LOS


1 Julia Krämer


2 Chloé Berthélémy


3 Maya Thomas


4 Paula Lamo


5 Romain Lanneau

CUESTIONARIO

1 ¿Desde qué perspectiva abordas la privacidad digital en tu investigación o trabajo?

2 ¿A través de qué medios estamos proporcionando datos sobre nosotros mismos sin darnos cuenta?

3 ¿De qué datos estamos hablando, quién los utiliza y con qué finalidad?

4 Tres pasos clave para proteger nuestra privacidad digital.

Y EL ASUNTO DE LA PRIVACIDAD

La investigación y el análisis son las herramientas con las que este ecléctico grupo de brillantes académicos analiza una cuestión tan trascendente como la privacidad en la era digital. Ya sea poniendo el foco en las grandes tecnológicas, los organismos regulatorios, los derechos ciudadanos o los dispositivos que nos rodean, todos alertan de la amenaza que supone el rastreo y la comercialización masiva de datos y ofrecen pistas sobre cómo tener bajo control a quién y qué exponemos.

TEXTO: **LAURA G. DE RIVERA** ILUSTRACIÓN: **JEFF BENEFIT**

“El ecosistema móvil actual, con sus fallas de privacidad, es decisión de Apple y Google”



Para Krämer, experta en el ecosistema móvil, las infracciones de las tecnológicas pueden afectar a la seguridad.

ELLA SABE LO QUE PASA EN TU TELÉFONO

Julia Krämer

1 Soy investigadora especializada en Derecho y examino la privacidad digital desde la perspectiva de la legislación de protección de datos de la UE, en particular el RGPD y la Directiva ePrivacy. Me interesa lo que dice la ley, pero también si funciona en la práctica. En mi investigación doctoral combiné análisis jurídico con investigación empírica, recopilando datos de más de 2,5 millones de aplicaciones de Apple App Store y Google Play Store para evaluar si lo que ocurre cumple la legislación. A menudo, no es así.

2 Mi investigación se centra en el ecosistema móvil: cómo las aplicaciones procesan nuestros datos y qué papel desempeñan Apple y Google, dado su control sobre los sistemas operativos móviles y las tiendas de aplicaciones. La mayor parte de este procesamiento es invisible. Los datos salen a través de rastreadores integrados en las aplicaciones (los *Software Development Kits*, o SDK). Algunos tienen fines legítimos, como informar de errores o facilitar el inicio de sesión, pero muchos están destinados a la publicidad y a la elaboración de perfiles. Como un SDK *hereda* los permisos de la aplicación en la que está integrado, su proveedor recibe los mismos datos que el desarrollador. Google, por sí solo, está presente en más del 85 % de las aplicaciones de iOS y Android a través de sus SDK. Desde el punto de vista jurídico, se requiere consentimiento. En la práctica, muchas veces ni se solicita.

3 La ubicación es el ejemplo más evidente: utilizarla en una determinada app puede revelar información sensible, como una enfermedad crónica, la orientación sexual o las afiliaciones políticas. Estos datos están vinculados a un identificador publicitario —el número de matrícula de tu teléfono— que permite combinar diferentes datos de distintas aplicaciones para crear un único perfil. Estos perfiles son comprados por *data brokers*, que posteriormente los revenden a ignotos terceros. El informe *The Databroker Files*, elaborado por netzpolitik.org, y trabajos periodísticos similares en los Países Bajos, sacaron a la luz los patrones de movimiento de millones de personas de la UE, incluidos trabajadores de prisiones y ministerios de Defensa. Esto plantea riesgos para la privacidad y para la seguridad.

4 **1.** Comprueba qué contienen las aplicaciones que instalas. Ni Apple App Store ni Google Play Store indican qué rastreadores contiene una aplicación, pero iniciativas comunitarias como Exodus Privacy y Tracker-Control sí lo hacen. **2.** Desactiva los servicios de localización de tu teléfono. **3.** Sé escéptico. Apple App Store y Google Play Store ofrecen etiquetas de privacidad en la página de instalación de las aplicaciones. Pero no están verificadas: he encontrado información contradictoria en más de 36 000 aplicaciones. Además, la función *App Tracking Transparency* de Apple solo bloquea el acceso a un identificador concreto, en lugar de impedir el rastreo en sí. Las propias apps de Apple y Google quedan fuera de sus definiciones de rastreo. Dicho esto, no creo que la responsabilidad deba recaer sobre los usuarios.

