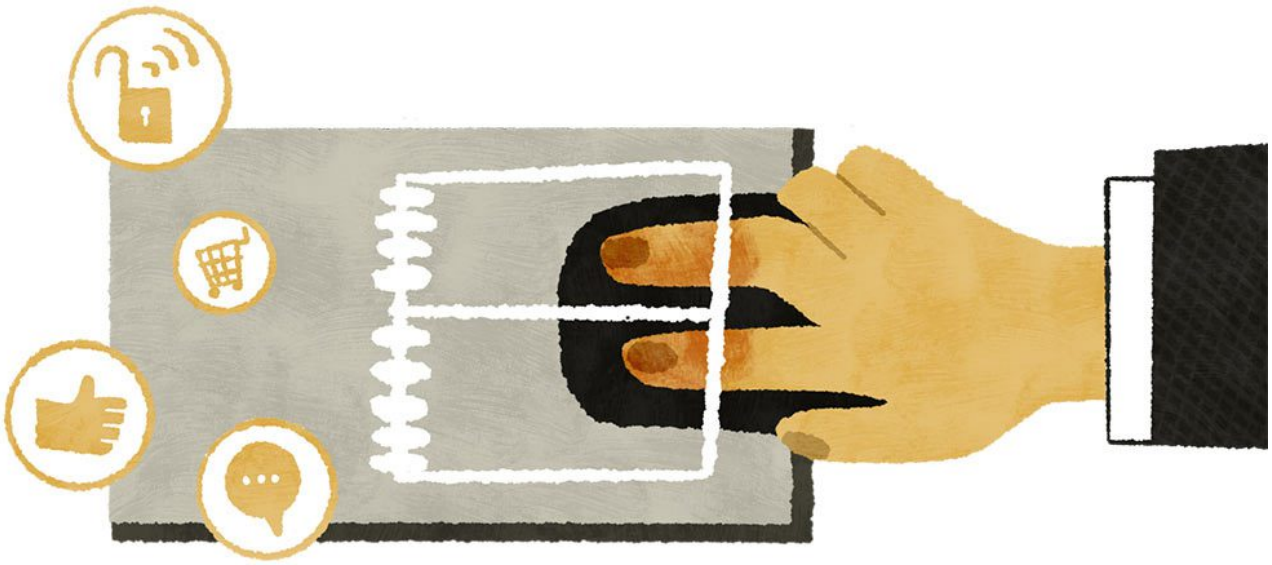
Los escenarios que amenazan tu privacidad

Es hora de formular nuevas teorías y tener una mejor formación en privacidad. Sigue leyendo antes de hacer clic en “aceptar todo”.



1 de enero de 2024

Por Tawfiq Alashoor

Son incontables las veces que cada día te topas con esta pregunta: ¿aceptas, rechazas o

personalizas las *cookies*? Tu elección dirá mucho de cómo concibes la privacidad. La mayoría dirá que le preocupa, aunque lo que hace realmente suele revelar una historia diferente.

Esta paradoja de la privacidad, la de "decir una cosa y hacer otra", explica por qué, en un estudio de 2018 realizado un mes después de la entrada en vigor del Reglamento General de Protección de Datos de la Unión Europea, el 76% de los internautas seguía haciendo clic en "aceptar todo" sin pensárselo dos veces. En la mayoría de los casos, el clic inconsciente es un comportamiento arraigado, ajeno a cualquier preocupación real sobre el uso de sus datos personales por parte de terceros.

Con todo, hay señales de que ese comportamiento está cambiando. Según una encuesta de 2021, menos del 32% de los usuarios aceptan siempre las *cookies* cuando abren una web, un porcentaje que desciende al 25% entre los 45 y 54 años. ¿Será que cada vez somos más conscientes de la necesidad de proteger nuestros datos en Internet?

La privacidad es el foco de mi investigación, concretamente en el ámbito digital, que suscita un sinfín de dudas a nivel personal, organizacional y social. La preservación de la privacidad se ha centrado en los ciberataques y las brechas de seguridad de datos, lo que nos ha concienciado sobre los peligros de la ciberestafa y la importancia de la protección de las contraseñas.

Pero hay otro aspecto de la privacidad que trasciende la seguridad de la información; tiene que ver con las pequeñas decisiones que tomamos a la hora de dar nuestros datos personales. Como el número de interacciones digitales que realizamos cada día se ha disparado, es preciso conocer y comprender mejor los factores que influyen en las decisiones de privacidad que tomamos para que sean mejores y acordes con nuestros valores.

