Software de monitoreo de redes y crimen predictivo, #BlameCanada

Cada vez que escuchan “Canada”, los fanáticos de la serie South Park no pueden evitar recordar el pegajoso estribillo de la canción (nominada a un Oscar, con performance de Robin Williams en vivo) con la cual la madre de uno de los personajes culpaba a la nación del extremo norte por las palabrotas que su hijo había aprendido.

Más allá de que pueda o no gustarte el tipo de humor, la serie ha sido una crítica aguda de la sociedad norteamericana, ocupando el lugar que en algún momento supieron llenar Los Simpsons antes de caer en la desgracia de las “nuevas temporadas”‘, y en muchos casos premonitoria de fenomenos sociales que retrató antes de que exploten.

Para muestra basta un botón, según dicen. El año pasado presentó varios hilos argumentales convergentes, conectando la disparatada campaña electoral estadounidense con el fenómeno de los trolls de Internet, especialmente en Twitter. Por motivos de la trama que no les pienso spoilear, Dinamarca (que en eso vienen siendo como los noruegos del himno de Les Luthiers) declaran la guerra -digital y en las redes- a los americanos, creando un arma capaz de desenmascarar al cobarde detrás del troll, a través de un “algoritmo contextual analizador de identidad a través del uso de emojis”. En criollo, un software que sabía quien era el autor detrás de un posteo anónimo de internet, analizando su forma de escribir y los emoticones que usaba.
Inverosímil? Disparatado? Seguí leyendo...

Abarajame el emoticón

Según una nota publicada por Vice, el Gobierno de Canadá (blaaaameee Canadaaaa, maldición, se me pegó la melodía), lleva dos años desarrollando un software que puede **monitorear las redes sociales buscando amenazas en tiempo real**. Para esto, puede colectar y almacenar los tweets, traducirlos de su idioma original, archivarlos para seguimiento, “interpretar la emoción” detrás de ese posteo y, compilando toda esa

data, **contrastarlo con perfiles públicos de Internet** para identificar al autor, **incluso si es anónimo.**

Casi como un paralelo real del software danés de South Park, este algoritmo les permite a los investigadores buscar entre toneladas de post de social media y blogs, *para detectar un patrón en el lenguaje, forma de escribir*, localización geográfica y fecha de los posteos, y detectar los "sentimientos y emociones del autor".

Básicamente, usa todos los datos que están disponibles en la red a los que se pueda acceder sin clave de acceso, como ser los perfiles y fotos publicos, cuentas no protegidas, bases de datos de consulta libre, tus comentarios en canales de youtube y hasta ese tweet tan simpático donde te acordabas de toda la familia del servicio que te dejó sin internet el fin de semana.

Hay muchisima informacion de este tipo lista para ser recolectada, hace la prueba, googlea tu nombre, anda a imagenes y sorprendete, cortesía del big data. Podés encontrar correlaciones insolitas, desde ese like que pusiste alla por el 2010, la foto de la bicicleta que querias vender en esa app donde usabas un seudonimo, o (la boca se te haga a un lado) varias fotos en baja calidad de tu Fotolog, que en paz descanse.
Si ya te estas empezando a paranoiquear y te preguntás si este tipo de búsqueda es legal, la respuesta es afirmativa. Esta pesquisa sobre los datos de acceso publico se conoce como "**investigacion de redes abiertas**", implicando que en el marco de la instrucción de un proceso penal, el Estado puede licitamente acceder a la informacion que se encuentren en Internet de manera pública (no asi lo protegido o privado) y usarlo como prueba de cargo.

<u>Se me llena el software de preguntas</u>

El prototipo fue construido en cooperación entre varios actores públicos y privados, incluyendo el Consejo Nacional de Investigación de Canadá, la multinacional Thales Group (dedicada al desarrollo de sistemas de información y servicios para los mercados

aeroespacial, de defensa y seguridad), una firma de monitoreo de redes sociales y una agencia de inteligencia, secreta obvio. Cero participación de la sociedad civil para que pueda fiscalizar los límites de este tipo de aplicación.
Recordemos que el objetivo de este pedacito de código es rastrear y analizar los post públicos "para anticipar y prevenir potenciales amenazas a la seguridad publica". Lo peligroso es que esta acepción de prevenir esta más cerca de "**minority report"** que de la imagen de un patrullero parado en la esquina vigilando, es mucho mas "predecir" que "prevenir". No se trata de esperar a que el hecho se produzca, sino de ser capaces de evitar que pase.

