



REVISTA DE DIFUSIÓN ACADÉMICA

ISSN 2718-6318

Año I | Número 2 | Agosto 2020

El control de los datos en el mundo digital y la utopía de la privacidad

Josefina Romero Barberá ¹

josefinaromerobarbera@gmail.com

¹ Estudiante de la Licenciatura en Comunicación Social de la Universidad de San Isidro (USI)



La escritora y periodista española Marta Peirano afirmó en su célebre charla TED de Madrid (2015): “No hay que desmerecer la cantidad de información que producimos cada día”. En 2010, Eric Schmidt, CEO de Google, nos contó que, hasta 2003 y a lo largo de su historia, la humanidad había generado 5 exabytes de información. Para 2007, se habían generado 281 exabytes, según las investigadoras Hardy y Williams. Y, sólo cuatro años después, se llegó a los 1.800 exabytes. Hoy en día, cualquier persona genera una gran cantidad de datos a su paso (López, 2019):

Actualmente, la capacidad de enviar y gestionar datos aumenta y el consumo informativo no sólo es ingente en empresas y en el ámbito comercial, sino que la cantidad de datos que un individuo genera, gestiona, edita o comparte cada día es difícilmente calculable. Ante la gran abundancia de información y de la sobreexposición a los demás, el individuo queda desprotegido. (Giones-Valls y Serrat-Brustenga, 2010. p. 2)

El problema es que la existencia misma de esa información nos hace vulnerables de una forma en que no nos podemos anticipar (Peirano, 2015). Toda la actividad que uno produce en la red crea una identidad digital personal, lo cual “es una representación virtual que nos permite interactuar

en el ciberespacio, proyectar una personalidad y difundir una trayectoria personal o profesional para aprender y compartir información” (Giones-Valls y Serrat-Brustenga, *ibídem*, p. 9). Esta identidad es una representación de uno mismo, y se va construyendo a la par de nuestra actividad en Internet. De todas formas, si una persona decide no crearse una identidad digital, eso no quita que otras personas publiquen material con o de ellos, como ocurre con las fotografías.

“Es siempre útil, comprende usted, someter la vida pasada de los reformadores políticos a una minuciosa investigación” (Asimov, 1975. p. 180). Acerca de este diálogo en “Yo Robot”, Peirano (2015) nos explica que toda esa información que contiene nuestro perfil, nuestra identidad digital, se convierte en “nuestros antecedentes”. Y no hace falta ser una persona “importante” para que estos datos sean recolectados, ya que “a nuestros vigilantes no les importa que no seamos nadie, que no seamos importantes, porque son algoritmos, no son personas. Y nuestro perfil es automático, existe, aunque nadie lo mire” (*ibídem*). Por lo que, en cualquier momento, puede ser rastreado y utilizado.

Los nativos digitales, son aquella generación que no conoce la vida sin la red y utiliza internet de manera intensiva. “Estos jóvenes digitales se caracterizan también por ser exhibicionistas y multitareas” (Giones-Valls y Serrat-Brustenga, 2010. p. 2). Quedando todavía más expuestos, ya que “(...) los jóvenes no suelen leer ni conocer la política de privacidad de las redes sociales que utilizan y, por consiguiente, la mayoría de ellos no tiene configuradas las opciones de privacidad de las redes sociales que emplean.” (Rodríguez García y Magdalena Benedito, 2016. p. 19)

Gracias a Goffman (1956) entendimos que el individuo pone en práctica, durante toda su vida, una serie de signos para expresar durante la interacción lo que desea transmitir. Se trata de construir una impresión de realidad, una “fachada” con base en ciertos modales, apariencias, etc. (p. 34). En el siglo veintiuno, esto mismo sucede en las redes. Una misma persona puede tener diferentes identidades y todas se pueden ver reflejadas en la red: “La

tergiversación se considera un acto intencional, por lo que para evitar que el auditorio se entere, el individuo se exige valerse de signos para construir una representación de su actividad en la actuación” (Goffman, 1956. p. 78)

