

Big Data te está observando.

Por: Pressenza. 04/06/2018

Aquí se publican otra vez artículos de [The Conversation](#) que muestran la necesidad de mantenernos vigilantes ante los que las redes sociales están haciendo con la información que compartimos.

Cuatro maneras en las que tus búsquedas en Google y redes sociales afectan tus oportunidades en la vida.

[Lorna McGregor, University of Essex](#), [Daragh Murray, University of Essex](#) y [Vivian Ng, University of Essex](#)

Ya sea que te hayas dado cuenta o hayas dado tu consentimiento, o tal vez no, “big data” puede afectar la forma en la que vives tu vida. Cuando usamos las redes sociales, [navegamos en Internet](#) o usamos seguidores de actividad o “fitness trackers” para monitorear nuestra forma física y las calorías que quemamos haciendo ejercicio, creamos datos que son recolectados, categorizados y [usados por compañías](#) y por [el estado](#) para crear perfiles sobre nosotros. Estos perfiles se usan para orientar anuncios de productos y servicios hacia quienes tienen más probabilidades de comprarlos, o para informar a los gobiernos y para que de acuerdo con eso tomen decisiones.

Big data permite que los estados y las compañías tengan acceso, combinen y analicen nuestra información y construyan perfiles de nuestra vida que son reveladores pero [incompletos](#) y probablemente [imprecisos](#). Esto es posible mediante la identificación de correlaciones y patrones en los datos sobre nosotros y sobre las personas con perfiles similares al nuestro, con el fin de hacer predicciones sobre nuestros comportamientos.

Pero el hecho de los análisis de big data estén basados en algoritmos y estadísticas no quiere decir que sean [precisos, neutrales o inherentemente objetivos](#). Y aunque big data puede proporcionar información sobre el comportamiento en conjunto de las personas, esta no es necesariamente una manera confiable de determinar el comportamiento individual. De hecho, estos métodos pueden [abrir la puerta a la discriminación](#) y a la [amenaza de los derechos humanos](#), podrían incluso estar

trabajando en contra de las personas. Estos son cuatro ejemplos de cómo los análisis de big data pueden conducir a la injusticia.

1.

Cálculo de calificación crediticia

Big data puede usarse para tomar decisiones sobre la [elegibilidad crediticia](#), lo que decidirá si a alguien se le concede una hipoteca o qué tan altas deben ser las primas de un [seguro para automóviles](#). Estas decisiones pueden ser informadas mediante [publicaciones en redes sociales](#) y los datos de otras aplicaciones que se toman para indicar el nivel de riesgo o de confiabilidad de alguien.

Pero datos como la formación académica o el lugar de residencia pueden no ser relevantes o fiables para dichas evaluaciones. Este tipo de información puede actuar como un indicador de la raza o el nivel socioeconómico, y su uso para tomar decisiones sobre el riesgo de crédito podría generar discriminación.

2.

Búsquedas de trabajo.

Big data puede usarse para determinar [quién ve un anuncio de trabajo o se preselecciona para una entrevista](#). Los anuncios de empleo pueden estar dirigidos a grupos de edad específicos, [como los de 25 a 36 años](#), lo que excluye a los trabajadores más jóvenes y mayores de incluso ver ciertos puestos de trabajo, además que presenta un riesgo de discriminación por edad.

La automatización también se usa para hacer que filtrar, sortear y clasificar candidatos sea más eficiente. Pero este proceso de selección puede excluir a personas en base a indicadores como la [distancia de su viaje diario](#). Los empleadores pueden suponer que aquellos con un viaje más largo tienen menos probabilidades de permanecer en un empleo a largo plazo, pero esto puede usarse para discriminar a las personas que viven más lejos del centro de la ciudad debido a la ubicación de viviendas asequibles.

3.

Decisiones sobre libertad condicional y libertad bajo fianza.

En los Estados Unidos y el Reino Unido, los modelos de evaluación de riesgos de big data se usan para ayudar a los funcionarios a decidir si se concede o no la [libertad condicional o bajo fianza](#), o si se remite a alguien a [programas de rehabilitación](#). También pueden usarse para evaluar cuánto riesgo presenta un delincuente a la sociedad, que es un factor que un juez podría considerar al decidir la duración de una sentencia.

