

10/2013

13 marzo de 2013

M^a José Caro Bejarano

**ALGUNOS RIESGOS MUNDIALES EN UN
MUNDO HIPERCONECTADO**

ALGUNOS RIESGOS MUNDIALES EN UN MUNDO HIPERCONECTADO

Resumen:

El Informe de Riesgos Mundiales (Global Risks 2013) del Foro Económico Mundial (WEF) plantea el llamado “incendio digital” como uno de los casos de riesgo mundial en un mundo hiperconectado. La proliferación de redes sociales en la última década junto con la falta de regulación de ciertos comportamientos en la red plantean la necesidad de un código de conducta. Sobre esta cuestión trabajan ya algunas organizaciones.

Abstract:

The Global Risks Report 2013 from the World Economic Forum poses the so-called “digital wildfire” as one of the global risk cases in a hyperconnected world. Social media proliferation in the last decade along with the regulation lack of certain behaviors in Internet raises the need of an ethos. Some organizations are already working on this issue.

Palabras clave:

Foro Económico Mundial, riesgos mundiales, incendio digital, redes sociales, código ético.

Keywords:

World Economic Forum, Global Risks Report, digital wildfire, social media, ethos.

VIVIMOS EN UN MUNDO HIPERCONECTADO, CON SUS RIESGOS... GLOBALES

Uno de los casos de riesgo planteados en la octava edición del Informe de Riesgos Mundiales (Global Risks 2013) presentado el pasado mes de enero por el Foro Económico Mundial (WEF¹) se sitúa en el centro de una constelación de riesgos tecnológicos y geopolíticos que varían desde el terrorismo a los ciberataques y el fallo de la gobernanza global. Este caso se denomina “Incendio digital incontrolado en un mundo hiperconectado” sobre la desinformación masiva que se extiende vía Internet. Este riesgo examina cómo la hiperconectividad podría permitir un incendio digital que sembraría el caos en el mundo real. Este caso considera el desafío presentado por el uso equivocado de un sistema abierto y fácilmente accesible como Internet y el peligro mayor de los intentos equivocados de evitar tales resultados.

En el caso de riesgo se recuerda que en 1938 el programa de radio “La guerra de los mundos” adaptación de la novela de H.G. Wells, causó el pánico entre la población de EE.UU. que creía ser invadida por los marcianos. Hoy en día es difícil imaginar una situación parecida por diversas razones: una mayor precaución y responsabilidad por parte de las emisoras, la regulación de los medios de comunicación, y la mayor inteligencia y escepticismo de la audiencia. Además, la industria de los medios está experimentando una transformación ya que Internet ofrece múltiples opciones para refutar o confirmar una noticia. Sin embargo, Internet es aún un medio joven relativamente. El hecho de que una noticia por tweet, blog o video pueda hoy provocar un pánico similar no es en absoluto improbable.

Internet es aún un territorio inexplorado y en rápida evolución. Las generaciones actuales son capaces de comunicarse y compartir información de forma instantánea y a una escala mayor que nunca antes. Las redes sociales permiten que la información se extienda por el mundo a toda velocidad. Mientras que los beneficios son obvios y están documentados, este mundo hiperconectado podría permitir la rápida expansión viral de información engañosa o provocadora, con intención o sin ella, con consecuencias serias. Las oportunidades de que esto ocurra es exponencialmente mayor hoy que con el programa de radio mencionado anteriormente, a pesar de la sofisticación de los medios.

Internet carece de mecanismos de autocorrección. Cualquiera puede cargar información falsa, aunque la comunidad de voluntarios de Wikipedia normalmente encuentra y corrige los errores rápidamente. Aunque la corta vida de una información falsa en la web generalmente no produce consecuencias reales graves, es concebible que un rumor falso extendido viralmente a través de las redes sociales pudiera tener un impacto devastador antes de ser corregido de

¹ Véase www.weforum.org. Global Risks 2013, eighth edition.

forma efectiva. Es incluso posible que el autor original de un contenido ofensivo no fuera consciente de su uso incorrecto o tergiversación por otros en Internet, o que fuera lanzado por un error de traducción de un idioma a otro. Tal escenario es un ejemplo de incendio digital.

