer, Guillory y Hancock, 2014: 8789). Esta contundencia abre la puerta a muchas especulaciones, pero también a la descripción de algunas certezas. Si es posible alterar el contenido que los usuarios acceden en la web y si es posible alterar el estado emocional a través de esa manipulación, se anticipa una era en la que será muy difícil saber si aquello que pensamos y sabemos, o creemos pensar y saber, es fruto de nuestra actividad autónoma como animales racionales o no.

Hirsh, Kang y Bodenhausen (2012) emplean el concepto de estrategias de comunicación "personality-based" para describir lo que sucede cuando se intenta manipular a un sujeto mediante la adecuación a su perfil psicológico de los mensajes que recibe. De nuevo advertimos que este tipo de investigaciones no son nuevas en el campo de la psicología, pero sí lo son desde el punto de vista del ámbito de experimentación implicado. Se invierte cada vez más en experimentación e investigación en ámbitos de la psicología, la comunicación y la neurociencia para crear nuevas herramientas que sean capaces de manipular la atención y la actitud de los usuarios hacia determinados productos (boyd, 2016).

¹⁵ Es difícil hablar de frecuencias y de coincidencias, puesto que las redes sociales, especialmente Facebook, frecuentan la actualidad noticiosa, justamente, con noticias relacionadas con sus prácticas *no confesadas*: "Un informe acusa a Facebook de rastrear a los internautas ilegalmente", en <http://goo.gl/dDMz8s> y "Facebook hace frente a una demanda masiva por uso de datos privados", en <http://goo.gl/a3qlxt>. Que Facebook publique un artículo académico sobre estas cuestiones y que en él se especifique que se ha demostrado que el contagio emocional en Facebook funciona, es, sin duda, una contribución más al mundo académico pero quizá es de mayor interés para sus inversores y para el sector publicitario.

¹⁶ En el artículo, los autores afirman que el algoritmo que ejerce de filtro en la sección de últimas noticias (*News Feed*) está en constante desarrollo y hacen explícito el hecho de que esta investigación sobre contagio emocional ha sido, simplemente, *una* prueba más.

Aquí debe plantearse una pregunta: ¿hasta qué punto son conscientes los usuarios de cualquier aplicación informática de la capacidad de sus gestores para manipular el contenido al que acceden? Aquí también se plantea una paradoja que es que, contrariamente a lo que podría deducirse, Facebook, así como otras redes sociales y aplicaciones, no oculta a sus usuarios que en el *News Feed* se muestran prioritariamente las historias de los contactos con los que más se interactúa: “El número de comentarios y *me gusta* que recibe una publicación y el tipo de historia que es (por ejemplo, foto, video o actualización de estado) también pueden aumentar las probabilidades de que aparezca en la sección de noticias”¹⁷. Lo que no se dice es que la compañía tiene la capacidad de utilizar los datos personales de los usuarios para manipular también la prioridad en la que vemos la información.¹⁸

Es por este motivo que debemos considerar otra línea de aproximación. La cultura acerca de los riesgos que corremos al proyectarnos digitalmente es muy escasa. ¿Quién lee los acuerdos de uso y privacidad, o declaraciones de derechos y responsabilidades, de los datos que cedemos cuando usamos una aplicación? Un reciente estudio llevado a cabo por Durán y Mejías (2014) sobre el conocimiento y comportamiento de los usuarios respecto a las redes sociales, alumbraba el hecho de que aproximadamente el 70% de los usuarios de Facebook no había leído nunca la política de privacidad. Esto, sumado al conocimiento real que tienen las empresas de los usuarios de sus servicios, resulta en un combinado altamente explosivo.

