Miércoles
28 de marzo
de 2018

Ciberpolítica

la diaria | DAT&SOC

Cuestiones éticas

La privacidad en la era digital: desafíos y perspectivas

Los desafíos de la privacidad en la era digital

Dra. Ana Tuduri, investigadora, Datysoc

El derecho a la privacidad es la protección de la esfera íntima y reservada de la persona, quien no puede ser objeto de injerencias o ataques arbitrarios, así es reconocido en la Declaración Universal de Derechos Humanos y en diversos acuerdos internacionales y leyes nacionales. La privacidad no es lo que era, particularmente desde que las redes sociales juegan un papel protagónico en las relaciones humanas y en la comunicación, lo que torna difuso el límite entre lo público y lo privado. En este artículo planteo tres desafíos para la privacidad en la era digital.

El primer desafío es que el marco regulador –nuestras normas– logre acompasar las nuevas tecnologías.

Como consecuencia de lo antedicho, se vuelve fundamental sensibilizar a los usuarios sobre los contratos de adhesión que consienten para utilizar las aplicaciones gratuitas, el volumen de información personal que comparten en línea, la accesibilidad que otros tienen a ella y cómo esa información puede ser utilizada por terceros.

Lo cierto es que ese flujo de información, en particular los datos personales, se convirtió en un activo con valor económico. Esto lleva al segundo desafío de la privacidad, que es la retención de datos personales en manos de actores públicos y privados.

La Ley Nº 18.331 sobre protección de datos personales y *habeas data* establece que las bases de datos, tanto de titularidad pública como privada, deben ser registradas. Incluso, ante un incumplimiento, la Unidad Reguladora de Datos Personales podrá aplicar medidas sancionatorias a los responsables de las bases.

Además, prevé la acción de *habeas data,* que reconoce el derecho de las personas a entablar una acción judicial para tomar conocimiento de los datos existentes sobre ellas y de la finalidad y uso de esa información, tanto en bases de datos públicas o privadas. Como también en caso de error, falsedad, prohibición de tratamiento, discriminación o desactualización se podrá exigir la rectificación, inclusión, supresión o lo que corresponda.

Si bien esta norma vino a dar protección y garantía a esta nueva arista de la privacidad, nada dice respecto del derecho de las personas a saber, específicamente, quiénes han accedido a sus datos, cuándo y por qué.

Un caso que pone de manifiesto este desamparo de la legislación es el de las empresas dueñas de las bases de datos comerciales y crediticias. Estas poseen información sobre la solvencia patrimonial o crediticia de las personas, y si bien la norma citada estipula la posibilidad de entablar la acción de *habeas data*, no regula la posibilidad de saber qué empresas clientes o terceros consultan esos datos, cómo son tratados, quién tiene acceso a los datos consultados dentro de esas empresas y, en caso de que los almacenen, cómo lo hacen, dónde y por cuánto tiempo.

Por último, el tercer desafío para la privacidad es la vigilancia masiva de las comunicaciones. Esta puede ser entendida como la interceptación de las comunicaciones privadas de una persona por medio de herramientas tecnológicas y puede abarcar el teléfono, el correo electrónico, el tráfico de internet o los metadatos.

Desde que en 2013 se filtró por la prensa la compra secreta del software de vigilancia El Guardián, no es una novedad el uso de este tipo de mecanismos para la recolección masiva de datos en pos de la seguridad y la lucha contra el crimen organizado. El caso de El Guardián, sin embargo, debe ser matizado, pues su capacidad es limitada a diferencia de los softwares utilizados en otros países.

El uso de estas nuevas tecnologías trae consigo la necesidad de adecuar el marco regulatorio para garantizar el derecho a la privacidad de las personas y a la confidencialidad de sus comunicaciones.