Para poder prevenir los incendios digitales una posible vía sería la restricción legal sobre el anonimato online y la libertad de expresión, pero podría tener también consecuencias indeseables. ¿Qué sucedería si la fuente de un incendio digital fuera una nación o una institución internacional? En última instancia, los productores y consumidores de redes sociales necesitarán evolucionar hacia unos valores de responsabilidad y escepticismo saludable similar al que evolucionó entre las emisoras y los oyentes de radio desde 1938. Este caso de riesgo se plantea si el reconocimiento explícito de este problema potencial y el atraer la atención hacia posibles soluciones podrían facilitar y acelerar la evolución de estos valores o comportamientos responsables.

BENEFICIOS Y RIESGOS ASOCIADOS A LAS REDES SOCIALES

Desde los primeros manuscritos del hombre hasta los impresos, siempre ha resultado difícil predecir de qué manera las nuevas tecnologías de comunicación conformarán la sociedad. No obstante, la escala y velocidad de creación y transferencia de información no tienen parangón en este mundo actual. Así, la red Facebook alcanzó 1.000 millones de usuarios activos en menos de una década de existencia en octubre de 2012, mientras que Twitter atrajo unos 500 millones en siete años y genera unos 65 millones de tweets/día. Weibo, la red social china de micro-blogs alcanzó los 400 millones en el verano de 2012, cada minuto se sube a YouTube 48 horas de video, los usuarios únicos diarios en redes sociales siguen aumentando: 310 millones en Facebook, 37 millones en Qzone, 22 millones en Twitter². El mundo de las redes sociales es multicultural y joven. Su distribución por países y por edades también es variada.

Este fenómeno tiene muchos efectos que transforman la realidad y genera también pérdidas o ganancias: la actividad en Twitter y Facebook en Egipto y Túnez tuvo sus efectos en la primavera árabe; el análisis de los mensajes de Twitter y otras redes sociales permite predecir resultados electorales; la red social Patientslikeme.com permite conectar a individuos y ayudarles a acelerar el desarrollo de nuevos tratamientos; etc.

Se han producido casos muy diferentes y consecuencias diversas tras la propagación de una noticia: una respuesta humorística de un cliente contrariado que se traduce en la caída en bolsa de una compañía aérea, la revelación en Twitter de la identidad errónea de un supuesto

² Fuente: <http://www.concepto05.com/2012/01/estadistica-usuarios-de-redes-sociales-en-espana-2012/> y <http://www.searchenginejournal.com/wp-content/uploads/2011/09/social-media-black.jpeg>.

pederasta que se tradujo en una demanda contra la difusión de información falsa, un video en YouTube subido por un individuo en EE.UU. titulado “Innocence of Muslims” provocó revueltas en Oriente Medio, etc, y varían y aumentan cada día. El nexo de unión de estos casos es que la hiperconectividad amplifica sus impactos hasta un grado que hubiera sido impensable en la era previa a Internet, cuando sólo un pequeño número de organizaciones tenía la capacidad de transmitir información. Esta nueva realidad tiene implicaciones que plantean desafíos notables.

