

Artículo 12: Derecho a la privacidad

¿Deben las escuelas usar cámaras en el aula para controlar las caras de los niños y determinar si están prestando atención? ¿Usaría wifi gratis en un quiosco de la calle si supiera que sus cámaras y sensores están recopilando información sobre Usted, y que le seguirían rastreando incluso después de salir de la zona de wifi? Si lleva en su muñeca una pulsera inteligente que recopila información sobre su rutina de ejercicio, ¿cómo se sentiría si una compañía de seguros usara sus datos para negarle cobertura?

Estos no son fragmentos de una pesadilla distópica, sino problemas muy reales de nuestra era digital que los redactores de la Declaración Universal de Derechos Humanos (DUDH) no podían haber previsto en 1948. Sin embargo, con el incremento en la recopilación de datos por parte de los gobiernos y las empresas, el concepto de privacidad consagrado en el artículo 12 se ha vuelto más fundamental en nuestras vidas en los últimos 70 años.

A menudo, el derecho a la privacidad se presenta como un pasaporte que refuerza otros derechos, en la red y fuera de la red, incluyendo los derechos a la igualdad y a la no discriminación, y a la libertad de expresión y reunión.

Sin embargo, la privacidad también es un valor en sí mismo, esencial para el desarrollo de la personalidad y la protección de la dignidad humana, que es uno de los temas centrales de la DUDH. Nos permite protegernos de las interferencias injustificadas en nuestras vidas y determinar cómo queremos interactuar con el mundo. La privacidad nos ayuda a establecer fronteras para limitar quién tiene acceso a nuestros cuerpos, lugares y objetos, así como a nuestras comunicaciones y a nuestra información.

La privacidad no es un derecho absoluto, y puede ser limitada en algunos casos, como cuando las autoridades penitenciarias buscan en las celdas por contrabando. Sin embargo, las intrusiones en la privacidad deben ser proporcionales al beneficio que esto aporta a la sociedad. El Tribunal Europeo de Derechos Humanos, por ejemplo, dictaminó en 2000 que no era "necesario en una sociedad democrática" que el servicio secreto acumulara un expediente contra un ciudadano rumano, incluidos detalles (algunos falsos) de hace 60 años.

La privacidad, especialmente la privacidad digital, puede parecer un concepto abstracto. A medida que han ido aumentando las preocupaciones sobre el terrorismo en los últimos años, los gobiernos han tratado de inmiscuirse cada vez más en la privacidad de los ciudadanos, apelando a la seguridad nacional. "Si no tiene nada que ocultar", argumentan, "¿qué le preocupa?".

Quizás el valor de la privacidad se pueda entender más fácilmente en el mundo de lo físico. Supongamos que alguien irrumpió en su casa y no se llevó nada, sino que husmeó en sus armarios y leyó sus cartas privadas. Tal intrusión, a la mayoría de nosotros, como mínimo, nos haría sentir incómodos. No obstante, algo muy similar está sucediendo hoy en las ciudades repletas de cámaras de televisión de circuito cerrado, con empresas que venden información sobre su historial de búsquedas en Internet y con la vigilancia del gobierno sobre las personas.

“Los gobiernos en todas las regiones están utilizando también herramientas de vigilancia digital para localizar y atacar a los defensores de los derechos humanos y a las personas percibidas como críticas, incluidos abogados, periodistas, activistas de derechos a la tierra o al medio ambiente, y personas que apoyan la igualdad para los miembros de la comunidad LGBTI ”.

- **Michelle Bachelet, Alta Comisionada de las Naciones Unidas para los Derechos Humanos**

En ocasiones elegimos renunciar a aspectos de nuestra privacidad. Cada vez que compramos algo en la red, o usamos un servicio wifi gratuito, renunciamos a cierto grado de privacidad a cambio de algo de valor.

Sin embargo, las personas no siempre son conscientes de lo que están entregando, o a quién se lo están entregando. Es posible que no sepan que cada vez que se obtiene algo gratis en el mundo digital, no somos el

cliente sino el producto. En 2018, unos 87 millones de usuarios de Facebook descubrieron que se habían convertido en un producto, sin su conocimiento o permiso, cuando sus hábitos de navegación, compras, opiniones políticas y redes de amigos se analizaron y se vendieron con fines de lucro.

A los defensores de la privacidad también les preocupa que muchos usos de la tecnología presentados como una ventaja puedan tener un lado más oscuro. Algunas compañías de seguros ofrecen un descuento a los clientes que pueden probar sus hábitos de salud usando una pulsera inteligente. ¿Se considera un salto al vacío negar un seguro a aquellos que se niegan a usar la pulsera "inteligente"? Es posible que le haga feliz "sonreír y pagar" – es decir, usar el reconocimiento facial como acceso directo a su cuenta bancaria. Pero, ¿qué pasa si su rostro pasa a formar parte de un plan de vigilancia masiva a cargo del gobierno que puede rastrearle en cualquier lugar?

Actualmente, en ciertas partes del mundo, los enormes bancos de datos tienen información (historial de búsqueda, ubicación, datos financieros y de salud) sobre cada mujer, hombre y niño. Esto no significa "todos los que son percibidos como críticos o activistas, o incluso todos los usuarios de Internet, sino simplemente todo el mundo", afirma la Alta Comisionada de las Naciones Unidas para los Derechos Humanos, Michelle Bachelet.

El alcance de la intromisión a cargo de los gobiernos a nivel global salió a la luz en 2013, cuando el antiguo contratista de la Agencia Central de Inteligencia (CIA, por sus siglas en inglés), Edward Snowden, filtró información clasificada de la Agencia de Seguridad Nacional de los Estados Unidos. Según las filtraciones, alrededor del 90 por ciento de las comunicaciones interceptadas no pertenecían a objetivos, sino a gente común. Esto tiene importantes ramificaciones, ya que se puede abusar de la recopilación y la vinculación de muchos tipos de información sobre personas para determinar su "valor social" para recompensarlos o incluirlos en una lista negra de maneras que ellas desconocen.

Alrededor del mundo, algunas personas están luchando por preservar la privacidad. La presión pública ha provocado que muchas empresas refuercen su seguridad digital y ofrezcan a sus clientes servicios de comunicaciones totalmente encriptados. Algunos gobiernos están adoptando marcos legales que protegen a las personas contra las intrusiones de los Estados y las empresas. Y proyectos tan innovadores como la construcción de un vecindario "inteligente" en Toronto se enfrentan a un mayor escrutinio de sus prácticas relacionadas con el uso de sus datos. "Imaginaba crear una Ciudad Inteligente de Privacidad, no una Ciudad Inteligente de Vigilancia", escribió Ann Cavoukian, una experta canadiense líder en privacidad, cuando renunció al proyecto.

Setenta años después, la DUDH ofrece un marco claro para garantizar la dignidad y los derechos de todas las personas, incluso en una era digital que sus redactores no pudieron prever. La jefa de Derechos Humanos de la ONU, Michelle Bachelet, ha declarado que los abogados de derechos humanos, informáticos e ingenieros, y los representantes de los gobiernos tienen que trabajar juntos "para garantizar la continua aplicación de los derechos humanos sobre la forma en que los Estados operan en la era digital y regulan las actividades de las empresas en el espacio digital".

Este es uno de una serie de artículos publicados por la Oficina del Alto Comisionado para los Derechos Humanos (OACNUDH) para conmemorar el 70 aniversario de la adopción de la Declaración Universal de Derechos Humanos el 10 de diciembre de 1948. Todos los derechos consagrados en la DUDH están relacionados con entre sí, y todos son igualmente importantes.