Julia Krämer (29 años) es profesora adjunta de Derecho de Protección de Datos en la Universidad Erasmus de Róterdam.

Chloé Berthélémy

2

EL CONTROL PRODUCE MONSTRUOS

Chloé Berthélémy (33 años) es asesora política sénior en European Digital Rights (EDRi), la mayor red de ONG de derechos digitales de Europa.

1 Para mí, la privacidad digital es una cuestión de justicia social. Protegerla significa trabajar por la igualdad, garantizando que las personas —especialmente las comunidades trabajadoras, *queer* y racializadas, históricamente marginadas— tengan realmente los medios para resistir los abusos, tanto del Estado como del sector privado, y para cuestionar a quienes ostentan el poder. Hoy, la manera en que se desarrollan y utilizan las tecnologías va en detrimento del interés público con demasiada frecuencia: amenaza el ejercicio de los derechos fundamentales de las personas, empeora sus condiciones materiales de vida y refuerza la discriminación contra las minorías. La privacidad es una herramienta para hacer frente a estos perjuicios derivados de la tecnología.



La investigadora cree que sin privacidad ni anonimato se potencia la desigualdad.

2 El nivel de explotación comercial de los datos se ha disparado. La industria de la tecnología publicitaria y de los intermediarios de datos, bastante opaca y cuya razón de ser es comprar y vender la atención de los usuarios mediante publicidad dirigida o contenido promocionado, todavía no ha sido regulada de manera eficaz. Es enorme la cantidad de datos que se recopilan, comparten y procesan para dirigir anuncios con un alto nivel de precisión y, a menudo, esto es algo desconocido para las personas aunque pueda utilizarse en su contra. Además, los nuevos servicios y productos digitales, especialmente los relacionados con la IA generativa, extraen enormes cantidades de datos personales y permiten una invasión masiva de la privacidad. Los riesgos y perjuicios, tanto para las personas como para las sociedades, siguen sin ser abordados adecuadamente por las autoridades. Otra forma de recopilación de datos especialmente preocupante es la vigilancia en el espacio público, con la proliferación de tecnologías de vigilancia biométrica, drones, cámaras corporales, seguimiento de ubicación, etc. Es extremadamente difícil ser anónimo en los espacios públicos, incluso cuando esto constituye una condición fundamental para ejercer derechos como el derecho a protestar o la libertad religiosa.

3 El abanico de datos recopilados es muy amplio: desde datos biométricos —rostro, forma de caminar, voz— hasta información muy íntima, como hábitos, estado de ánimo, estado de salud, red social, preferencias sexuales... Las tecnológicas los recopilan para la industria de la publicidad *online* y para entrenar sus modelos de IA. Los organismos encargados de hacer cumplir la ley y los servicios de inteligencia están interesados en acceder a estos datos para ejecutar sus labores de vigilancia y control.

4 **1.** Conoce los límites de las herramientas que usas para tomar decisiones informadas sobre qué compartir. Si estás comprometido, abandona los productos de GAFAM —Google, Amazon, Meta, Apple y Microsoft— y elige alternativas como GrapheneOS, Linux, NextCloud, Signal... El kit de Surveillance Self-Defense de la EFF es un buen arranque. **2.** Encripta, encripta, encripta. **3.** Recuerda que ningún sistema de privacidad digital es infalible.

“La recopilación de datos en el espacio público es especialmente preocupante”

Maya Thomas

3

CONVIENE VIGILAR AL VIGILANTE

Maya Thomas (28 años) es responsable de Asuntos Jurídicos y Políticos en Big Brother Watch, ONG británica que busca reducir el Estado de vigilancia.

1 Con demasiada frecuencia, los políticos asumen que las tecnologías que facilitan la privacidad digital son herramientas para cometer delitos. Es una suposición peligrosa. Herramientas como el cifrado de extremo a extremo y las VPN protegen a una enorme variedad de personas, incluidos periodistas, manifestantes, denunciantes, víctimas de violencia doméstica... La posibilidad de comunicarse de forma anónima es parte fundamental de vivir en democracia y debe protegerse. Intento mostrar a los políticos que privacidad y seguridad no son opuestos; la privacidad es justo lo que hace posible una verdadera seguridad.

“La posibilidad de comunicarse de forma anónima es parte fundamental de la democracia”



El trabajo de Thomas se centra en la privacidad, los derechos digitales y los derechos de protesta.