En los desafíos planteados no es fácil encontrar un balance entre la privacidad y los usos de la información personal cuando alguien es objeto de vigilancia, sea por una entidad pública o privada. Por un lado, en materia de vigilancia existen una serie de medidas vinculadas a la rendición de cuentas del sistema, como el derecho de las personas a ser notificadas de que fueron vigiladas; la información periódica sobre el uso de herramientas tecnológicas de vigilancia de las comunicaciones; los posibles estándares de publicación de información relacionados con estas prácticas; la regulación de los procedimientos de compra de estas herramientas; la posibilidad de auditar el funcionamiento de las herramientas de vigilancia con representantes de todos los sectores de la sociedad y la necesidad de regular la vigilancia privada. A quién proporcionamos nuestros datos voluntariamente a cambio de nuestra conveniencia, quién nos monitorea y qué grado de poder tienen las fuerzas de seguridad (de forma justificada) en este nuevo escenario, requiere de una mejor discusión pública. ■

Inteligencia artificial y grandes datos: algunos apuntes

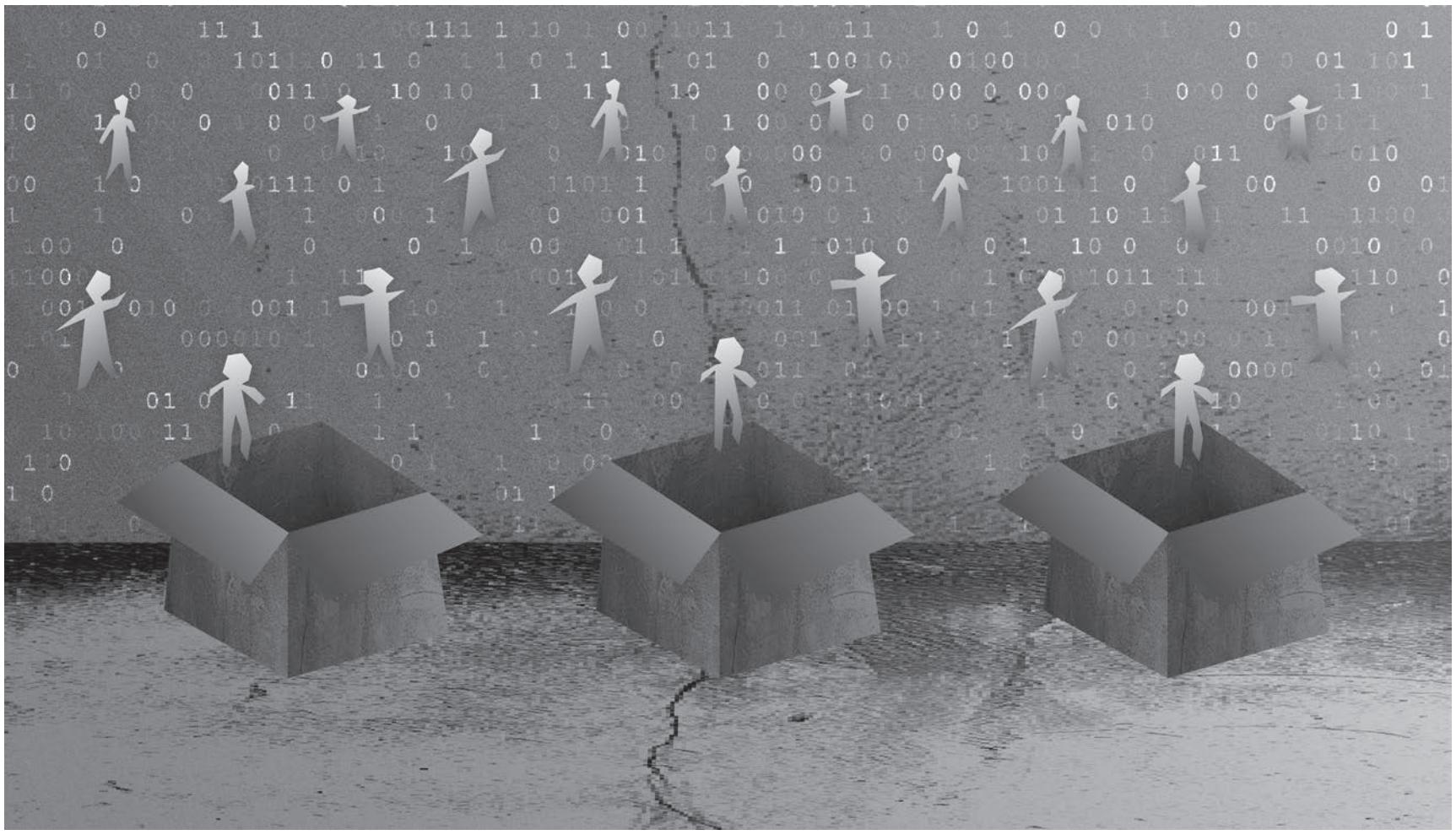
Dr. Tomas Laurenzo, profesor asociado, Universidad de la Ciudad de Hong Kong