Lanier (2014: 356 y ss.) ha expuesto que como usuarios de la red nos enfrentamos a tres problemas “desasossegantes”, a saber la privacidad, la identidad y la seguridad. Los tres “tienen largas historias a sus espaldas, pero son ahora catastróficamente más confusos debido al *Big Data* y a los efectos de red [...]. Hay una creciente fauna de poderosos intereses remotos que, deseosos de tomar el control de nuestra vida informacional, promueven estos tres aspectos desasossegantes”. Lo que el autor propone es implementar una cultura de uso consciente de las herramientas de intermediación con la Internet, es decir, una actitud activa hacia los potenciales peligros que encierra la falta de prevención que, como usuarios, se da con demasiada frecuencia.

Como señala boyd (2016), este experimento es un ejemplo y no debe distraernos de lo que ejemplifica: no se trata de Facebook o de su grupo de investigación, sino de reflexionar sobre cómo hacer que las empresas sean responsables ante este tipo de acciones que dicen tomar en beneficio del usuario. boyd (2016) afirma que más allá de la ausencia o presencia de ética en la investigación llevada a cabo por Facebook, que no es la primera en publicarse (Puschmann y Bozdog, 2014)¹⁹, pero sí que es la que ha tenido repercusión mundial, lo que más ha calado en la población es la investigación con sus datos: “There is a growing amount of negative sentiment towards Facebook and other companies that collect and use data about people. This study provided ammunition for people’s anger about “big data” because it’s so hard to talk about harm in the abstract.” (boyd, 2016: 11)

A este respecto Lanier (2014: 357) explica: “*Google* quiere que seamos ‘abiertos’ para poder rastrear todos los datos relacionados con nosotros, incluso si inicialmente no los introdujimos a través de alguno de sus servicios. Pero *Google* también quiere ser cerrado respecto a los métodos que emplea para recopilar nuestra

¹⁷ Facebook; funcionamiento de la sección “Últimas noticias”. En <http://goo.gl/Mv0br6>

¹⁸ Cabe mencionar que en marzo de 2016 Instagram, otra plataforma de la compañía de Facebook, anunció la implementación de un algoritmo personalizado (similar al funcionamiento del NewsFeed) y que los usuarios no reaccionaron tampoco bien a la noticia (Skrubbeltrang, Grunnet y Tarp, 2017).

¹⁹ Pueden consultarse trabajos científicos referidos a otros experimentos de Facebook publicados por Das y Kramer (2013), Taylor et al. (2013), Bakshy et al. (2013), Bakshy et al. (2012) o Bond et al. (2012) en los que se ha investigado sobre la autocensura, la publicidad personalizada y la influencia del voto, entre otros aspectos.

información y sacar provecho de ella. Facebook quiere que tengamos una sola identidad, para que sea más fácil acumular información a nuestro alrededor e influir sobre las opciones que se nos presentan, pero al mismo tiempo no quiere difundir cómo se utiliza nuestra información (ni que *Google* tenga acceso a ella)". El panorama se presenta, pues, desalentador.

Cuando existen sólidas evidencias de que es posible alterar la percepción de lo que creemos que es público en el ámbito digital, así como de lo que es privado y cuando sabemos que las compañías tienen acceso a nuestros datos personales, deben plantearse aún muchas más preguntas. En febrero de 2015 el Ministerio de Hacienda español anunció el inicio del uso de programas espía que debían servir para rastrear nuestra huella digital²⁰. Esta iniciativa estaría encaminada a luchar contra el fraude fiscal, pero estaría aprovechándose de la enorme laguna legal que existe respecto a la protección de los datos personales de los usuarios de Internet²¹.

El problema no es privativo de ningún país en concreto. Tal y como defiende el crítico de la tecnología Evgeny Morozov (2012; 2013), las compañías radicadas en Silicon Valley colaboran en el desarrollo de sofisticados algoritmos de análisis que permiten un mayor control policial sobre la población, con planteamientos cercanos a la ciencia ficción. "Companies like *Facebook* have begun using algorithms and historical data to predict which of their users might commit crimes using their services" (Morozov, 2013: 186). Es decir, obviando las lógicas diferencias, hablamos en realidad de una situación muy próxima a la planteada en el film *Minority Report*²², en el que la policía detiene a los criminales antes de que lleven a cabo sus fechorías²³. "In many respects, Internet companies are in a much better position to predict crime than police" (Morozov, 2013: 197).