Esta **"precognición delictiva"** levanta muchas alarmas, la primera de todas, porque colisiona con un principio fundamental de los Estados de derecho por el que las ideas no pueden ser castigadas, mientras no se traduzcan en hechos que estén prohibidos (gracias Constitucion Nacional, te queremos). Segundo, pone una importante mordaza al libre debate y circulación de ideas. Quien se animaria a expresarse libremente sabiendo que existe un software secreto capaz de encontrarte y clasificarte de amenaza por un hecho que aun no ocurrió? Como el "crimental" de la policía del pensamiento de las que nos hablaba Orwell en 1984, parece un engendro salido de la peor pesadilla distópica totalitaria.
También sienta un precedente peligroso, al sumar a esta ecuación el análisis de tu red social de contactos y allegados como elemento para subir tu *score* de peligrosidad.

Con la sabiduría de una madre a la que no le gustan tus amigos, el software sopesa tus conexiones y contactos, de ahí que podes terminar como un culpable por asociación o, sino obligado a abstenerse de aceptar malas juntas que contaminen tu perfil.

Como otros desarrollos de big data, es cuestionable que no podamos acceder a conocer la fórmula por la que se arriba a un resultado que nos afecta, ni los parámetros que la componen para determinar posibles sesgos discriminatorios en la construcción del algoritmo.

Además de no saber cómo llega el algoritmo a la determinación del carácter negativo de tu emoción, tampoco existiría la manera de que puedas probar lo contrario, que el software se equivocó y llegó a una conclusión errada.
Justamente por eso, reaviva el debate de la necesidad de anonimato y herramientas de encriptación, para evitar que toda esa informacion pueda ser usada en tu contra.

Brave new world

Quizás lo más terrible es que ese rótulo secreto, en la sociedad de la información tiene la potencialidad de transformar la vida de una persona en un infierno, sometiendolo a una vigilancia no explícita o a consecuencias injustas.O peor aún, que los resultados de esas calificaciones de riesgo se compartan como "verdad revelada" con otros agentes privados que puedan tomar decisiones sobre una persona basadas en esa información.
En el caso, imaginate pasar por los controles de un aeropuerto cuando un software te señala como un potencial peligro, sin saber porqué sos detenido en todos los controles migratorios. O porque tu pasaje sale mucho mas caro, ya que la aerolínea sopesó quien eras al momento de venderlo y consideró que llevarte es un riesgo que amerita un incremento proporcional.
Mientras tanto vos, que no sabés que por *retweetear* o compartir ese post estás siendo vigilado, estarás inocentemente prendiendo inciensos de ruda macho para alejar la mala suerte de todo lo que te esta pasando. Todo por culpa de un software secreto, nada mal para "un mundo feliz".

Ciberpatrullaje 2.0

Antes de que salgas corriendo a borrar por completo tu historia en Internet o que te conviertas en un ermitaño digital que desaparezca de las redes, contextualicemos.
Thales sostiene que el software analiza en tiempo real los datos de social media usando técnicas y algoritmos de minería de datos para identificar tendencias. Entre los ejemplos de uso, mencionan la traducción de tweets en árabe o chino que puedan sugerir atentados o signos de incontento popular dentro de la misma nación que indiquen la proximidad de una protesta o revuelta, midiendo la temperatura social a través de las emociones negativas de los contenidos.
El prototipo se testeó en casos reales para medir las reacciones del ataque terrorista al Parlamento de Ottawa en 2014, así como los tweets relativos a la guerra civil en Siria. Pero no se limita a eso, ya que investigaciones revelaron que las agencias canadienses

de inteligencia lo usaron para calibrar casos que involucran, entre otros, a activistas ambientales.
A pesar de las descripciones generalizadoras como un termómetro de la reacción social a determinados eventos, esta tecnología está dirigida a identificar usuarios concretos, ya que además de su nombre de usuario, rastrea la geolocalización del post, y una lista de a quienes sigue la cuenta, de los followers de este usuario y, por ejemplo que tweets ha marcado como favoritos o retweeteado.

Recapitulando, este algoritmo podría usar cada pedacito de información y gota de creatividad que hayas puesto en esos 140 caracteres y unirlo a todas las pistas digitales de tu historia en Internet, para definirte, identificarte y clasificarte, sin que vos tengas la chance de saber que estás siendo vigilado ni recurso para oponerte. #MarchePreso

Mientras buscas todo lo que estarías necesitando eliminar (anda tranquilo que te esperamos antes de terminar la nota), pensa que en el tiempo que tardas en decir *"vigilancia- masiva- inconstitucional"*, (o ciberpatrullaje, que es más cortito), los canadienses ya prendieron el motor, prepararon el fernet y están todos a bordo del ciberpatrullero.

Lamentablemente, el uso de este tipo de software es una tendencia en alza entre las agencias de inteligencia, ya que como nos enseñaron unos filósofos argentinos contemporáneos, el que no levanta las manos, maneja el cibepatrullero.