El cálculo de la privacidad

La introducción de ChatGPT ha puesto el turbo a una tecnología que lleva con nosotros más de una década: los asistentes de voz. En comparación con ChatGPT, Siri (Apple) o Alexa (Amazon), son "más tontos que una piedra", decía recientemente el CEO de Microsoft, Satya Nadella, en el Financial Times.

Hoy, los chatbots de la IA generativa pueden hacer mucho más que poner una canción o apagar las luces cuando se lo pedimos; de hecho, conversan con nosotros. Pero, para eso, necesitan nuestros datos personales; cuantos más les proporcionamos, más relevantes y precisas son sus respuestas.

Durante la pandemia, el uso de chatbots en telemedicina devino indispensable para hacer diagnósticos y chequear la salud de los pacientes confinados, quienes debían estar dispuestos a compartir datos médicos privados a través de las aplicaciones. Habrá quien diga que se trata de una autodivulgación legítima, es decir, cada cual calcula su privacidad sopesando los costes de dar información sensible a cambio de recibir un beneficio mayor (atención médica).

Este pacto de reciprocidad es, precisamente, el objeto de una línea de investigación relacionada con la divulgación de datos. Los chatbots imitan las normas sociales de la conversación. Según estas, cuanta más información personal comparte un interlocutor, más obligado se siente el otro a corresponder con información sobre sí mismo. La confianza que se genera entre las partes da pie a una relación interpersonal.

Las empresas que recopilan datos tratan de replicar esta dinámica haciendo que los chatbots participen en conversaciones recíprocas. Pero hay una delgada línea entre animar a las personas a revelar más información sobre sí mismas de un modo que genere confianza y con una finalidad positiva y manipularlas para que cedan esa información privada. Esto último hace que se sientan explotadas, vulnerables o utilizadas y, a su vez, perjudica la utilidad global del sistema, incapaz de producir resultados fiables.

Junto con mis colegas de investigación, he analizado los entornos y las condiciones que influyen en que los usuarios den o no información privada. A continuación, resumo los hallazgos más importantes.

El efecto antropomórfico

El antropomorfismo es la atribución de cualidades similares a las humanas a algo que no lo es. Nuestro interés no recae tanto en la similitud de la voz de un chatbot con la humana como en el efecto que puede tener la interacción de los usuarios con la tecnología y su posterior nivel de confianza.

Para nuestro estudio, desarrollamos un chatbot llamado Amanda y realizamos dos experimentos: uno con un chat basado en texto y el otro en voz. Pedimos a los participantes que conversaran con Amanda, primero presentándose y después interactuando con preguntas y respuestas recíprocas.

En un grupo, Amanda compartió información como: “¿Sabes lo que me molesta? A veces, la gente pronuncia mal o, aún peor, hablan bajo y esperan que les entienda. Y a ti, ¿qué te molesta?”. Cuando la persona respondía, Amanda expresaba una reacción emocional diseñada para crear un alto grado de intimidad: “¡Cuéntamelo todo!”. En cambio, en el otro grupo restringía sus expresiones a la continuidad del proceso: “Vale, vamos con la siguiente pregunta”. Tras la interacción, los participantes rellenaron un cuestionario con el que

evaluamos la sucesiva confianza en los agentes conversacionales.

En ambos experimentos observamos que la participación del chatbot en una autodivulgación recíproca con cualidades más prototípicamente humanas incitaba a los usuarios a confiar más en el sistema. Eso sucedía tanto a nivel cognitivo (la decisión racional de confiar en el chatbot basada en la percepción de su competencia y capacidades de pensamiento superior) como afectivo (la decisión de confiar basada en la percepción de un vínculo emocional o sentimientos de empatía o afinidad).

Elementos conversacionales a mejorar

Este hallazgo puede ayudar a los desarrolladores de chatbots a mejorar los elementos conversacionales de sus aplicaciones; en concreto, aquellos en los que la autodivulgación recíproca y la confianza son fundamentales para la prestación de servicios críticos, como la atención médica.

A su vez, los usuarios deben ser conscientes de que los cibercriminales, por ejemplo, pueden explotar estos mismos rasgos para manipularlos y hacer que tomen decisiones de divulgación que no se corresponden con sus preferencias de privacidad.

Por un lado, el que los chatbots antropomórficos sintonicen más con el género, la etnia o el acento del usuario ayuda a hacerlos más cercanos y procura una experiencia más personalizada e intuitiva.