Con toda seguridad, no se trata de menospreciar sin matices los posibles beneficios de este tipo de tecnologías. Pero, de nuevo, se plantea la cuestión de hasta qué punto debe ser víctima de estos procesos un usuario no informado e inconsciente de la invasión de su privacidad. Que determinadas webs no permitan el control sobre las *cookies* que alojan en nuestros servidores²⁴, o que solo sea posible deshacerse de cierto *malware* destruyendo físicamente el disco duro de nuestros dispositivos²⁵, nos aproxima a tesituras de tintes dictatoriales debido a un desequilibrio creciente de poder (Lanier, 2014: 375) contra las que sin duda hay que empezar estar prevenidos. Como afirma Gehl (2016), hay que tener en cuenta que las redes sociales implican libertad para el usuario: referida esta a la posibilidad de publicación, producción, organización y socialización; pero también poder para la empresa, pues tiene absoluta capacidad para ejercer la vigilancia

²⁰ La Agencia Tributaria del Gobierno de España especifica que tiene previsto cruzar más de 200.000 dominios para incorporarlo a sus bases de datos. Asimismo también afirma poner en funcionamiento la identificación de patrones de comportamiento que se correspondan con actividades defraudadoras. Nota de prensa: <http://goo.gl/FF1xwK>

²¹A nivel europeo, la regulación principal de protección de datos, la Directiva 95/46/CE, data de 1995. Desde entonces, el ecosistema digital ha cambiado y avanzado de forma considerable. Tanto la Comisión Barroso II (2009-2014) como el Supervisor Europeo de Protección de datos coinciden en que es necesario un mayor fortalecimiento de la legislación y una concienciación del control de los datos por parte del individuo. Dicha Comisión presentó una propuesta de reforma legislativa que fue aprobada por el Parlamento Europeo pero aún está a expensas de ser aprobada por el Consejo para su entrada en vigor: <http://goo.gl/ZArUPM>

²² Película del realizador Steven Spielberg realizada en 2002.

²³ También podemos ver en dicho film el ejemplo de espacio personalizado involuntariamente. En la ficción, el entorno – sobre todo la publicidad- identifica a los individuos y se adapta. De hecho, el personaje protagonista se ve obligado a desfigurarse la cara y a trasplantarse los ojos para poder moverse por la ciudad sin ser reconocido por el sistema.

²⁴ "Las web no dan control total sobre las 'cookies' que instalan en el ordenador"; noticia publicada en *El País.es* en febrero de 2015. Accesible en este enlace <http://goo.gl/2EZQ0K>

²⁵Artículo de la periodista de tecnología Lily Han Newman, publicado en *Slate.com* en febrero de 2015: "Smashing Your Hard Drive Is the Only Way to Get Rid of This Awful Spyware". Disponible en el enlace <http://goo.gl/7VcVsr>

de sus usuarios, para regular la información mediante algoritmos y para establecer los límites estructurales de la plataforma.

Desde la comunidad académica se ha criticado el experimento de contagio emocional de Facebook principalmente desde dos perspectivas: la ética, por los posibles daños causados a los usuarios, y la legalidad, por la ausencia de un consentimiento verdaderamente informado por parte de los usuarios (boyd, 2016). La respuesta por parte de la empresa, la editora de la publicación y los autores del trabajo ante las críticas recibidas no se hizo esperar: la editora de la revista publicó una corrección²⁶ y el autor principal pidió perdón²⁷ y un alto cargo de Facebook también se disculpó en nombre de la empresa por la falta de comunicación a los usuarios²⁸ (Flick, 2016).

El hecho de que Facebook se acogiese a su política de tratamiento de los datos para justificar su investigación sólo ha conseguido que aumente la preocupación sobre la ética de la investigación (Chan, 2015). Y es que una de las cosas que más se ataca no es el análisis de big data o de la información de los usuarios, sino la manipulación del entorno particular de cada usuario sujeto de ese estudio sin previo aviso (Jouhki, 2016). Tal es la consternación que ha causado la magnitud de este experimento, que autores como Recuber (2015), llegan a comparar a los investigadores de Facebook con Milgram²⁹ o Zimbardo³⁰, dejándolos incluso en una peor posición en cuanto al trato hacia los sujetos estudiados.