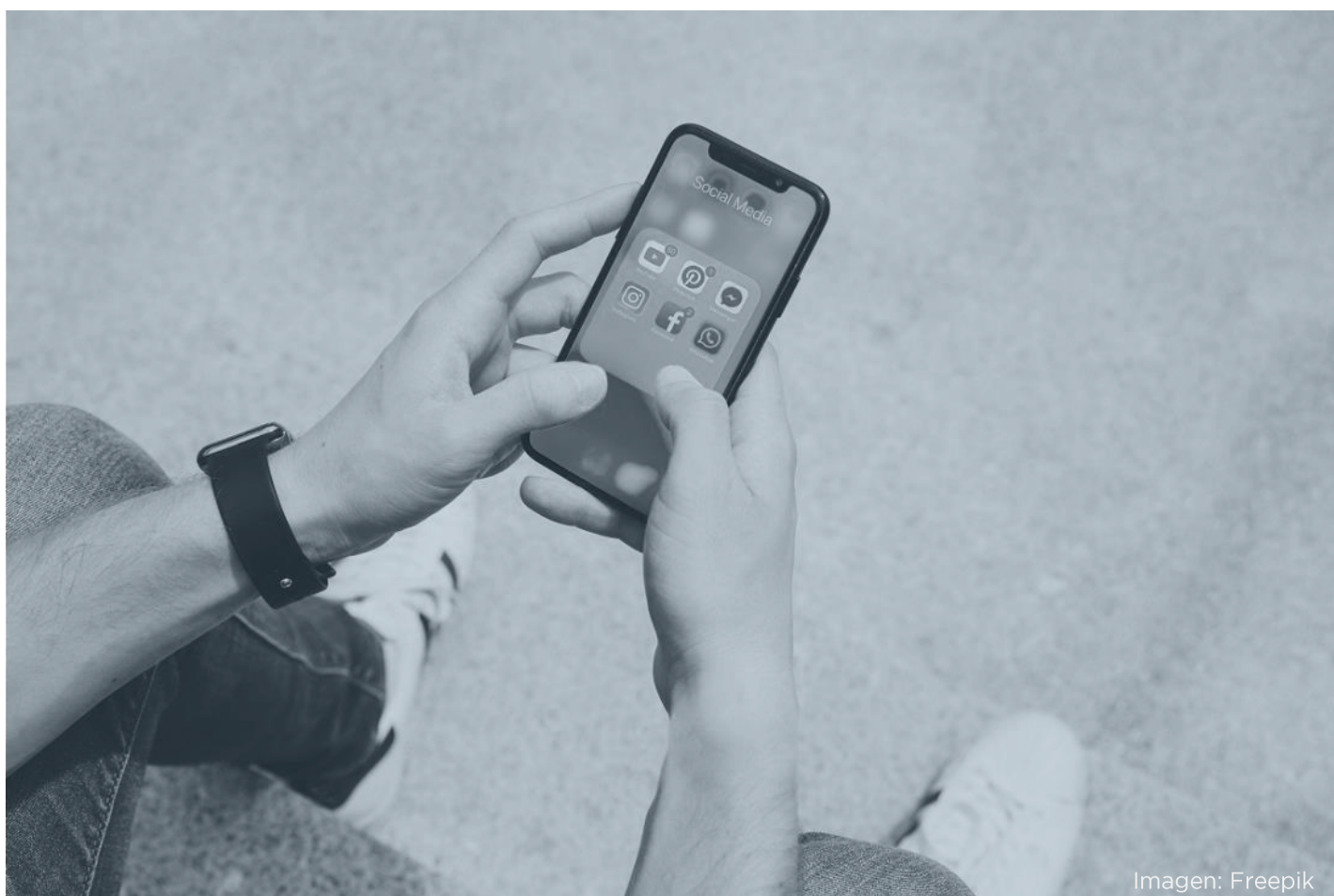
La cantidad de datos personales existentes en la red es muy elevada, y la información de un perfil pueden coincidir o no con la identidad analógica, es decir, con las características que se pueden atribuir a una determinada persona en su vida fuera de la red u *offline* (Giones-Valls y Serrat-Brustenga, 2010. p. 2). En otras palabras, es el acto de una persona que utiliza los medios digitales para generar una identidad que no es real, por ejemplo, fotos de otras personas, vocabulario específico, etc. Esta es la base del *phishing*, un término informático que se refiere a una persona que tiene una identidad falsa y manipula a un usuario con fines maliciosos.

Pero más allá de la identidad que uno quiere mostrar en las redes, por lo general solemos buscar en los servidores aquel contenido que nos interesa realmente. Lo que nos lleva a preguntarnos: ¿sólo nosotros accedemos a nuestros historiales de búsqueda o a los datos de nuestros perfiles de usuarios? Toda la información que ingresamos en forma permanente, ¿es realmente nuestra?

Cuando una persona navega en el mundo web “cede todos los datos personales y los contenidos a la red social, en algún caso, incluso después de que el usuario se haya dado de baja del servicio, estos datos y contenidos se mantienen visibles para otros usuarios” (Giones-Valls y Serrat-Brustenga, 2010. p. 7). Hoy en día, la privacidad es un tema latente en las redes virtuales, y es cada vez más difícil de controlar, siendo que los mismos usuarios son quienes exponen sus datos de manera voluntaria. Sin embargo “no siempre son conscientes de la repercusión que este hecho puede tener (...) Todos estos datos están a menudo al alcance de perfectos desconocidos” (ibídem, p.6)

Un usuario que navega en internet nunca está totalmente a salvo de los problemas de seguridad y privacidad. Para usar internet de manera responsable y tener todo el control posible sobre nuestros datos, es

importante saber qué información compartimos con los sitios web que visitamos. Un buen ejemplo son las *cookies*, es decir un archivo creado por un sitio web, el cual recolecta cierta cantidad de nuestros datos a partir de nuestra navegación y son enviadas de un emisor a un receptor. El propósito de las *cookies* es “(...) identificar al usuario almacenando su historial de actividad en un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos” (González, 2014).