Por el otro, el uso del antropomorfismo para manipular la autodivulgación –llevar a los usuarios a una falsa sensación de familiaridad para que revelen más de la cuenta sobre sí mismos– no es transparente y plantea toda una serie de problemas éticos relacionados con la privacidad.

Cuando bajamos la guardia

En otro estudio premiado realicé, junto con otros colegas, una serie de experimentos para probar el efecto de varios factores contextuales en la disposición de los usuarios a compartir información personal en Internet.

Primero comprobamos el efecto de la saturación mental o el cansancio, pues solemos bajar la guardia cuando estamos cognitivamente agotados. Reunimos a los participantes, tras medir sus preocupaciones de privacidad y su propensión a compartir información personal. Les dimos un reportaje sobre una aplicación de salud –con el pretexto de que eran decisivos para su desarrollo– para que hicieran una serie de tareas de lectura y redacción pensadas para agotarlos. Luego les pedimos que describieran su estado de ánimo con adjetivos que iban de feliz y contento a harto y enfadado. Con estos datos, medimos su comportamiento de divulgación real. Repetimos el experimento dos veces, una para manipular el estado de ánimo de los usuarios y otra para manipular tanto este como su agotamiento.

Los experimentos revelaron los factores contextuales que influyen en nuestra propensión a actuar o no de acuerdo con nuestros intereses de privacidad. La paradoja de la privacidad es real, aunque depende de la combinación de factores externos (cognitivos) e internos (estado de ánimo). No es solo que las personas cognitivamente agotadas sean más propensas a compartir en exceso, pese a las preocupaciones de privacidad que dicen tener, sino que, cuando además están de buen ánimo, aumenta esa propensión.

La paradoja de la privacidad

Imagínate un viernes por la noche tras una semana agotadora. ¡Por fin viernes! Coges el móvil y empiezas a interactuar animadamente en las redes sociales. Aquí es cuando podrías hacer clic en “aceptar todo” sin pensártelo y relajarte con una divertida encuesta online en la que dejas fluir una verdadera mina de oro de información sobre lo que te gusta, lo que no, tus rasgos de personalidad y tus opiniones políticas. Algo impensable cuando estás mentalmente alerta y de mal humor.

Un inciso: esto no significa que sea preferible el afecto negativo. Otras investigaciones muestran que los usuarios con una predisposición negativa o frustrados pueden ser más propensos a violar las políticas de seguridad en Internet. Como explico más adelante, el contexto importa.

Los peligros de compartir información privada cuando no lo deseamos pero estamos demasiado relajados quedaron de manifiesto en otro estudio, en el que, junto con colegas de *Copenhagen Business School*, empleé técnicas de respiración para aliviar el estrés. Tras hacer una serie de ejercicios respiratorios, los participantes respondieron preguntas sobre

demografía, salud, estilo de vida y otros datos personales. Las conclusiones indican que es más probable que revelemos información personal cuando estamos relajados que cuando nuestro estado de ánimo es neutro.

Sé proactivo en privacidad

Necesitamos entender el impacto de los factores psicológicos y ambientales en nuestras decisiones de privacidad y cómo estas podrían acabar contradiciendo nuestras preferencias si no tenemos cuidado. Deberíamos activar el cerebro y esforzarnos más cuando procesamos información e interactuamos en Internet.

Las empresas también tienen la responsabilidad de equilibrar las posibles ganancias económicas que podrían obtener explotando los datos de los usuarios con su deseo (y derecho) de privacidad. Cada vez hay más webs que cambian sus métodos de recopilación de datos y ofrecen avisos de privacidad emergentes –a veces, de forma granular para seguir navegando–. Con ello, facilitan las decisiones de privacidad de los internautas (aunque algunas opciones son tan exhaustivas que llevan al usuario a abandonar la web o a rendirse y "aceptar todo" debido, una vez más, a la saturación mental).

La regulación sobre privacidad ya surte efecto en empresas y usuarios. Eso debería traducirse en una mejor protección de la privacidad, aun cuando ambas partes la configuren porque no les queda otra, no por convencimiento o concienciación.

SETA vs. PETA

Pese a algunos avances, aún queda mucho por hacer a nivel legislativo. El reglamento de la UE y algunas leyes sobre la privacidad del consumidor en ciertos estados de Estados Unidos constituyen pasos importantes para inculcar la idea de protección de la privacidad en la opinión pública. Pero me preocupa que, con respecto a la protección de la información, se ponga el énfasis en los programas de educación, formación y concienciación en seguridad (SETA, por sus siglas en inglés); es decir, que la información sobre seguridad se limite a los mecanismos técnicos de protección.