1. Hay mucho escrito sobre tratamiento automático de datos, aprendizaje automático y grandes datos. Resulta difícil no dejarse deslumbrar por los avances técnicos.
2. Lo más importante es entender que un cambio cuantitativo (más poder de cómputo, más cantidad de datos de entrenamiento) generó un cambio cualitativo.
3. La importancia de este cambio cualitativo es enorme, porque echó por tierra nuestra intuición de qué era imposible de resolver por medio de la informática. Es decir, muchas cosas que pensábamos que requerían atención humana, pasaron a ser automatizables; es, en cierta medida, similar a la revolución industrial, pero más grande.
4. La razón fundamental es que pensábamos que resolver un problema implicaba comprenderlo. El aprendizaje automático demostró que no es preciso entender, sino que "basta" con entrenar una descripción estadística ciega, que reacciona a patrones subyacentes en los datos.
5. Esto, claro, precisa muchísimos datos y de gran poder de cómputo, para poder procesar esos datos.
6. Entonces aquí aparecen –entre muchos otros– tres terrenos importantes de discusión. En primer lugar, ¿qué pasa con el trabajo humano? Si ahora hay muchas cosas que ya no requieren atención humana, ¿qué pasa con la economía que depende de esa atención (que, además, se ramifica de una forma difícil de apreciar)? Por ejemplo, si tenemos autos que se manejan solos, entonces ya no es preciso tener restaurantes u hoteles de alta rotatividad en la carretera.

   En segundo lugar, esta conversación, sin embargo, no es técnica. Es decir, no existe una conversación que sea técnica y no política. Eso es una falacia postmoderna que quiere convencer a quienes sufren la desigualdad de que hay un orden natural. El capitalismo (o el feudalismo, o cualquier orden social) son órdenes artificiales y, por definición, arbitrarios (más allá del orden moral que se use para evaluarlos, y más allá de cuán de acuerdo esté uno o no). Por ejemplo, disponemos de la tecnología para tener autos que no contaminan, pero seguimos usando autos que contaminan en gran cantidad. La decisión de usar autos que no contaminan es económico-política, y no técnica. O, vale decir, que no hay soluciones técnicas que no sean políticas. O, en realidad, no hay decisiones que no sean políticas.

   Incluso si no cuestionamos el gran orden (social) de las cosas, la asunción de que las decisiones algorítmicas son ungidas desde una cierta objetividad es un delirio. Como se dijo, estos sistemas son "entrenados" con conjuntos de datos que provienen de nuestra sociedad y que no sólo reflejan las condiciones de desigualdad estructural, sino que, además, son interpretados, utilizados, y manipulados, desde un entendimiento del mundo, que cristaliza los órdenes sociales imperantes (es decir, que reedita las condiciones de desigualdad estructural). Ejemplos de esto hay en abundancia, por ejemplo, predictores de crimen que castigan a determinados grupos de personas o determinados barrios.