PELIGRO DE LOS INCENDIOS DIGITALES

Se han sucedido ya diferentes casos que muestran dos situaciones en las que estos incendios digitales son más peligrosos: situaciones de gran tensión cuando se presenta información visual falsa o inexacta que pueda causar daño antes de que sea posible propagar la información correcta. Esto es equivalente al efecto de gritar ¡Fuego! en un teatro lleno. Aunque sólo lleve un minuto o dos darse cuenta de que no hay fuego, puede ser tarde para evitar un tumulto hacia la salida con resultado de muertes por aplastamiento. La otra situación peligrosa es cuando circula información entre gente de ideas afines y resistentes a rectificarla. Es el caso de un tweet anónimo en octubre de 2012 que afirmaba que la bolsa de Nueva York se había visto inundada por el huracán Sandy; aunque enseguida otros usuarios de Twitter corrigieron rápidamente el falso rumor, no fue antes de que la noticia fuera difundida por la CNN³. En este caso, no había un interés particular en seguir creyendo la noticia original errónea. Sin embargo, en otras redes sociales cuya información es menos pública puede existir un problema con este tipo de información falsa, por ejemplo, redes de amigos en Facebook u otras redes más opacas como correos electrónicos o mensajes de texto. La propagación de información falsa en estas “redes de confianza” puede ser especialmente difícil de detectar y corregir porque los destinatarios son más proclives a confiar en cualquier información con origen en su propia red.

Por tanto, no hay que subestimar el riesgo de conflicto por falsos rumores, que circulen entre dos conjuntos de individuos de igual opinión, y que puedan crear una situación explosiva. Un ejemplo de ello fue el uso de Twitter por ambas partes en noviembre de 2012 en los enfrentamientos entre Israel y Hamas en Gaza⁴, esto señala la posibilidad de situaciones futuras en las que compitan versiones diferentes de un suceso entre grupos de gente predispuesta a creer a uno u otro bando y no compartan una fuente de información común que ayude a disipar estos bucles de información auto-ampliada.

³ Véase Keller, J. “How Truth and Lies Spread on Twitter”. Bloomberg Business Week, <http://www.businessweek.com/articles/2012-10-31/how-truth-and-lies-spread-on-twitter>, 2012.

⁴ Véase Borger, J. “Israel and Hamas Deploy Twitter Feeds in Media War”. The Guardian, <http://www.guardian.co.uk/world/2012/nov/15/israel-hamas-twitter-media-war>, 2012.

MÁS FENÓMENOS EN LA RED

Existen ya ejemplos en los que un incendio digital no comienza por accidente sino de manera intencionada por aquellos que quieren obtener algunos beneficios. En política se ha utilizado la práctica de crear una falsa impresión de que un movimiento popular apoya una idea o persona, es el caso de las elecciones al senado americano de 2009, donde una red de falsas cuentas de Twitter extendieron con éxito enlaces a una página web que difamaba a uno de los candidatos. Otros tweets falsos han afectado a los mercados haciéndose pasar por algunos políticos, como cuando se hizo creer que el ministro de interior ruso había tuiteado en julio de 2012 que el presidente sirio “había sido herido o asesinado”, lo que hizo subir el precio del crudo aproximadamente un dólar, antes de que se detectara la falsedad de la noticia⁵. Desde entonces se han producido múltiples casos con noticias falsas suplantando incluso cuentas de agencias de noticias⁶.

Las grandes corporaciones se enfrentan a cuestiones como la reputación online de la que puede depender el buen fluir de sus negocios, a partir de rumores lanzados desde cuentas de redes sociales⁷.

En estos casos no es siempre fácil localizar la fuente del incendio digital. De esto podría aprovecharse un ciberatacante para cubrir su rastro, de modo que una organización o un país pudiera ser falsamente acusado de propagar información inexacta o provocativa. Según las tensiones existentes en ese momento, las consecuencias de una atribución falsa podrían ser incluso exponencialmente peores que si no se hubiese atribuido.

¿NECESITAMOS UN CÓDIGO DIGITAL GLOBAL?

En todo el mundo los gobiernos se están enfrentando a la posibilidad de que las leyes existentes que limitan la libertad de expresión, por razones como incitación a la violencia o al pánico, se puedan aplicar también a las actividades online. Esta cuestión es altamente controvertida.