Aunque el argumento más utilizado para justificar este tipo de acciones que comete Facebook cuando quiere es que es una empresa privada y que los usuarios han aceptado formar parte de ella libremente y con unas condiciones concretas por delante. Y es que, como señala boyd (2016) el verdadero producto de Facebook, más allá de sus usuarios, es su capacidad de captar la atención de los usuarios y conseguir que abandonen un *estado pasivo* para interactuar en la red. Para que exista algún tipo de regulación que impida a este tipo de empresas manipular y experimentar con sus usuarios, como señala Schroeder (2014: 9), consistiría en entender Internet y sus espacios sociales como "part of an essential infrastructure for citizens, along similar lines as broadcast, communication via phone, energy or transport".

Conclusiones

La tecnología, en un sentido laxo, lo impregna todo. La tecnología media en la relación que las personas establecen con su entorno y de forma especial en el ámbito de la comunicación. Sin duda, la tecnología es, al mismo tiempo, el resultado del potencial creativo del ser humano y un potenciador de sus capacidades y limitaciones. Pero como advertiera Paul Virilio, la invención de toda tecnología conlleva la invención de su accidente específico. La invención del tren supuso también la invención del descarrilamiento, así como la invención del barco supuso la invención del hundimiento. Mientras los accidentes asociados a estas tecnologías tenían un ámbito local, el accidente de las tecnologías digitales de la comunicación tendría un alcance planetario (Virilio, 1997).

²⁶ <http://www.pnas.org/content/111/29/10779.1.full>

²⁷ <https://www.facebook.com/akramer/posts/10152987150867796>

²⁸ <https://www.theguardian.com/technology/2014/jul/02/facebook-apologises-psychological-experiments-on-users>

²⁹ Referencia original del estudio: Milgram, S. (1963). Behavioral study of obedience. *Journal of Abnormal and Social Psychology*, 67(4), 371–378.

³⁰ Referencia original del estudio: Haney, C., Banks, W. C., & Zimbardo, P. G. (1973). A study of prisoners and guards in a simulated prison. *Naval research reviews*, 9, 1-17.

El metarrelato proyectado sobre la cibercomunicación es tendenciosamente positivo. Sin denostar el potencial beneficioso de Internet y de todas las aplicaciones de comunicación que utilizamos diariamente, se da una enorme falta de conciencia de los peligros de ceder una parte de nuestra información personal a unas empresas que no garantizan un uso respetuoso de las mismas. Existen pruebas de que dichas empresas, a través del análisis del *Big Data*, emplean la información obtenida de forma, como mínimo, éticamente cuestionable. El control absoluto que ejercen, o pueden ejercer, sobre los contenidos e informaciones a las que accedemos a través de las aplicaciones informáticas, debería ser una alerta de prevención a los excesos de intromisión en la vida privada de las personas que empiezan a cometerse.

Internet acerca lo que está lejos, pero nos aleja de lo que está cerca. Tal y como hemos visto en la primera parte de nuestro trabajo, el uso de la red se asienta en una extrema hipercomunicabilidad que nos aísla de nuestro entorno inmediato. Esta falta de contexto, sumada a la inconsciencia con la que por lo general nos entregamos al uso de las tecnologías de la comunicación digital, propicia el aprovechamiento de nuestros datos con fines comerciales o de control. Tal y como demuestran los experimentos referidos en este trabajo, ya es posible manipular estados de ánimo e influir de forma invisible en las actitudes de las personas en una escala sin precedentes en la historia de la comunicación. La diferencia con el antiguo paradigma mediático radica en la absoluta invisibilidad de todo el proceso y en el aislamiento del sujeto en todo el proceso comunicativo.