Nos enseñan a tener cuidado con las contraseñas, las actualizaciones de software, la

verificación en dos pasos, las ciberamenazas..., pero hay otro nivel de la protección de la información que también merece atención. De ahí que defienda la necesidad de introducir programas de educación, formación y concienciación en privacidad, o PETA, que complementen a los SETA.

Así lo demuestra otro estudio en el que organizamos un curso SETA sobre riesgos y protecciones de seguridad de datos. Dividimos a los participantes en dos grupos y solo a uno se le impartió una lección recordatoria sobre privacidad. Todos completaron tres encuestas –antes, después y a las dos semanas de la formación– con preguntas como: "¿Usas la misma contraseña en todas las webs? ¿Usas tu cumpleaños como contraseña? ¿Compartes datos personales en las redes sociales?". Mientras que un grupo podía responder sí o no o saltarse las preguntas, el otro podía contestar sí o no o elegir una tercera opción, "Prefiero no dar esa información", con lo que se les hacía explícitamente conscientes de su capacidad para retener información privada.

Tal y como esperábamos, quienes recibieron la lección recordatoria compartieron menos información personal que quienes no. La sorpresa fue que tanto los unos como los otros siguieron revelando información muy sensible; un hallazgo alarmante que refuerza mi llamamiento a favor de los programas PETA.

¿En qué se diferenciaría un programa PETA?

- Para empezar, explicaría la distinción entre privacidad y seguridad.
- A continuación, formaría en la psicología y economía conductual de las decisiones de privacidad, relacionadas con cuestiones tratadas en este artículo.
- Por último, propiciaría un debate a fondo sobre las teorías de la privacidad y la importancia de la regulación y las buenas prácticas en esta área.

Lo más importante es que haya un pensamiento a dos niveles, lo que el Nobel Daniel Kahneman describió como sistema 1 y sistema 2 en su libro Pensar rápido, pensar despacio. En su mayor parte, el pensamiento es automático, intuitivo y menos consciente (sistema 1), como hacer clic en "aceptar todo" sin pensar en las consecuencias.

El objetivo de los programas PETA sería acostumbrarnos a un pensamiento más lento, deliberado y consciente (sistema 2), como hacer pausas para procesar la información relacionada con una decisión de privacidad y, de ese modo, sopesar los posibles pros y contras de permitir que terceros nos rastreen en Internet. Si los errores humanos siguen siendo la mayor causa de las brechas de ciberseguridad, parece una vía de progreso

razonable un programa que nos enseñe a resistir la fatiga de la privacidad y nos dote de modelos mentales para decidir de forma informada.

La relatividad de la privacidad

En 2023, un médico australiano, Graeme Siggs, vio por televisión una entrevista a un profesor, Dan Angus. Tras advertir una mancha marrón en la mejilla de este, Siggs, especialista en cáncer de piel, buscó en Internet viejas fotos del individuo y pudo comprobar que la mancha había crecido. Contactó con el profesor y le urgió a chequeársela. Resultó ser un melanoma, que se operó con éxito. Todo gracias a la búsqueda de Siggs en Internet.

¿Estamos ante una violación de la privacidad? Después de todo, el profesor no había consentido aquel uso de sus fotos por parte de un extraño. Este caso ilustra una nueva teoría que estoy elaborando, que he llamado "teoría de la relatividad general de la privacidad". Dándole un giro a la "teoría general de la relatividad" de Einstein –por la que todos los estados son relativos según el continuo espacio-tiempo–, propongo que la privacidad es relativa según el continuo contexto-tiempo.

Piénsalo: aunque es cierto que el espacio, como la geolocalización, te identifica en el mundo digital, el factor más determinante de tu presencia online en cuanto a privacidad es el contexto. La salida a la luz de las fotos de Angus, aunque violara sus preferencias de privacidad, le benefició en ese contexto específico, algo que él mismo reconoció cuando agradeció a Siggs haberle salvado la vida.

En cambio, los viejos chistes verdes del humorista estadounidense Kevin Hart, que tal vez no ofendieron a muchos en 2009, dejaron de resultar graciosos cuando se repitieron en 2019. Hart tuvo que disculparse y renunciar a presentar los Óscar de ese año. Sin duda, el contexto era diferente. Las normas sociales y las leyes de privacidad cambian. Además, el tiempo en el mundo digital es un constructo atemporal: las fotos, vídeos y publicaciones del pasado están perennemente presentes, pero nuestra percepción cambia según el contexto.