No está claro qué datos se utilizan para ayudar a hacer estas evaluaciones, pero a medida que avanzamos hacia la [vigilancia digital](#), es cada vez más probable que estos programas incorporen información de fuente abierta, como la [actividad en redes sociales](#), si es que aún no lo hacen.

Estos análisis pueden no solo mirar el perfil de una persona, sino también cómo se compara con el de otros. Históricamente, algunas fuerzas policiales han [supervisado excesivamente](#) a ciertas comunidades minoritarias, lo que ha llevado a un número desproporcionado de reportes de incidentes delictivos. Si estos datos se incorporan a un algoritmo, distorsionarán los modelos de evaluación de riesgos y darán como resultado una discriminación que afecta directamente el [derecho de la persona a la libertad](#).

4.

Investigar las solicitudes de visa

El año pasado, la Agencia de Inmigración y Control de Aduanas (ICE) de los Estados Unidos anunció que quería introducir un programa automatizado para “[investigar visas de forma extrema](#)”. Este programa analizaría de forma automática y continua las cuentas de las redes sociales, para evaluar si los solicitantes realizarían una “contribución positiva” a los Estados Unidos, y si podría surgir algún problema de seguridad nacional.

Además de presentar riesgos para la libertad de pensamiento, opinión, expresión y asociación, existían riesgos de que este programa discriminara a personas de ciertas nacionalidades o religiones. Los [comentaristas](#) lo caracterizaron como una

“prohibición musulmana por algoritmo”.

El programa [fue retirado recientemente](#), según los informes, alegando que “no había un software ‘listo para usar’ que pudiera ofrecer la calidad de monitoreo que la agencia quería”. Pero incluir dichos objetivos en los documentos de adquisiciones puede crear malos incentivos para que la industria tecnológica desarrolle programas discriminatorios por diseño.

No hay duda de que los análisis de big data funcionan de tal manera que puede afectar las oportunidades de vida de los individuos. Sin embargo, la [falta de transparencia](#) sobre cómo se recopilan, utilizan y comparten estos datos hace que sea difícil para las personas saber qué información se usa, cómo y cuándo. Los análisis de Big Data son simplemente demasiado complicados para que las personas puedan proteger sus datos del uso inapropiado. En cambio, los estados y las empresas deben hacer, y seguir, las reglamentaciones para garantizar que su uso de big data no conduzca a la discriminación.

[Lorna McGregor](#), Directora, Centro de Derechos Humanos, IP y Codirectora, Gran Subvención de Derechos Humanos, Grandes Datos y Tecnología de ESRC, [Universidad de Essex](#); [Daragh Murray](#), profesor de derecho internacional de los derechos humanos en la Essex Law School, [Universidad de Essex](#), y [Vivian Ng](#), investigadora principal en derechos humanos, [Universidad de Essex](#).

Este artículo fue publicado originalmente en [The Conversation](#). Leer el [artículo original](#).

Lo que Facebook no nos está diciendo sobre su lucha en contra del abuso online

[Laura Bliss](#), [Universidad Edge Hill](#)

Facebook por primera vez ha puesto a disposición datos sobre la [escala de comentarios abusivos](#) publicados en su sitio. Esto puede haberse hecho bajo la creciente presión de las organizaciones para que las compañías de redes sociales sean más [transparentes sobre el abuso en línea](#), o para ganar credibilidad luego del [escándalo de datos de Cambridge Analytica](#). De cualquier manera, las cifras no son una lectura placentera.

En un [período de seis meses](#), desde octubre de 2017 hasta marzo de 2018, se eliminaron de este sitio 21 millones de imágenes sexualmente explícitas, 3.5 millones de publicaciones gráficamente violentas y 2.5 millones de todo tipo de discursos de odio. Estas cifras ayudan a revelar algunos puntos sorprendentes.

Como se esperaba, los datos indican que el problema está empeorando. Por ejemplo, entre enero y marzo se estimó que, por cada 10,000 mensajes en línea, entre 22 y 27 contenían violencia gráfica, de [16 a 19 en los últimos tres meses](#). Esto pone de relieve el hecho de que, en el Reino Unido, las acusaciones por abuso en línea han ido disminuyendo, como se demuestra en el siguiente gráfico.