Es como si alguien pretendiera programar nuestras conciencias sin que nos diéramos cuenta. Tal y como ha advertido Lanier en sus trabajos, corremos el riesgo de diluirnos en la red. Corremos el riesgo de perder nuestra definición compleja en tanto que personas, puesto que no somos plenamente conscientes del alcance del problema. La supuesta libertad de la red es una libertad altamente tecnificada y vigilada, en la que, siguiendo con la terminología viriliana, solo unos pocos privilegiados tienen acceso al paisaje de acontecimientos y, consecuentemente, detentan el control de la situación.

Las continuas mejoras en la programación algorítmica permiten aventurar la próxima capacidad de anticiparse incluso a nuestras acciones. Este tipo de experimentación algorítmica, de manipulación, adecuación, y personalización del espacio público digital, coincide con las técnicas psicopolíticas descritas por Byung Chul Han³¹, por lo que podríamos llegar a afirmar que estamos siendo reprogramados o preprogramados en función de unos intereses que nos son completamente ajenos. También, que las redes sociales como Facebook, o cualquier espacio web con sus mismas características, tiene la capacidad de analizarnos, clasificarnos, controlarnos e incluso influir en cómo nos sentimos. Una situación de tintes apocalípticos que nos dice que poco o nada hemos aprendido de los errores del pasado.

Bibliografía

ACAR, G., VAN ALSENOY, B., PIESSENS, F., DIAZ, C., & PRENEEL, B. (2015). Facebook Tracking Through Social Plugins. Disponible en <https://goo.gl/PbUjk4>

³¹ "La óptica digital posibilita la vigilancia desde todos los ángulos" (Han, 2014: 86), es capaz de llegar a la psique, de actuar desde un nivel prerreflexivo, trabajando con las emociones para influir en las acciones.

- BAZAROVA, N. N., & CHOI, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication, 64*(4), 635-657.
- BAUMAN, Z. Y LYON, D. (2013). *Vigilancia líquida*. Buenos Aires: Paidós.
- BAKSHY E., ECKLES D., YAN R., ROSENN I. (2013). Social Influence in Social Advertising: Evidence from Field Experiments. *Proceedings of the 13th ACM Conference on Electronic Commerce* (pp. 146-161).
- BAKSHY E., ROSENN I., MARLOW C., ADAMIC L. (2012). The Role of Social Networks in Information Diffusion. *Proceedings of the 21st international conference on World Wide Web* (pp. 519-528)
- BERGMAN, M. K. (2001). White paper: the deep web: surfacing hidden value. *Journal of electronic publishing, 7*(1). Disponible en <https://goo.gl/7qe89g>
- BOND, R. M., FARISS, C. J., JONES, J. J., KRAMER, A. D. I., MARLOW, C., SETTLE, J. E., & FOWLER, J. H. (2012). A 61-million-person experiment in social influence and political mobilization. *Nature, 489*(7415), 295–298. doi:10.1038/nature11421
- BOYD, D. (2016). Untangling research and practice: What Facebook's "emotional contagion" study teaches us. *Research Ethics, 12*(1), 4–13.
- BOZDAG, E. (2013). Bias in algorithmic filtering and personalization. *Ethics and information technology, 15*(3), 209-227.
- BOZDAG, E., & VAN DEN HOVEN, J. (2015). Breaking the filter bubble: democracy and design. *Ethics and Information Technology, 17*(4), 249-265.
- BRAKE, D. R. (2014). *Sharing Our Lives Online: Risks and Exposure in Social Media*. Palgrave Macmillan.
- Bucher, T. (2012). Want to be on the top? Algorithmic power and the threat of invisibility on Facebook. *new media & society, 14*(7), 1164-1180.
- CASTELLS, M. (2012). *Redes de indignación y esperanza: los movimientos sociales en la era Internet*. Madrid: Alianza.
- CHAN, A. (2015). Big data interfaces and the problem of inclusion. *Media, Culture & Society, 37*(7), 1078-1083.
- DAS S. Y KRAMER A. (2013). Self-Censorship on Facebook. *Proceedings of the Seventh International AAAI Conference on Weblogs and Social Media (ICWSM)*. Palo Alto, CA: The AAAI Press.
- DURÁN, M. Y MEJÍAS, J.F. (2014). Conocimientos y comportamientos de los usuarios de la red social Facebook relacionados con la privacidad. *Ámbitos, 26*. [Consultado el 2 de enero 2015]. Disponible <http://goo.gl/ofQuSJ>
- FERRARA, E., & YANG, Z. (2015). Measuring emotional contagion in social media. *PloS one, 10*(11), e0142390.
- FLICK, C. (2016). Informed consent and the Facebook emotional manipulation study. *Research Ethics, 12*(1), 14-28.
- FORNAS CARRASCO, R. (2003). La cara oculta de Internet [en línea]. *Hipertext.net, 1*. [Consultado el 6 de Enero 2015]. Disponible <http://goo.gl/G6DMkh>
- FOUCAULT, M. (1983). *Vigilar y castigar: nacimiento de la prisión*. México: Siglo XXI.
- GEHL, R. W. (2014). Power/freedom on the dark web: A digital ethnography of the Dark Web Social Network. *New Media & Society, 1*-17.
- GOZÁLVEZ PÉREZ, V. (2011). Educación cívica en la cultura digital. Una aproximación crítica a la socialización-en-red. *Revista Iberoamericana de Educación, 55*(2), 10.