2 La mayoría sabe que las grandes tecnológicas *cosechan* datos personales y, por desgracia, lo ha acabado aceptando. Ahora existe una indignación justificada por la cantidad de datos de menores que han recopilado las plataformas. La ironía es que la respuesta política que han elegido los gobiernos constituye una nueva exigencia de datos. Para identificar a los menores, que tienen derecho a una protección especial, están exigiendo la presentación de documentos de identidad o la realización de un escaneo facial biométrico basado en IA. Estas medidas se presentan como mecanismos de verificación de la edad con fines de seguridad y no como procedimientos de recopilación de datos, por lo que la mayoría no se dan cuenta de que los riesgos de ataques informáticos, filtraciones, vigilancia y rastreo son los mismos.

3 Los documentos de identidad no pueden anonimizarse, y una filtración puede revelar el nombre, la fecha de nacimiento y, a menudo, la dirección. Los escaneos faciales biométricos generan datos únicos que un usuario no puede cambiar, salvo que se someta a una cirugía estética. En las manos equivocadas, pueden utilizarse para crear imágenes o vídeos *deepfake*, o para eludir sistemas de reconocimiento facial de otros servicios, como las *apps* bancarias. Hay muchos ejemplos de datos utilizados para la verificación de edad que han sido comprometidos: en 2024, la empresa de verificación de identidad AU10TIX, utilizada por TikTok y X, dejó expuestas credenciales de administrador durante más de un año. En 2025, se filtraron documentos de identidad de 70 000 usuarios de Discord. La *app* para mujeres Tea sufrió una filtración en la que más de 72 000 documentos de identidad y selfis de verificación fueron subidos a 4chan, pese a que se había informado de que estas imágenes se eliminarían. .

4 **1.** Utiliza servicios cifrados y VPN para limitar la información que puede recopilarse o interceptarse. **2.** Lee los permisos de las *apps* antes de concederlos, desactiva los identificadores de seguimiento publicitario y desactiva el acceso a la ubicación y al micrófono en *apps* que no lo necesiten. **3.** (Re)descubre tecnologías analógicas como vinilos, cámaras y diarios en papel. No solo es un rechazo al capitalismo de la vigilancia, sino también una manera de recuperar experiencias que no dejan ningún rastro de datos.

4

Paula Lamo

LA AMENAZA ESTÁ DENTRO DE CASA

Paula Lamo (38 años) es doctora en Ingeniería Industrial en el ámbito de las Tecnologías de Diseño y Producción Industrial.

1 Trabajo en el ámbito de internet de las cosas (IoT), con dispositivos conectados, redes IoT, identidad digital, arquitecturas distribuidas y gobierno del dato. Mi investigación se centra en garantizar la trazabilidad de la información en sistemas en los que intervienen multitud de máquinas y actores. Mi visión de la privacidad también abarca los datos que recogen los objetos que nos rodean.

2 Un reloj inteligente sabe a qué hora despertamos, cuánto dormimos y cuándo hacemos ejercicio. Un coche conectado genera información de trayectos, horarios y forma de conducir. Cualquier dispositivo domótico habla de cuándo estamos en casa. Un solo dato no es un problema; si son muchos y se correlacionan, el problema es mayor.



La especialidad de esta investigadora es la gobernanza del dato.

3 Hay datos evidentes: nombre, DNI, teléfono, *email*, fotos, información bancaria o información sanitaria. Pero, desde un punto de vista tecnológico, son igual de interesantes otros que parecen menos personales: dirección IP, identificador de un dispositivo, ubicación, hora de conexión, datos de sensores, historial de navegación, patrones de consumo o interacción con una aplicación. Saber que una bombilla inteligente se ha encendido no parece un dato sensible. Pero disponer durante meses de los horarios de encendido y apagado de todas las luces de una vivienda puede permitir deducir cuándo hay alguien en casa, cuándo se acuesta o cuándo está de vacaciones. ¿Quién utiliza esos datos? Primero, la empresa que presta el servicio. Pero pueden intervenir terceros (proveedores de infraestructuras, servicios en la nube, herramientas de analítica, plataformas publicitarias u otros), dependiendo del servicio, de los permisos y de las bases jurídicas aplicables. ¿Y para qué? Para prestar y mejorar los servicios, detectar fraudes, garantizar la seguridad, hacer analíticas, personalizar la publicidad o los contenidos, automatizar las decisiones, entrenar determinados sistemas o desarrollar nuevos productos. Por eso, no es suficiente con almacenar la información de forma segura. Hay que poder determinar quién accede, para qué, durante cuánto tiempo y qué sucede con ella a lo largo de todo su ciclo de vida. No hace falta desaparecer de internet para tener privacidad. Hace falta saber qué información estamos generando y decidir cuál queremos compartir. En esto consiste la gobernanza del dato.