Sin embargo, lo que Facebook no nos ha dicho es igual de significativo.

La red social ha estado [bajo una creciente presión](#) para combatir el abuso en su sitio, en particular, la eliminación de la [propaganda terrorista](#) después de eventos como el ataque de Westminster 2017 y el bombardeo de Manchester Arena. Aquí, la compañía ha sido proactiva. Entre enero y marzo de 2018, Facebook eliminó 1.9 millones de mensajes que fomentaban la propaganda terrorista, un aumento de 800,000 comentarios en comparación con los tres meses anteriores. Un total del 99.5% de estos mensajes se localizaron con la ayuda de los avances en tecnología.

A primera vista, parece que Facebook ha desarrollado con éxito un software que puede eliminar este contenido de su servidor. Pero Facebook no ha publicado cifras que muestren qué tan frecuente es la [propaganda terrorista](#) en su sitio. Entonces, realmente no sabemos cuán exitoso es el software con respecto a esto.

Eliminar publicaciones violentas

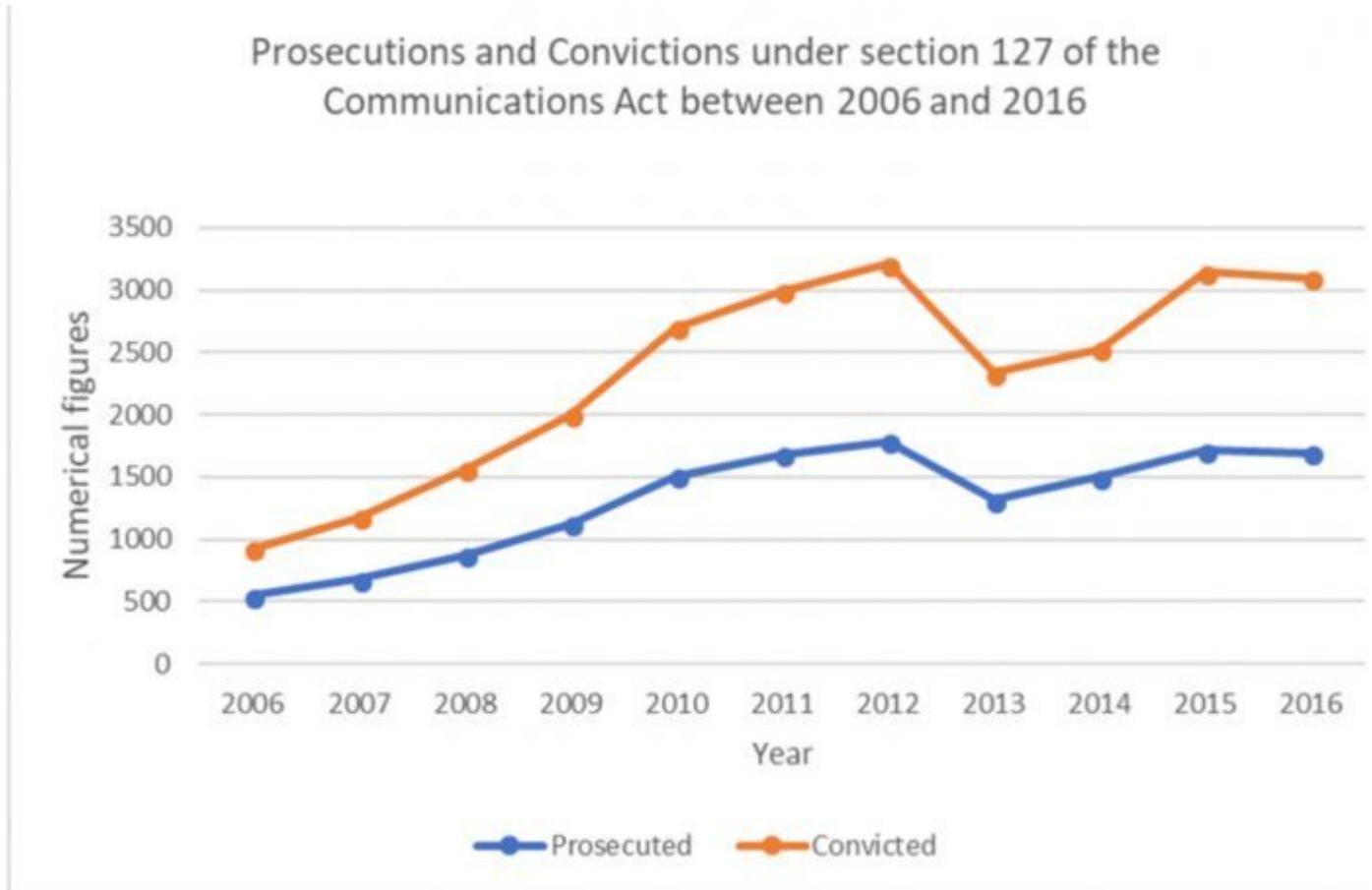
Facebook también ha utilizado la tecnología para ayudar a eliminar la violencia gráfica de su sitio. Entre los dos períodos de tres meses hubo un aumento del 183% en la cantidad de publicaciones eliminadas que se etiquetaron como gráficamente violentas. Un total de 86% de estos comentarios fueron marcados por un sistema informático.