   Por último, esta automatización, además de introducir nuevos, exagera problemas que ya existen en nuestra sociedad (el "efecto red", o el "filtro burbuja" son claros ejemplo). Es interesante como el ser evaluado por un humano pasa a ser, cada vez más, un privilegio de las clases dominantes, y las clases bajas pasan a ser procesadas de forma automática. Lo increíble es que la narrativa trata de convencernos de que eso es más justo. Otro aspecto, incluso si uno no quisiera discutir las injusticias del sistema capitalista, es que en la era de los grandes datos se genera una *plusvalía 2.0.* La tierra para el que la trabaja pasaría a ser los datos para quien los genera. Es decir, si hay un acuerdo económico en el que los datos son valiosos, entonces tiene que haber una contrapartida económica para quien los produce. Es como si fuéramos a un productor de naranjas y le dijéramos: "Tus naranjas no tienen valor, dámelas gratis y luego las vendemos por millones de dólares". En un gobierno de izquierda hay que generar la normativa y la inercia social para que se sistematice la generación de contextos de intercambio económico más justos. Uruguay no parece estar apuntando para ese lado. Por ejemplo, el valor económico de los datos almacenados por las operadoras de telefonía móvil no se discute. Tampoco se discute su propiedad, ¿por qué esos datos que son generados por los usuarios le pertenecen a la telefónica? *Plusvalía 2.0.* Lo mismo sucede con la tarjeta del Sistema de Transporte Metropolitano, aunque el caso más obsceno probablemente sea el del Clearing de Informes.
7. Es necesario plantear la discusión en estos términos, de otro modo, si la discusión sólo se estructura en función de un supuesto orden natural de las cosas (capitalismo), un estado de control (mal llamado "paternal") y una deshumanización de los ciudadanos, entonces estamos perdidos. ■



Luciana Peinado

El análisis de datos y la mirada humana

Dra. Ing. Lorena Etcheverry, profesora adjunta del Instituto de Computación, Facultad de Ingeniería, Udelar

En los últimos años nos hemos acostumbrado a encontrar en los medios menciones al *big data* y al aprendizaje automático. Estos términos suelen usarse indiscriminadamente para referir a técnicas y algoritmos que extraen información desde los datos. Pero ¿qué tipo de información se extrae? Típicamente se busca relacionar y clasificar individuos, ya sean personas o cosas, según algunas de sus características, para luego predecir su comportamiento. Netflix, por ejemplo, recomienda películas y series a sus usuarios, basándose en lo que otros usuarios similares prefieren. Parte del problema consiste en definir qué características se usan y cuáles son los criterios para medir la similitud entre dos usuarios, pero esta discusión está más allá del objetivo de esta columna.

Pero ¿cuál es el impacto que estas técnicas tienen en nuestras vidas? Cuando el sistema de recomendaciones de Netflix se equivoca, puede sugerirnos una serie que no nos gusta, pero ¿qué pasa cuando un software utilizado por el Poder Judicial indica, incorrectamente, que los afrodescendientes tienen casi el doble de probabilidad de reincidir en crímenes que los blancos [1]?

Los aspectos éticos detrás de las técnicas de análisis de datos no son nuevos. En áreas como la medicina o las ciencias sociales, diferentes herramientas estadísticas son utilizadas desde hace más de un siglo, y se conocen, por ejemplo, los riesgos de extraer conclusiones desde un conjunto sesgado de datos. Lo que sí es novedoso en nuestros tiempos es la masificación del uso de las técnicas de análisis de datos (auspiciada por la abundancia de datos existente), su aplicación en áreas como la educación, la seguridad pública, o la política, y el impacto que estas tienen en los procesos de toma de decisiones en ámbitos públicos y privados.

Estos contextos de aplicación son inherentemente diferentes, y deberían, por lo tanto, regirse por premisas diferentes. Una cosa es aplicar algoritmos para segmentar un mercado y vender más productos, y otra cosa es definir políticas públicas siguiendo lógicas similares. En este segundo escenario se suele argumentar que estas técnicas permiten conocer mejor a las poblaciones objetivo, mejorar la gestión de los recursos y, en consecuencia, contribuir al bienestar de la población, lo cual no es necesariamente cierto. Nuestro país no está libre de este tipo de iniciativas que anuncian con bombos y platillos las bondades del análisis de datos. A modo de ejemplo, el proyecto EduData propone recopilar información para evaluar y predecir el desempeño de preescolares que asisten a los Centros de Atención a la Infancia y a la Familia[2]. Sin las precauciones adecuadas, estas herramientas pueden ser peligrosas y potenciar la desigualdad, como veremos a continuación.

