Cuidado con los zombis digitales: cómo gestionar los fantasmas del pasado online

Un nuevo estudio sobre los zombis digitales –esos contenidos que publicaste en su día en internet y ahora se te vuelven en contra– insta a repensar el concepto de privacidad.



1 de septiembre de 2024

Cuando al humorista estadounidense Kevin Hart le ofrecieron presentar la gala de los Premios Óscar de 2019, seguramente lo último en lo que pensaba eran los tuits que había

©IESE Business School

publicado diez años antes. Pero los sabuesos de internet no tardaron en desenterrar una serie de chistes homofóbicos que había tuiteado y que terminaron por arruinar sus posibilidades de presentar los Óscar.

Se trata del típico ejemplo de zombi digital. Así se denominan los contenidos publicados en el pasado, dirigidos a menudo a un público y en un contexto determinados o en un momento en el que no se los consideraba problemáticos, pero que resurgen más tarde y suponen un quebradero de cabeza para su autor.

Una nueva investigación del profesor del IESE Tawfiq Alashoor –junto con Mazen Shawosh (King Fahd University), Nicholas Berente (Universidad de Notre Dame) y Thomas Grisold (Universidad de St. Gallen)– estudia qué puede ocurrir cuando los zombis digitales resucitan y se le giran en contra al usuario, desde el hundimiento de su reputación hasta cuestiones legales y amenazas a su persona.

Las 5 etapas de un zombi digital

Los autores resumen el ciclo de vida de un zombi digital en cinco etapas:

1. **Nacimiento.** Cuando publicas cualquier cosa en internet creas una huella digital, es decir, un contenido que tiene asignada una marca de tiempo y está vinculado a un contexto determinado. Incluso tus desplazamientos por la pantalla dejan para siempre vestigios de tu perfil psicográfico.
2. **Latencia.** La huella digital puede permanecer latente durante meses o años, al tiempo que cambia el contexto social y jurídico, el llamado “espíritu de la época”.
3. **Resurrección.** Tras ese cambio de contexto, es posible que la huella digital resurja, como cuando otras personas hurgan en el historial online de un usuario. Un mensaje latente resucitado puede cobrar vida propia, y es entonces cuando la huella muta en zombi digital.
4. **Posresurrección.** El autor del contenido interviene retroactivamente para gestionar (bien o mal) el resurgimiento de esa huella digital.
5. **Muerte.** Sobreviene cuando se produce algún efecto, como la pérdida del trabajo, que es lo que le ocurrió a Kevin Hart.

Hay que destacar que el efecto inicial no tiene por qué ser el desenlace. Tal vez haya una desescalada de la reacción al zombi y la opinión pública se olvide de ello. Y es que los zombies pueden volver arrastrándose a su tumba, como le sucedió al director de cine James Gunn, que fue despedido por Disney a causa de su zombi digital y recontratado cuando la

©IESE Business School

indignación remitió.

¿Seguro que no tienes esqueletos en el armario?

Aunque los autores han estudiado los casos de tres personalidades de alto perfil mediático (Kevin Hart, James Gunn y Alexi McCammond), se muestran partidarios de ampliar el debate más allá de los titulares de prensa. Un zombi digital no solo está relacionado con discursos homofóbicos, racistas, sexistas o de odio en internet. De hecho, puede surgir de contenidos mucho más sutiles que le parezcan inofensivos al usuario.

Hasta las opiniones "seguras" pueden convertirse en un problema. La Primavera Árabe es un ejemplo dramático de cómo lo "aceptable" puede volverse "inaceptable" cuando cambian el momento y el contexto. Los mensajes que los manifestantes antigubernamentales, esperanzados con la posibilidad de un cambio real, publicaron en las redes sociales les causaron no pocos problemas, incluida la cárcel, cuando el movimiento prodemocrático se desinfló.

La mayoría de las personas protegen su privacidad digital evitando publicar su número de teléfono o dirección en internet, pero luego opinan sin filtro en foros. La sobreexposición en redes sociales se ha normalizado tanto que muy pocos piensan en cómo ha cambiado el concepto de privacidad, que hoy día es mucho más que proteger nuestros datos personales. Debemos tener en cuenta que la privacidad depende del continuo contexto-tiempo y, asimismo, que fenómenos como el de los zombis digitales constituyen un problema cada vez mayor por las consecuencias imprevistas y no deseadas que tienen.

Todos dejamos huellas digitales, desde las historias que hemos leído hasta los vídeos que hemos visto y durante cuánto tiempo. Un estudio sobre Facebook ha demostrado que las características personales de los usuarios, como sus creencias religiosas u orientaciones políticas, pueden predecirse con precisión a partir de solo diez *likes*. Los usuarios casi nunca se preguntan qué perfil psicográfico están creando con su actividad diaria online.

