TECNOLOGÍA INFORME

Ese miedo de que usen los datos de uno sin permiso

Son incontables los debates sobre la ética del uso de datos personales, sin embargo, hay mecanismos para defenderse.
Mire cuáles son.

Por **LAURA TAMAYO GOYENECHE**

Desde que usted se levanta hasta que bloquea el celular antes de dormir está generando datos. Aunque son distintos a los que no cambian, como la cédula y la fecha de nacimiento, lo que hace en línea o los lugares que visita, aún en cuarentena, dicen algo de su personalidad.

Para que se haga una idea de la cantidad, si en el futuro usted se movilizara en un carro autónomo, estaría generando 30 terabytes de información en 8 horas de conducción. En dos años, superaría el número de datos generados desde la llegada de los computadores, explicó el semanario británico *The Economist* en su edición de febrero de este año.

Ese mismo medio advirtió, en 2017, que los datos son el petróleo de este siglo, ¿por qué?

En palabras de la abogada *Manuela Battaglini*, investigadora en ética digital, un dato suelto no significa nada y muchos datos almacenados tampoco. El verdadero valor llega cuando esa información alimenta sistemas con inteligencia artificial que, dependiendo de la forma en que estén entrenados, predicen comportamientos, enfermedades, gustos, intenciones de compra.

Por eso es que tal vez le ha pasado que habla sobre un producto con alguien y luego le aparece publicidad sobre eso mismo en Internet. Lo primero que uno piensa es que lo están espiando por medio del micrófono del teléfono, y aunque Apple reconoció en 2019 que sus trabajadores escuchaban conversaciones de los usuarios por medio del asistente virtual Siri, la cosa va por otro lado.

"Hemos dejado en la web tantos datos que consideramos insignificantes, y los sistemas de inteligencia arficial son tan precisos que logran perfilarnos para ofrecernos cosas de las que hemos hablado", señala Battaglini en llamada desde Dinamarca.

En el estudio *Transparencia, procesos automatizados de toma de decisiones y perfiles personales* (2019), que hizo junto al profesor *Steen Rasumssen* y fue publicado en *Journal of Data Protection*, concluyó que el problema no son los datos en sí mismos, sino que en muchas ocasiones, usted, que es el dueño de esa información, no sabe que está siendo usada para crear un perfil suyo, ni tiene acceso a él.

Sobre los cuestionamientos éticos que tiene la economía de los datos "hay amplitud de documentación al respecto, pero también pasos previos que hay que cumplir en el camino", señala *Víctor Saavedra*, investigador de la línea Transparencia, Tecnología y Derechos Humanos de DeJusticia. Él recomienda comenzar por los mínimos con los que ya contamos: las normas e instrumentos jurídicos que lo protegen como ciudadano. Aunque suene a cuento viejo, la ley de habeas data es la herramienta que usted tiene para defenderse cuando sienta que algo no está bien con su información personal. Desde la perspectiva del investigador, la ley colombiana es clara y se complementa con mecanismos como el juicio de proporcionalidad, "que permite hacer análisis caso a caso en términos de idoneidad, necesidad y ponderación en la afectación a nuestros derechos".

Así que lo malo no es solicitar datos o usarlos, dice *Pilar Sáenz*, investigadora en Karisma, una organización que vela por los derechos humanos y la tecnología, "siempre y cuando haya transparencia, una finalidad determinada, proporcional y que tenga como base la confianza del usuario". Los análisis advierten que la economía de datos, lejos de acabarse, se robustece, por eso pregúntese hasta qué punto quiere ceder. Usted sigue siendo el dueño de la información ■

EN DEFINITIVA

Los dueños de los datos personales deberían estar enterados no solo de la finalidad con la que será usada la información, sino los perfiles que se están creando a partir de ella.

EL ABC DE LOS DATOS PERSONALES

¿Cuándo se pueden recopilar datos sin autorización?
No es necesario cuando se trata de información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, datos de naturaleza pública, casos de urgencia médica o sanitaria, tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos, datos relacionados con el Registro Civil de las personas.

¿Cuáles datos se pueden tratar y cuáles no?
Según la ley de habeas data, cualquier institución le debe pedir autorización para recolectar un dato personal e informarle cuál es la finalidad de forma clara. Usted puede negar esa información y también revocar la autorización si no cumple con los principios de finalidad, legalidad, veracidad, transparencia, seguridad y confidencialidad. Ningún dato sensible puede ser tratado, a menos que haya una autorización explícita. Tampoco los datos personales de los menores de edad.

¿Por qué con la pandemia hay preocupación por los datos?
Con el decreto 637 del 6 de mayo de 2020, el Gobierno Nacional declaró el estado de emergencia, eso quiere decir que puede adoptar medidas legales nuevas, con el fin de mitigar la pandemia.
Eso incluye recopilar y tratar datos sensibles, relacionados con salud, con el fin de mitigar la propagación del virus en el país. Según *Pilar Sáenz*, el problema ha sido por la desconfianza de los ciudadanos en el uso que el gobierno le puede dar a la información.

¿Es lo mismo que el Gobierno le pida datos a que lo haga una empresa privada o su empleador?
La investigadora de Karisma *Pilar Sáenz* explica que no, porque hay asimetría de poder. "Uno no le puede negar al empleador o al gobierno un dato porque eso puede traer represalías. No obstante, la relación con una empresa privada, como Google o Facebook, es voluntaria y uno puede pedirles en cualquier momento que borren toda la información que han recopilado de uno en sus servidores", señala.

Si por la emergencia van a tratar datos sensibles, ¿qué lineamientos se deben seguir?
La ley vigente dice que, como se trata de una emergencia de salud, no se requiere su autorización para recolectar y tratar datos sensibles. Sin embargo, le deben comunicar con claridad la finalidad y comprometerse a proteger la circulación de esa información. Está prohibido usar medios engañosos para tener sus datos y le deben decir hasta qué momento los van a guardar. Un ejemplo internacional lo pone la compañía Abartys Health, de Puerto Rico, que es una plataforma que busca conectar en ese país todo el sistema de salud y ha sido reseñada por Forbes. Su fundadora, *Dolmarie Mendez*, anotó a EL COLOMBIANO que uno de sus principios para integrar datos sensibles de todo el país entre laboratorios, aseguradoras y pacientes es la confianza y una protección tal que ni siquiera los empleados de Abartys pueden acceder a la información privada de sus clientes.