- HAN, B-C. (2013). *La sociedad de la transparencia*. Barcelona: Herder.
- HAN, B-C. (2014). *Psicopolítica*. Barcelona: Herder.
- HIRSH, J.B; KANG, S.K. Y BODENHAUSEN, G.V. (2012). Personalized persuasion: tailoring persuasive appeals to recipients' personality traits. *Psychological Science*, 23, 6, 578–581 [Consultado el 29 de enero de 2015]. Disponible <http://goo.gl/xAqZnf>
- JARVIS, J. (2012). *Partes públicas. Por qué compartir en la era digital mejora nuestra manera de trabajar y vivir*. Barcelona: Gestión 2000.
- JOUHKI, J., LAUK, E., PENTTINEN, M., SORMANEN, N., & USKALI, T. (2016). Facebook's emotional contagion experiment as a challenge to research ethics. *Media and Communication*, 4(4), 75-85.
- KÖSTER, M., RÜTH, M., HAMBORG, K. C., & KASPAR, K. (2015). Effects of personalized banner ads on visual attention and recognition memory. *Applied Cognitive Psychology*, 29(2), 181-192.
- KRAMER, D.I.A.; GUILLORY, J.E. Y HANCOCK, J.T. (2014). Experimental evidence of massive-scale emotional contagion through social networks. *Proceedings of the National Academy of Sciences*, 111, 24, 8788–8790. [Consultado el 2 de febrero 2015] Disponible <http://goo.gl/XDgrCt>
- LANIER, J. (2014). *¿Quién controla el futuro?* Barcelona: Debate.
- LI, C. (2016). When does web-based personalization really work? The distinction between actual personalization and perceived personalization. *Computers in Human Behavior*, 54, 25-33.
- LLORCA-ABAD, G. Y CANO-ORÓN, L. (2016). Espacio y tiempo en el siglo XXI: velocidad, instantaneidad y su repercusión en la comunicación humana. *Revista ComHumanitas*, 6(1), 219-233.
- LLORCA-ABAD, G. (2012). Exclusión digital y límites de la comunicación mediada [en línea]. *Trípodos*, 31. [Consultado el 25 de Marzo de 2015]. Disponible <http://goo.gl/aCLasz>
- LÓPEZ GARCÍA, G. (2005). *Modelos de comunicación en Internet*. Valencia: Tirant lo Blanch.
- MADDEN, M. et al. (2007). *Digital Footprints: Online identity management and search in the age of transparency*. Washington, DC: Pew Internet & American Life Project. [Consultado el 22 de Febrero de 2015]. Disponible <http://goo.gl/XLSyoZ>
- MARDER, B., JOINSON, A., & SHANKAR, A. (2012, JANUARY). Every post you make, every pic you take, I'll be watching you: Behind social spheres on Facebook. En *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 859-868). IEEE.
- MARWICK, A. E. (2011). I tweet honestly, I tweet passionately: Twitter users, context collapse, and the imagined audience. *New media & society*, 13(1), 114-133.
- MOROZOV, E. (2012). *El desengaño de internet. Los mitos de la libertad en la red*. Barcelona: Ediciones Destino.
- MOROZOV, E. (2013). *To save everything, click here*. Londres: Penguin Books.
- MÜLLER, P., SCHNEIDERS, P., & SCHÄFER, S. (2016). Appetizer or main dish? Explaining the use of Facebook news posts as a substitute for other news sources. *Computers in Human Behavior*, 65, 431-441.
- PARISER, E. (2011). *The filter bubble: What the Internet is hiding from you*. New York: The Penguin Press.
- PUSCHMANN, C., Y BOZDAG, E. (2014). Staking out the unclear ethical terrain of online social experiments. *Internet Policy Review*, 3(4).
- RECUBER, T. (2016). From obedience to contagion: Discourses of power in Milgram, Zimbardo, and the Facebook experiment. *Research Ethics*, 12 (1) 44-54.
- RHEINGOLD, H. (2004). *Multitudes inteligentes. La próxima revolución social*. Barcelona: Gedisa.