Cada vez que cambian el contexto y el momento, nuestras huellas digitales se ven con otra luz, algo para lo que no estamos preparados. Incluso las leyes de privacidad, como el Reglamento General de Protección de Datos de la Unión Europea, son insuficientes. Como estas normativas tardan mucho en elaborarse e implementarse, lo que nos protege hoy

©IESE Business School

puede ser ineficaz mañana. Incluso el “derecho al olvido”, por el que una persona puede exigir el borrado de sus datos personales, no impide las capturas de pantalla o que esa información se archive en la Wayback Machine.

Mejora tus herramientas para neutralizar a los zombis digitales

No solo las personas sufren las consecuencias; también las empresas deben hacer frente al riesgo reputacional. Los zombis digitales pueden comprometer el apoyo público de una celebridad o el nombramiento de un CEO, paralizar proyectos, productos y eventos y, en definitiva, afectar a la cuenta de resultados. Las típicas estrategias de gestión en tales circunstancias no bastan para neutralizar a los zombis digitales:

- **Ignorarlos.** Aunque la estrategia de hacer caso omiso de la indignación tal vez funcione, pues la capacidad de atención actual es menor, también puede resultar contraproducente. El silencio podría ser interpretado como una muestra de apoyo, lo que no haría sino alimentar al zombi.
- **Negarlos.** Borrar el mensaje y dar una explicación creíble del contexto original puede servir de ayuda. En el caso de James Gunn, surgió un contramovimiento en su defensa que al final condujo a su rehabilitación. Dicho esto, a veces los desmentidos pueden contribuir a que el zombi siga coleando.
- **Aceptarlos y disculparse.** Admitir el error cometido y pedir disculpas es una estrategia tan sencilla como razonable. Pero hay ocasiones en las que tampoco basta, como pudo comprobar la periodista Alexi McCammond. Tras pedir perdón, acabó dimitiendo de su puesto como editora de *Teen Vogue*.

Donde hay riesgo también hay oportunidad

Las limitaciones de estas estrategias subrayan la urgencia de enfocar de un modo más integral la gobernanza de datos y la gestión de la privacidad, no solo de personas y organizaciones, sino de la sociedad en su conjunto. Los autores se suman al llamamiento a “concebir la toma de decisiones sobre privacidad en la era digital con sensibilidad hacia el contexto y en sintonía con el momento”.

A su criterio, debemos dejar de contemplar las huellas digitales como algo neutro y concebirlas, a ellas y sus implicaciones, dentro de su contexto social más amplio, ligado a los

©IESE Business School

valores y normas específicos de cada periodo histórico y cada acontecimiento social y político.

¿Cómo cambiaría esta nueva concepción el modo en que abordamos los datos?

Por un lado, las redes sociales están diseñadas para mostrar los mensajes cronológicamente, de modo que los antiguos van quedando relegados a medida que pasa el tiempo. Este formato posibilita que las huellas digitales se amontonen en una "tumba digital". En lugar de apoyarse en el "ojos que no ven, corazón que no siente", las redes sociales deberían facilitar a los usuarios el acceso a sus huellas digitales para que puedan borrarlas o gestionarlas como crean conveniente.

Dado el carácter impredecible de las huellas digitales –no podemos saber cuáles mutarán en zombi digital–, los diseñadores de las redes sociales deben esforzarse por prever mejor los riesgos potenciales, así como integrar en sus arquitecturas soluciones para los usuarios.

Por otro lado, es preciso que los usuarios entiendan la realidad de los zombis digitales y las cinco etapas de su ciclo de vida. También deberían estar al tanto de los cambios sociales para prepararse y gestionar de forma planificada cualquier posible consecuencia.

Existe ya un mercado de proveedores de soluciones de gestión avanzada de la privacidad. Empresas como ReputationDefender y BrandYourself mitigan los perjuicios causados por los zombis digitales mediante la supresión de la información negativa, la divulgación de contenidos positivos y el asesoramiento en materia de privacidad digital.

Los navegadores de internet también tienen un papel que desempeñar. Los motores de búsqueda que reducen la recogida de datos y el intercambio con los anunciantes, como Brave, marcan la pauta respecto a la privacidad, lo que de algún modo presiona a los demás para que sigan su ejemplo. Hay margen de sobra para que el sector tecnológico transforme el problema de los zombis digitales en una oportunidad para innovar.

Al final, es posible que la gestión de la privacidad por parte de los usuarios solo cambie significativamente cuando perciban que sus datos personales tienen un valor monetario tangible, es decir, cuando la privacidad dé dinero.

Esta posibilidad casa con la tendencia de los usuarios a pedir una mayor transparencia y control del uso de sus datos. Si la gente participara de la gestión de sus datos, tendría un

©IESE Business School

mayor incentivo para protegerlos de manera proactiva.

+ INFO: Los escenarios que amenazan tu privacidad

https://www.youtube.com/embed/pzLhk440A1A?list=PLu80P54BN4lMS5tT0QbsEq9se310t5D5L

https://www.youtube.com/embed/IRfpW0WKY0k?si=_YDs_7A6sBQTLjI7



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.

©IESE Business School