Ya en 2012 algunos autores advertían sobre los riesgos del uso indiscriminado del análisis de datos y cuestionaban algunas de sus premisas[3]. En particular, quisiera destacar dos ideas centrales. Por un lado, la necesidad de derribar el mito de que la tecnología, y en particular estos programas, son neutrales y objetivos. En tanto artefactos creados por humanos, suelen estar contaminados por el sistema de creencias de quien los diseña o de quien interpreta los resultados. Por otro lado, la importancia de que las organizaciones que utilicen estas técnicas sean capaces de rendir cuentas acerca de por qué tomaron ciertas decisiones, y, en particular, qué datos y técnicas utilizaron. Retomando estas ideas, Julia Stoyanovich y otros investigadores definen el uso responsable del análisis de datos en términos de tres conceptos: equidad, diversidad y transparencia[4]. La *equidad* refiere a que el análisis deberá estar libre de sesgo, que puede provenir de los datos en sí, por ejemplo debido a los mecanismos usados para recabarlos, o de los algoritmos utilizados y la interpretación de los resultados, los cuales pueden reflejar las preferencias políticas, comerciales, sexuales, religiosas, etcétera, de sus desarrolladores y eventualmente resultar discriminatorios. La *diversidad* refiere a que no basta con que los algoritmos retornen los resultados más populares, sino que también deben considerar resultados menos frecuentes que enriquezcan las opciones, ya que sin diversidad se corre el riesgo de excluir resultados menos populares ("los ricos son más ricos y los pobres son más pobres"). Por último, el concepto de *transparencia* aplica, por un lado, a aspectos relacionados con la privacidad –que los usuarios puedan conocer qué datos se están recopilando sobre ellos y para qué están siendo utilizados, por ejemplo–, aunque también refiere a la posibilidad de verificar y auditar los algoritmos para demostrar que respetan los principios de equidad, diversidad y privacidad.

Algunas organizaciones y gobiernos no son ajenos a estas preocupaciones. La Unión Europea, que es referencia a escala mundial en normativa sobre protección de datos personales y en la cual se inspira la normativa uruguaya, ha publicado recientemente un estudio que explora cómo aplicar técnicas de análisis de datos que promuevan el crecimiento económico y, además, consideren las dimensiones éticas de este análisis. En particular, se proponen acciones entre las que se destacan un marco general para el análisis ético de datos y su aplicación a datos de salud y educación[5].

En resumen, pese a estar fuertemente asistido por las máquinas, el análisis de datos es una actividad humana y por tanto subjetiva y enmarcada en un sistema de creencias. Es imprescindible desmitificarla, no creer en sus resultados como si fuese una cuestión de fe, y reglamentarla para ser capaces de transparentar el marco político e ideológico subyacente. ■

1 Angwin, J. y otros (2016). "There's software used across the country to predict future criminals. And it's biased against blacks". *Machine Bias ProPublica.* https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

2 Castro, L. (2017). "Página web sistematizará datos del alumno generados por centro educativo y otras instituciones para devolver un análisis", ver ***la diaria*** del 31/7/2017.

3 Boyd, D. y Crawford, K. (2012). "Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon". *Information, Communication & Society,* 15(5), 662-679.

4 Stoyanovich,J.; Abiteboul, S. y Miklau, G. (2016). "Data, Responsibly: Fairness, Neutrality and Transparency in Data Analysis" en *International Conference on Extending Database Technology,* Burdeos, Francia. https://hal.inria.fr/hal-01290695/document

5 European Economic and Social Committee, (2017). *The ethics of Big Data: Balancing economic benefits and ethical questions of Big Data in the EU policy context.* http://www.eesc.europa.eu/en/our-work/publications-other-work/publications/ethics-big-data

Una vigilancia sin precedentes

Dr. Fabrizio Scrollini, investigador a cargo de Datysoc

Luciana Peinado

En junio de 2017, el diario *The New York Times* informó que prominentes activistas y periodistas mexicanos fueron blanco de un software de vigilancia que supuestamente se vende en exclusiva a los gobiernos y sólo puede usarse contra objetivos muy específicos. Investigadores internacionales de la Comisión Interamericana de Derechos Humanos se enfrentaron a la vigilancia ilegal mientras investigaban la muerte de 43 estudiantes en el estado de Guerrero.

A pesar de las revelaciones de Edward Snowden, los debates sobre la privacidad se mantienen apagados en América Latina.

