ALEXA, ¿DEBERÍA PREOCUPARME POR **MI PRIVACIDAD?**

Con el aumento de la información generada por el creciente uso de la tecnología por parte de los ciudadanos, la defensa de la privacidad de estos es una exigencia cada vez mayor. Sobre este asunto versa el siguiente artículo, centrado, en este caso, en el ámbito de los asistentes virtuales por voz.

Álvaro Saavedra Montejo
Colaborador del Proyecto Universidad Pública de Navarra

Durante las últimas décadas ha emergido con fuerza la legislación sobre la privacidad como resultado de las interacciones digitales entre personas, empresas, organismos, etcétera.

El marco legislativo en las cuestiones de protección de la privacidad digital consta del Reglamento General de Protección de Datos (RGPD), del Parlamento Europeo y del Consejo (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos, aplicable desde el 25 de mayo de 2018. Y, por otro lado, se encuentra la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En España, la Agencia Española de Protección de Datos trata de velar por la privacidad y protección de datos de los ciudadanos, actuando como un órgano independiente. El objetivo de esta Agencia es "por un lado, fomentar que las personas conozcan sus derechos y las posibilidades que la Agencia les ofrece para ejercerlos y, por

LAS POLÍTICAS DE EMPRESA REFERIDAS A LA PRIVACIDAD TIENEN QUE ESTAR BLINDADAS LO SUFICIENTEMENTE PARA QUE NO PUEDAN SER VULNERADAS

otro, que los sujetos obligados tengan a su disposición un instrumento ágil que les facilite el cumplimiento de la normativa"[1].

Organizaciones tanto en el plano internacional como nacional han establecido la privacidad como una política clave en el sigo XXI (van Zoonen, 2016). Por otro lado, la pregunta que puede surgir es: ¿son todos los datos igual de importantes? Se podría decir que de manera general, los datos más sensibles son de carácter financiero, médico e incluso civiles, mientras que aquellos referentes a la nacionalidad, género o edad pertenecen a una 'segunda categoría' de importancia (Eurobarometer, 2011; Rose et al., 2012).

A medida que las diferentes tecnologías que nos rodean se están haciendo más personales, dominantes y, sobre todo, omnipresentes, se acrecienta la preocupación de los usuarios por la privacidad de su huella digital (Rauschnabel et al., 2018). Todas las tecnologías almacenan enormes cantidades de información, por lo que el uso de alguna tecnología va acompañado de ciertos riesgos para los usuarios. Estos factores negativos de riesgo percibido producen en las personas desconfianza, ya que el principal miedo es no saber cómo se usan sus datos por parte de las empresas.

El almacenamiento de información del usuario es muy importante porque, al final, es la clave en la personalización. Como resultado, las empresas podrán mejorar sus servicios/productos y, por lo tanto, podrá haber una mayor satisfacción para el usuario.

Estas cuestiones de privacidad se tratan no solo desde el punto de vista del uso que hacen las empresas con los datos, sino que también existe un miedo de que los usuarios se sientan controlados en el contexto de la autonomía percibida (Walter & Lopez, 2008). Estas cuestiones finalmente generan barreas en el uso o adopción de las tecnologías presentes, por consiguiente, se debe trabajar por ampliar la regulación concreta en este campo (con el fin de proteger a los usuarios) y que las empresas la cumplan al mismo tiempo que dejan claro a los usuarios que pueden confiar en ellas.

Ha habido escándalos muy conocidos respecto a los fallos o ciberataques hacia empresas, organismos públicos, etcétera. Se puede destacar el caso de LexNet. Esta es una plataforma para el intercambio de toda aquella información de carácter judicial del Ministerio de Justicia en la que trabajan gran cantidad de órganos judiciales. Pues bien, un fallo dejó al descubierto miles de documentos judiciales y, según la Agencia Española de Protección de Datos, "284 usuarios accedieron a 692 buzones ajenos", es decir, se produjeron consultas no autorizadas por usuarios que tampoco estaban autorizados. Los datos vulnerados eran de suma relevancia ya que hacen referencia a escritos procesales, demandas, notificaciones, etcétera. Son muchos los ciberataques producidos, y siempre que aparece uno nuevo se vuelve a poner la duda sobre la mesa: ¿dónde queda

nuestra privacidad como usuarios? Las políticas de empresa referidas a la privacidad tienen que estar blindadas lo suficientemente para que no puedan ser vulneradas.