4 **1.** Revisar los permisos del móvil. Ir a las apps y comprobar quién tiene acceso a ubicación, cámara, micrófono, fotografías y contactos. Y aplicar una regla: si una aplicación no necesita ese dato para funcionar, no debería tener acceso. **2.** Proteger las cuentas, no solo las contraseñas. Contraseñas distintas para servicios distintos, gestor de contraseñas y autenticación en dos pasos si es posible. **3.** Inventariar nuestra vida conectada: televisión, cámaras, reloj, altavoz, aspirador, juguetes, electrodomésticos, coche... Cambiar las credenciales que vienen por defecto, actualizar los dispositivos y desactivar los servicios que no utilizamos.

“Hay que saber qué información estamos generando y decidir cuál queremos compartir”

1 Me interesan la digitalización de los servicios públicos, especialmente cómo afecta a los derechos de las personas, y cómo la complejidad tecnológica puede ocultar políticas discriminatorias. La capacidad de las personas para proteger su derecho a la privacidad digital solo ha empezado a desarrollarse en los últimos tiempos. Aunque de vez en cuando se sigue afirmando que la protección de datos y el derecho a la privacidad están muertos, ambos continúan evolucionando. Espero, y trabajo para que así sea, que estos derechos sean más accesibles y eficaces a la hora de abordar las consecuencias de experimentos tecnológicos fallidos para la ciudadanía.

“Los datos dejan huella digital y pueden afectar al acceso a servicios públicos”

2 Los datos que se comparten dejan una huella digital en internet y pueden afectar al acceso a derechos y servicios públicos. La nueva era de la inteligencia artificial significa que las autoridades públicas están intentando tomar decisiones combinando y cruzando toda la información disponible sobre las personas. Cada elemento de información disponible *online*, incluidas las redes sociales, los perfiles de aplicaciones de citas y los itinerarios de viaje, puede utilizarse para evaluar a una persona. Por ejemplo, en todo el mundo se está denegando a personas el acceso a prestaciones sociales porque las autoridades detectan supuestos fraudes a partir de la información disponible sobre ellas en internet. En múltiples casos, esta elaboración de perfiles digitales ha dado lugar a actuaciones policiales discriminatorias contra los grupos minoritarios y a que se *oculten* las razones de determinadas decisiones. Sin embargo, cuando se analizan estos sistemas, se observa que las autoridades públicas intentaron utilizar *soluciones técnicas* como atajo para prestar servicios de manera más eficaz, en lugar de abordar de manera significativa problemas como el racismo y la misoginia.



Lanneau advierte de los peligros de digitalizar los servicios públicos.

3 No todos experimentamos la digitalización y la vigilancia de la misma manera. Las trabajadoras y los trabajadores sexuales, las personas racializadas, las solicitantes de asilo y las personas inmigrantes son los ‘canarios en la mina’. Son quienes sufren primero el impacto y padecen los experimentos de vigilancia digital más perjudiciales. Deberíamos aprender de su experiencia, porque las empresas siempre buscan ampliar la escala de estas tecnologías. Tenemos que decir que no desde el principio a la digitalización de los servicios públicos cuando esta no se realiza mediante procesos transparentes y participativos de consulta pública.

4 **1.** El primer paso es no votar a un gobierno que impulse la vigilancia digital y dé carta blanca a empresas privadas para experimentar con poco o ningún control. **2.** Recuerda que tienes derecho a la privacidad y a la protección de tus datos, y que puedes ejercerlos. Si estás en posición de poder hacerlo, abre camino a otros con menos oportunidades. **3.** Investiga el impacto de las herramientas digitales que usas o estás obligado a usar para acceder a los servicios públicos. Si por una cuestión de comodidad existe más riesgo, ¡cuestiónatelo!

Romain Lanneau (30 años) es un consultor independiente especializado en el impacto de la digitalización sobre las políticas públicas y el acceso a los derechos humanos.

DETECTOR DE FALLOS DEL SISTEMA

5

Romain Lanneau