Hablando de privacidad, cuando nos llegan publicidades de algo que nos interesa, por ejemplo, pensamos en una situación como la lectura de pensamientos de *Herbie* (robot protagonista del quinto cuento de Asimov: “¡Embustero!”, el cual tiene la extraordinaria propiedad de sincronizarse con las ondas del pensamiento ajeno), pero en realidad es un algoritmo que usó nuestros datos para ofrecernos lo que nos gusta. No es que nos han “leído la

mente”, sino que nos muestra aquel contenido que hemos buscado anteriormente o que, por relación, podría llegar a interesarnos. Así, la tecnología se nos presenta como una herramienta que nos ofrece lo que nos gusta y no como algo que busca causarnos daño o disconformidad.

¿Qué mejor ejemplo que *Speedy*? El robot del segundo cuento “Sentido Giratorio” de Asimov es localizado con un GPS, o sea, datos que transmitimos (o que transmiten los robots por nosotros). “«Manda un robot a buscar un robot»” (p. 38), tal como podría ser una computadora localizando a un celular en nuestro bolsillo. Esta herramienta lo convirtió en algo localizable físicamente en un mapa. Suena muy similar a *Google Maps* o muchas otras aplicaciones que cumplen con esta función.

Giones-Valls y Serrat-Brustenga (2010) afirman que “la construcción de una identidad digital en la red implica un aprendizaje y una actitud colaborativa y participativa en la cultura digital” (p. 11). No obstante, todo lo que se publica en internet queda registrado, hecho que puede traer consecuencias futuras en la imagen y la reputación personal. De todas maneras, es recomendable intentar ingresar la menor cantidad de datos personales posibles en la red. Y en todo caso, brindarlos en aquellos entornos que sean confiables y seguros. Sin embargo, los autores concluyen que hay

(...) dos perspectivas para aproximarse al tema de la identidad digital y de internet. Una es creer que la presencia virtual significa un peligro para la seguridad personal (...) La otra es entender la construcción de la identidad en la red como una oportunidad de aprendizaje tanto personal como profesional, dentro de la cultura informacional donde vivimos inmersos. (ibídem, p.8)

Conclusión

Acudiendo a responder el interrogante acerca de quién debería tener el control de nuestros datos personales en el mundo digital, podríamos concluir: nosotros, los usuarios, son quienes deberíamos tener el absoluto control. Justamente, porque son nuestros datos. Pero, al mismo tiempo, debemos

reconocer que, si tuviéramos ese control en forma absoluta, el mundo digital no sería el que conocemos hoy.

Hay quienes afirman que, en verdad, los usuarios de internet sí tenemos el dominio de nuestra información personal, ya que, como se explicó antes, nosotros decidimos si queremos ingresar o no esa información. Es que, si queremos formar parte del mundo digital, tendemos a otorgar ese consentimiento sin prestar demasiada atención. Nos mueve el afán de pertenecer a la sociedad tecnológica del siglo veintiuno.

En este tiempo, es muy fácil quedarse atrás con la cantidad de actualizaciones que nos ofrece la tecnología. Y los usuarios no estamos dispuestos a aceptar ese atraso. “Uno de los principios favoritos de Gregory Powell es que con la excitación no se gana nada” (Asimov, 1975. p.36). En medio de la excitación de querer ser parte de la masa, de la moda que ella impone y de la vida digital de la que no podemos escapar, terminamos cediendo nuestros datos personales, tal como los demás, para poder pertenecer. No ceder significa quedarse afuera. Es que, finalmente, el concepto de privacidad en las redes no es más que una utopía. Admitamos entonces que “la mejor manera de proteger tu privacidad en la red es asumir que no la tienes”. (Giones-Valls y Serrat-Brustenga, 2010, p. 7)

Bibliografía

Asimov, I. (1975). *Yo, Robot*. (1ra ed.) España: EDHASA.

Giones-Valls, A. y Serrat-Brustenga, M. (2010). *La gestión de la identidad digital: una nueva habilidad informacional y digital*. Recuperado de <http://eduteka.icesi.edu.co/gp/upload/giones2.pdf>

O'Reilly, Dennis (2007). *Five ways to protect your privacy online*. Cnet News.

Goffman, E. (1956). *La Presentación de la Persona en su vida cotidiana*. Canadá: Doubleday.

González, G. (2014). *Blogthinkbig.com*. [Oficial de Telefónica]. Recuperado el 3 de julio de 2020 de <https://blogthinkbig.com/que-son-las-cookies>

López, D. (2019). *By Orange*, [Blog oficial de Orange]. Recuperado el 1 de julio de 2020 de <http://blog.orange.es/red/datos-mundo/>

Rodríguez García, L. y Magdalena Benedito, J.R. (2016): *Perspectiva de los jóvenes sobre seguridad y privacidad en las redes sociales*, Icono 14, volumen (14), pp. 24-49. doi: 10.7195/ri14.v14i1.885

Peirano, M. (2015, 22 de septiembre). *¿Por qué me vigilan, si no soy nadie?* TEDxMadrid [YouTube]. Recuperado de <https://www.youtube.com/watch?v=NPE7i8wuupk>