Podríamos destacar una tecnología a la que los usuarios le tienen un respeto especial: la inteligencia artificial por voz. Cada vez es mayor el uso de los asistentes virtuales por voz como Alexa, Siri, Cortana, etcétera, y siempre surge la cuestión de si están continuamente escuchándonos. En líneas generales, cualquier persona lleva siempre encima un teléfono móvil (sin mencionar *gadgets* aparte), por lo que, si fuera verdad que escuchan en todo momento, el riesgo estaría en niveles extremos. La teoría es que no, o por lo menos es en lo que se centran las empresas en defender. La realidad es que hay estudios sobre fallos de seguridad en determinados asistentes, entre ellos, los estudios realizados por la Universidad Northeastern en Estados Unidos (Barca, 2020). De momento, el número de ventas a través del uso de los asistentes virtuales por voz, ya sea en el teléfono móvil u altavoz inteligente, son muy bajas. Precisamente por el miedo que conlleva a usar la voz para poder así hacer efectivo el pago. Al fin y al cabo, las barreras psicológicas vienen dadas por la incertidumbre y la vulnerabilidad.

Algunos académicos ya han señalado que a medida que aumenta la confianza en la tecnología, mayor podrá ser el rendimiento esperado de esta. Por lo tanto, la confianza es un factor muy importante en el uso de las tecnologías. A mayor uso de estas, por lo tanto, mayor cantidad de datos que las empresas podrán usar legalmente para mejorar las estrategias que tengan planteadas.

EN UNA SOCIEDAD CADA VEZ MAS DIGITALIZADA, TODAS LAS CUESTIONES RELATIVAS A LA PRIVACIDAD DEBEN SER ATENDIDAS Y HACER DEL ESPACIO DIGITAL UN LUGAR SIN RIESGOS EN EL QUE SE PUEDA CONFIAR

Con el crecimiento de las nuevas tecnologías basadas en *big data*, *cloud computing* y *blockchain*, el uso en sí mismo de la tecnología está incrementándose. Se podría destacar, en primer lugar, que tiene que respetarse el marco jurídico que defiende nuestra privacidad desde cualquier ámbito. En segundo lugar, las empresas deben favorecer que los usuarios/consumidores puedan confiar en el uso que se va a hacer de sus datos.

La tecnología debe ser entendida como una herramienta para mejorar en todo aquello que sea positivo y no crear vulnerabilidades que puedan afectar a la vida de las personas. En una sociedad cada vez mas digitalizada, todas las cuestiones relativas a la privacidad deben ser atendidas y hacer del espacio digital un lugar sin riesgos en el que se pueda confiar. ■

Notas

1. Página web oficial de la Agencia Española de Protección de Datos.

Referencias

Barca, K. (2020). Alexa, Siri y Google Home pueden grabar tus conversaciones hasta 19 veces al día sin que te des cuenta. *Businessinsider*. https://www.businessinsider.es/alexa-siri-google-home-activan-error-19-veces-dia-587111

Eurobarometer, S. (2011). 359. Attitudes on data protection and electronic identity in the European Union. *European Commission*.

Rauschnabel, P. A., He, J., & Ro, Y. K. (2018). Antecedents to the adoption of augmented reality smart glasses: A closer look at privacy risks. *Journal of Business Research*, *92*, 374–384. https://doi.org/10.1016/J.JBUSRES.2018.08.008

Rose, J., Rehse, O., & Röber, B. (2012). The value of our digital identity. *Boston Cons. Gr*.

van Zoonen, L. (2016). Privacy concerns in smart cities. *Government Information Quarterly*, *33*(3). https://doi.org/10.1016/j.giq.2016.06.004

Walter, Z., & Lopez, M. S. (2008). Physician acceptance of information technologies: Role of perceived threat to professional autonomy. *Decision Support Systems*, *46*(1), 206–215. https://doi.org/10.1016/j.dss.2008.06.004