- SHIRKY, C. (2012). *Excedente cognitivo: Creatividad y Generosidad en la era conectada*. Barcelona: Deusto.
- SKRUBBELTRANG, M. M., GRUNNET, J., & TARP, N. T. (2017). # RIPINSTAGRAM: Examining user's counter-narratives opposing the introduction of algorithmic personalization on Instagram. *First Monday*, 22(4).
- SCHROEDER, R. (2014). Big Data and the brave new world of social media research. *Big Data & Society*, 1(2), 2053951714563194.
- STEICHEN, B., ASHMAN, H., & WADE, V. (2012). A comparative survey of Personalised Information Retrieval and Adaptive Hypermedia techniques. *Information Processing & Management*, 48(4), 698-724.
- SUNSTEIN, C. R. (2003). *República.com. Internet, democracia y libertad*. Barcelona: Paidós.
- TAYLOR S., BAKSHY E., ARAL S. (2013). Selection Effects in Online Sharing: Consequences for Peer Adoption. *ACM Conference on Electronic Commerce (EC)*. EC'13, June 16–20, Philadelphia, USA.
- TELLO DÍAZ, L. (2013). Intimidad y «extimidad» en las redes sociales. Las demarcaciones éticas de Facebook. *Comunicar*, 21(41), 205-213.
- THURMAN, N., y SCHIFFERES, S. (2012). The future of personalization at news websites. *Journalism Studies*, 13(5-6), 775–790.
- TREMBLAY, G. (2006). Economía Política del espacio público y mutaciones mediáticas. *CIC Cuadernos de Información y Comunicación*, 11, 223-240.
- TUFEKCI, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *J. on Telecomm. & High Tech. L.*, 13, 203.
- VIRILIO, P. (1997). *El Ciber mundo: la Política de lo Peor*. Madrid: Cátedra.
- WU, D., et al. (2003). A framework for classifying personalization scheme use done – commerce websites. In R. SPRAGUE (ed.), *Proceedings of the 36th Hawaii International Conference on System Science*. Los Alamitos (California): IEEE Computer Society Press.
- YOUYOU, W., KOSINSKI, M., & STILLWELL, D. (2015). Computer-based personality judgments are more accurate than those made by humans. *Proceedings of the National Academy of Sciences*, 112(4), 1036–1040.
- ZIEWITZ, M. (2016). Governing Algorithms Myth, Mess, and Methods. *Science, Technology & Human Values*, 41(1), 3-16.