⁵ Véase <http://news.softpedia.es/El-mercado-de-petroleo-se-vio-afectado-por-un-falso-tweet-acerca-de-la-muerte-del-presidente-de-Siria-285355.html>

⁶ Véase <http://news.softpedia.es/Falsas-noticias-relacionadas-con-Siria-han-sido-publicadas-desde-la-cuenta-de-Twitter-hackeada-de-Reuters-285176.html>

⁷ Véase el caso de una cuenta satírica de Twitter atribuía un comentario a un directivo de BP tras el vertido del golfo de Méjico que atrajo doce veces más seguidores que la cuenta oficial de BP, Moreno, K. “Social Media Risk Is Like Wildfire. Where’s the Fire Engine?” Forbes, <http://www.forbes.com/sites/forbesinsights/2012/08/07/social-media-risk-is-like-wildfire-wheres-the-fireengine/>, 2012.

El establecimiento de límites razonables a las libertades de expresión online es difícil porque las redes sociales constituyen un fenómeno reciente y aún no se han establecido normas sociales adecuadas en la red. Esta cuestión plantea temas espinosos como hasta dónde sería posible imponer límites a la capacidad de mantener el anonimato online, sin comprometer seriamente la utilidad de Internet como herramienta de denuncia y disidencia política en regímenes represivos.

Incluso si la imposición de tales límites fuera aplicable, hay que plantearse qué autoridad sería responsable de hacerlo. La conferencia mundial de la Unión Internacional de Telecomunicaciones (ITU⁸ por sus siglas en inglés) celebrada en Dubai en diciembre de 2012 cuyo objetivo era la revisión del tratado de 1988, disparó la controversia ante los argumentos críticos de que una regulación técnica aparentemente inofensiva pudiera tener consecuencias negativas involuntarias. Una regulación presumiblemente diseñada para actuar contra el correo electrónico no deseado –conocido como *spam*– para asegurar la *calidad del servicio* del tráfico de Internet podría usarse por los gobiernos para reducir las comunicaciones entrantes o deshacerse de contenido específico que quisieran bloquear⁹ (pej., bloqueo de mensajes políticos o religiosos). Los delegados de Estados Unidos, Reino Unido, Australia y otros países expresaron durante la conferencia su rechazo a la nueva redacción del tratado que rige las llamadas telefónicas internacionales y el tráfico de datos. Entre los países que no firmaron se encuentran la mayoría de las naciones de Europa occidental junto con Canadá, Filipinas, Polonia, Egipto, Kenia y la República Checa.

Surgen preguntas como en quién confiar, cuándo se cuestiona la implantación de pruebas de calidad, o cómo crear una autoridad consolidada y reconocida que pueda intervenir o interrumpir flujos de desinformación.

También hay cuestiones profundas sobre educación e incentivos. Los usuarios de las redes sociales son, en general, muchos menos conocedores que los editores de los medios tradicionales sobre las leyes relativas a temas como libelo y difamación. Muchos también tienen menos que perder que los medios tradicionales al propagar información que no ha sido verificada correctamente. Aunque existen signos sobre la aparición de nuevas normas. La gente se muestra cada vez más menos tendente a re-tuitear información sin contrastar las fuentes para evitar enfrentarse a algún tipo de litigio.

⁸ Véase la página web de ITU <http://www.itu.int/en/wcit-12/Pages/default.aspx>

⁹ Véase <http://www.elmundo.es/elmundo/2012/12/14/navegante/1355482761.html>

Además de buscar formas de inculcar un código de responsabilidad entre los usuarios de las redes sociales, también será necesario que los consumidores de las mismas entiendan más al valorar la fiabilidad y sesgos de las fuentes. Las soluciones técnicas podrían ayudar, ya existen programas que ayudan al consumidor a valorar la credibilidad de la información y las fuentes que circulan online. Existen ratios que se realimentan de los usuarios para valorar la fiabilidad de los vendedores en webs de pago online. Este servicio ofrece un desarrollo de enorme potencial.

Aún no está claro el contenido de un código digital global o la mejor forma de desarrollarlo. Sin embargo, dados los riesgos planteados por un incendio digital en este mundo hiperconectado, esta es una cuestión a plantearse por los decisores políticos y comenzar cuanto antes el debate.

M^a José Caro Bejarano

Analista del IEEE