Pero también sabemos que las cifras de Facebook también muestran que hasta 27 de cada 10,000 comentarios que esquivaron la tecnología de detección contenían violencia gráfica. Eso no parece mucho, pero vale la pena considerar la gran

cantidad de comentarios publicados en el sitio por sus más de 2 mil millones de usuarios activos. [Una estimación](#) sugiere que se publican 510,000 comentarios por minuto. Si es preciso, eso significaría que se publican 1.982.880 comentarios violentos cada 24 horas.

Para compensar las fallas en su software de detección, Facebook, al igual que otras redes sociales, se ha basado durante años en la autorregulación, alentando a los usuarios a [denunciar los comentarios](#) que creen que no deberían estar en el sitio. Por ejemplo, entre enero y marzo de 2018, Facebook eliminó 2,5 millones de comentarios que se consideraron expresiones de odio, pero solo 950,000 (38%) de estos mensajes fueron marcados por su sistema. El [otro 62%](#) fue informado por los usuarios. Esto demuestra que la tecnología de Facebook no combate adecuadamente el discurso de odio en su red, a pesar de la creciente preocupación de que las redes sociales [estén alimentando](#) los crímenes de odio en el mundo real.

¿Cuántos comentarios se denuncian?



Prosecutions for offensive messages.

Based on figures obtained from the Ministry of Justice, Author provided

Esto nos lleva a la otra cifra significativa que no está incluida en los datos publicados por Facebook: la cantidad total de comentarios informados por los usuarios. Como este es un mecanismo fundamental para abordar el abuso en línea, la cantidad de informes que se hagan a la compañía debería estar a disposición del público. Esto nos permitirá comprender el alcance de los comentarios abusivos hechos en línea, al tiempo que se aclara la cantidad total de mensajes que Facebook no elimina del sitio.

La decisión de Facebook de publicar datos que expongan la escala de abuso en su sitio es un avance significativo. A Twitter, por el contrario, se le pidió información similar, [pero se negó](#) a publicarla, alegando que sería engañosa. Claramente, no todos los comentarios marcados por los usuarios de los sitios de redes sociales violarán sus términos y condiciones. Pero el hecho de que Twitter no haya divulgado

esta información sugiere que la compañía no está dispuesta a revelar la magnitud del abuso en su propio sitio.

Sin embargo, incluso Facebook tiene un largo camino por recorrer para lograr una total transparencia. Idealmente, todos los sitios de redes sociales publicarían informes anuales sobre cómo abordan el abuso en línea. Esto permitiría a los reguladores y al público hacer que las empresas respondan más directamente ante las fallas para eliminar el abuso en línea de sus servidores.

[Laura Bliss](#), candidata a un doctorado en derecho en redes sociales, [Universidad Edge Hill](#)

[LEER EL ARTÍCULO ORIGINAL PULSANDO AQUÍ.](#)

Fotografía: *Pressenza*

Fecha de creación

2018/06/04