Pongamos por caso otro escenario: una plataforma digital usa la IA para generar anuncios personalizados. Su éxito y acogida dependen sobre todo del contexto y el momento de su aparición. Por ejemplo, un anuncio de ropa deportiva podría resultarte oportuno si acabas de interesarte por eso mismo en Internet o parecerte intrusivo si te salta en medio de una conversación privada con un amigo en una aplicación de mensajería.

A tenor de mis hallazgos sobre el carácter dinámico del significado y valor de los datos personales, que cambian según factores situacionales (cognición, emoción, ética, etc.), creo que la "relatividad general de la privacidad" constituye un nuevo e importante rumbo para futuras investigaciones. Mientras, todos deberíamos dedicar tiempo a reflexionar profunda y seriamente sobre el concepto de privacidad en los ámbitos personal y laboral.

Los directivos de productos y servicios, sobre todo aquellos cuyos modelos de negocio dependen de los chatbots y la IA, deberían priorizar las medidas y procedimientos de privacidad, prestando especial atención al continuo contexto-tiempo al desarrollar procesos. Los directivos y directores de tecnologías de la información con visión de futuro deberían adoptar una mentalidad de "privacidad por diseño". Pregúntate: ¿tus avisos emergentes ayudan de verdad a los usuarios a pensar bien en sus opciones de privacidad y a tomar decisiones acordes con sus valores? ¿O los estás agotando o manipulando de forma poco ética para que cedan más datos personales?

En lugar de malgastar su presupuesto anual en programas SETA inefectivos, las organizaciones deberían invertir en mejores programas PETA que capaciten a las personas para hacer cálculos de privacidad más eficaces. Esto podría ayudar a los departamentos de atención al cliente, por ejemplo, a mejorar las solicitudes de información por motivos de autenticación, reduciendo así la suplantación de la identidad y evitando las amenazas de ciberseguridad y los ciberataques.

La privacidad y los datos personales están destinados a ser una moneda aún más valiosa y, con el tiempo, la base de una "puntuación de la confianza". Apple lleva varios años haciéndolo: "puntúa" la navegación, compras, búsquedas y descargas de los usuarios en función de un registro histórico de sus actividades digitales para prevenir el fraude y otras actividades maliciosas.

Nos encontramos en la cúspide de una nueva y revolucionaria edad de la privacidad digital. ¿Qué harás la próxima vez que te pidan que aceptes todas las *cookies*?

Fuentes:

"My name is Alexa. What's your name? The impact of reciprocal self-disclosure on post-interaction trust in conversational agents", de Kambiz Saffarizadeh, Mark Keil, Maheshwar Boodraj y Tawfiq Alashoor. Journal of the Association for Information Systems (2023).

"Too tired and in too good of a mood to worry about privacy: explaining the privacy paradox

through the lens of effort level in information processing", de Tawfiq Alashoor, Mark Keil, H. Jeff Smith y Allen R. McConnell. Information Systems Research (2022). Este artículo ha sido reconocido como mejor artículo publicado por la Communication, Technology & Organization (CTO) Division of the Academy of Management (AOM).

"Take a deep breath and tell me all about it: an experimental study on the effect of breathing on privacy decisions", de Tawfiq Alashoor, Andreas Blicher y Rob Gleasure. 15º aniversario del NeuroIS Retreat (2023).

"An online randomized field experiment on the importance of Privacy Education, Training & Awareness (PETA)", de Tawfiq Alashoor et al. 3ª Conferencia Internacional sobre Computación y Tecnologías de la Información (ICCIT, 2023).

"It is seriously time for Privacy Education, Training & Awareness (PETA) programs", de Tawfiq Alashoor, de próxima aparición como capítulo del libro *Effective methods for teaching business-related topics during and post crisis*.

"Mind your digital grave: how digital traces mutate into digital zombies", de Mazen Shawosh, Tawfiq Alashoor y Nicholas Berente. TREO (siglas en inglés de tecnología, investigación, educación y opinión) Talks, celebradas junto con la 43ª Conferencia Internacional sobre Sistemas de Información (2022).

Una versión de este artículo se publica en IESE Business School Insight 166 (enero-abril 2024).

https://www.youtube.com/embed/IRfpW0WKY0k

Array

Tawfiq Alashoor

Profesor de Operaciones, Información y Tecnología en el IESE. Su investigación se centra en la toma de decisiones de privacidad y ciberseguridad en tecnologías emergentes apoyadas en la IA, como aplicaciones, agentes conversacionales y robots.

www.iese.edu/es/insight