Las ONG mexicanas Social Tic, RD3 y Article 19, con el apoyo de Citizen Lab de la Universidad de Toronto, expusieron estos incidentes. También participaron en Open Government Partnership, una alianza de gobiernos y organizaciones de la sociedad civil que impulsa reformas gubernamentales a través de varios mecanismos de diálogo. Para agregar complejidad a este asunto, algunos de los activistas espiados fueron los principales miembros de esta alianza. La situación entonces parece ser la siguiente: líderes de la sociedad civil que avanzaban en el diálogo con el gobierno mexicano y participaban en conversaciones de buena fe para cambiar aspectos clave de la administración pública y la política fueron espiados por fuerzas de seguridad desconocidas. Sin duda, esta no es una forma de aumentar la confianza en un proceso de diálogo.

Que la vigilancia ilegal es un problema serio en muchos países latinoamericanos no es noticia, pero la escala y el enfoque de este acto en particular ponen en peligro un mecanismo que entregó algunas vías de reforma prometedoras en el caso mexicano, en particular sus datos abiertos, la anticorrupción y las reformas sobre transparencia.

En Uruguay, la última democracia plena en pie en América Latina –según la Unidad de Inteligencia de *The Economist*–, también están surgiendo desafíos. El gobierno compró secretamente El Guardian, una aplicación que intercepta llamadas y redes sociales. Sin embargo, está poco claro cómo se usa o los protocolos operativos que sigue. También adquirió Predpol, una herramienta para potencialmente "anticipar crímenes". Compró además un centro de vigilancia por 20 millones de dólares en la ciudad de Maldonado, instalando más de 2.000 cámaras en el área y cobrando a los residentes por este servicio, sin proporcionar información sobre los costos o procedimientos del centro.

Hasta el momento no hay evidencia de que el gobierno uruguayo tenga software para ejecutar operaciones específicas como su homólogo mexicano, pero las autoridades uruguayas sí se reunieron con Hacking Team, una compañía de software italiana que ha vendido ilegalmente software de piratería a numerosos gobiernos en América Latina. También hay una amplia evidencia de que los militares espiaron a todos los partidos políticos uruguayos utilizando técnicas más tradicionales, desde el año 1985 al menos hasta 2007. En resumen, ni siquiera un país tan pequeño y relativamente democrático es inmune a tales prácticas.

Los ciudadanos están hoy sujetos a un grado de vigilancia sin precedentes, aunque a menudo en formas menos obvias.

La situación actual es problemática. Por un lado, los gobiernos podrían necesitar de forma legítima nuevas herramientas para luchar contra los crímenes, en especial contra el crimen organizado, que es un tema muy serio en América Latina. Alguna tecnología de vigilancia podría ayudar a estandarizar operaciones y procedimientos dentro de las fuerzas de seguridad e inteligencia, limitando así sus actividades.

Por otro lado, los gobiernos parecen estar comprando este tipo de dispositivos sin ningún tipo de guía o marco para asegurar que se garanticen los derechos humanos y las libertades básicas de los ciudadanos. Dadas las tecnologías actuales disponibles para los organismos de seguridad, la libertad de expresión, la privacidad y la igualdad de trato por parte de las autoridades públicas podrían verse amenazadas.

En Abrelatam-Condatos, el foro de datos abiertos más relevante de la región, el relator especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Edison Lanza, remarcó la idea de que los gobiernos "no sean bifrontes". Es decir, que los mismos gobiernos que permiten la colaboración, brindan datos abiertos y mejoran el gobierno abierto, también están llevando adelante operaciones dudosa y la compra secreta de nuevas herramientas tecnológicas.

Hay cuestiones clave de política para abordar el tema de si las democracias deben permanecer seguras en una era de tecnología de vigilancia agresiva. La seguridad tiene un costo, pero este costo puede ser irrazonable.

Un marco claro debería considerar las cuestiones de necesidad y proporcionalidad para adquirir y utilizar estas tecnologías, así como identificar qué agencias podrán explotarlas. El mismo marco debería requerir un conjunto de informes sobre el uso de estas tecnologías, incluso si han utilizado a terceros (como las telecomunicaciones) para llevar a cabo sus operaciones.

Las organizaciones de la sociedad civil que trabajan en estos temas rara vez tienen la capacidad o los recursos para tomar una posición y participar en los procesos de reforma. La vigilancia tiene una larga historia en América Latina, pero esta nueva ola –cuyo software de espionaje es sólo la punta del iceberg– es completamente distinta dada la naturaleza, escala y costo de estas tecnologías. Se necesita una sociedad civil comprometida y consciente de los desarrollos internacionales para garantizar un escrutinio y debate adecuados.

Como Martin Lodge, profesor de Escuela de Economia y Ciencia Politica de Londres, ha argumentado persuasivamente, existe la espinosa cuestión de la rendición de cuentas y el cumplimiento. Los comités legislativos, las estrictas reglas de transparencia y los organismos internacionales son herramientas iniciales de política a considerar, pero pueden no ser suficientes para contrarrestar el uso indebido de algunas tecnologías en el contexto de las democracias frágiles.

No está claro cuándo o cómo los latinoamericanos tendrán el tipo de conversación necesaria para despejar la neblina que rodea el estado actual de la vigilancia en la región, así como sobre cuestiones más generales acerca de la mejora de la privacidad en la era digital. Pero si tal conversación no tiene lugar, cualquier esfuerzo noble hacia un gobierno abierto permanecerá manchado por la sombra oscura de la vigilancia. ■

Este texto fue tomado y adaptado de un texto original del mismo autor publicado en el blog LSE IDEAS.

Privacidad y protección de datos en la tecnología educativa

Soc. Mariana Fossatti,
investigadora, Datysoc y
Dra. Patricia Diaz,
investigadora, Datysoc

Desde hace algunos años varias herramientras tecnológicas están presentes en los ámbitos educativos: desde entornos virtuales de aprendizaje, hasta registro de asistencias, pasando por pruebas estandarizadas y espacios de trabajo colaborativo online. Muchas de estas tecnologías se basan en *cloud computing* o computación en la nube, es decir, un conjunto de infraestructuras técnicas para la gestión de plataformas y servicios en línea. En Uruguay, las tecnologías educativas en la nube están presentes en todos los niveles de la educación pública y privada. En la investigación *Privacidad y protección de datos en la educación pública uruguaya*, un estudio sobre *cloud computing* en educación realizado en 2017 por Patricia Díaz y Mariana Fossatti de Datysoc, se analizan dos casos: el Plan Ceibal y el Programa de Entornos Virtuales de Aprendizaje (ProEVA-Udelar).

De las tecnologías educativas en la nube surgen muchas posibilidades, pero también incertidumbres en cuanto a la protección de datos de los estudiantes. Por un lado, permiten el acceso desde cualquier lugar y con distintos dispositivos a diversas herramientas para la educación. Sin embargo, este acceso está mediado por infraestructuras técnicas y centros de datos, los cuales pueden estar bajo el control o no de las instituciones educativas.

Las tecnologías pueden recabar distinto tipo de información sobre los estudiantes: actividades, calificaciones, interacciones y hasta el tiempo en que están conectados a una plataforma educativa. Con esta información es posible hacer un seguimiento para apoyar y mejorar el aprendizaje, para identificar a los estudiantes que necesitan mayor atención, o para evaluar la efectividad de las tecnologías aplicadas. Pero también surge la posibilidad de utilizar ese gran volumen de datos para propósitos distintos a los educativos. Por ejemplo, la explotación comercial que podrían realizar las empresas que procesan los datos. Por eso, no se puede confiar ciegamente en las soluciones tecnológicas, hay que analizarlas con una mirada crítica para evaluar sus implicancias legales y éticas.

El marco legal que rige en Uruguay para el manejo de datos personales es la Ley Nº 18.331 de Protección de Datos Personales. Esta ley sigue estándares internacionales, pero es compleja de aplicar cuando los usuarios están en territorio nacional y los servicios en la nube en jurisdicciones extranjeras. Las instituciones educativas, como cualquier entidad, tienen la obligación de recabar el consentimiento informado de los estudiantes para el tratamiento de sus datos, o el de los adultos responsables, si aquellos fueran menores.

Estas complejidades están presentes en Ceibal, institución que tiene contratos con proveedores internacionales como Schoology (para la plataforma educativa CREA2) y Google (para cuentas de correo, acceso a Google Apps for Education y laptops Chromebook). Estos contratos cumplen con la ley, según el análisis de la Unidad Reguladora de Protección de Datos. Además, Ceibal cuenta con políticas de privacidad y herramientas para recabar el consentimiento de los padres. Sin embargo, en los contratos con los proveedores persisten dudas sobre la forma en que son procesados los datos por las empresas, más allá del propósito educativo. Google, por ejemplo, no usa los datos de los estudiantes con fines publicitarios en sus productos educativos. Pero el contrato con Ceibal tiene algunas indefiniciones que hacen dudosa la posibilidad de realizar auditorías o de establecer un control real del uso de los datos, y que permitirían (o al menos no prohíben claramente) usar la información para crear perfiles individualizados y mostrar publicidad a los estudiantes en los productos Google para el público general, como el buscador o YouTube.

El programa ProEVA de Udelar ha construido una infraestructura tecnológica propia basada en software libre. Este camino a veces es más complejo que el de la contratación de servicios a terceros, pero la inversión en tecnologías y el desarrollo de capacidades queda dentro de la institución. En el uso de esta infraestructura no hay transferencia internacional de datos de estudiantes, ni terceras partes involucradas en su procesamiento. No obstante, la Udelar no ha publicado una política de privacidad para sus entornos virtuales de aprendizaje (la cual está en proceso de elaboración y aprobación). Consideramos que, una vez que la Udelar disponibilice de forma expresa la política de privacidad de sus plataformas, constituirá un buen modelo de gobernanza de datos personales en el sector educativo, ya que la ubicación local del centro de datos y las caracterísitcas de su infraestructura habilitan un control real y mejoran las oportunidades de los estudiantes para defenderse.

Los dos casos analizados tienen algunas buenas prácticas y otras más cuestionables o mejorables, lo que hace necesaria una reflexión crítica en torno a estas experiencias. Es importante que las autoridades de la educación se asesoren y evalúen las tecnologías usadas por miles de estudiantes de todo el país. También es necesario revisar el marco legal de protección de datos, basado en la ficción jurídica del consentimiento informado, que quizás no responde adecuadamente al desafío del *big data* en educación. No se trata de optar entre el uso de tecnología en la educación y la privacidad de los estudiantes. Lo fundamental es estar al tanto de las discusiones contemporáneas al respecto, buscando alternativas que contemplen al mismo tiempo el derecho a la educación y el derecho a la privacidad. ■

Aparicio Abella

La ética hacker

Fernando Briano,
desarrollador y hacker civico, DatySoc

Aparicio Abella

Nunca está de más señalar que el término *hacker* es de los más malinterpretados por el público general. En esencia, un hacker es una persona que cuenta con cierta habilidad y disfruta de resolver problemas y meter mano en las cosas para que funcionen de manera distinta a como fueron programadas. La idea de trabajar en equipo y el libre acceso a la información son principios fundamentales. Poco tiene que ver con la forma general de usar el término como sinónimo de ciber-criminal.

Los hackers promueven la colaboración como uno de sus pilares. Es así que de esta subcultura surgió el movimiento del software libre. Este lucha por la libertad y la privacidad de los usuarios de computadoras, alegando que son estos quienes deberían tener el poder sobre la tecnología que manejan y no al revés. Varios de los programadores involucrados con el software libre podrían ser denominados hackers. Trabajan "gratis" para que el código llegue a la comunidad en mejores condiciones o simplemente lo adaptan a distintas situaciones. Usan sistemas operativos libres como GNU/Linux, que no son llevados adelante únicamente por una empresa, sino por grupos de personas.

La idea de compartir el código y mantener un proceso de desarrollo abierto y transparente fue rechazada y atacada fuertemente en un principio por las corporaciones, porque darle poder al usuario va directamente en contra de sus intereses. Pero, como cualquier revolución, fue tomando fuerza lentamente gracias a quienes participan de ella. Eventualmente, el modelo de desarrollo abierto fue reconocido prácticamente como la mejor manera de desarrollar software. Corporaciones tradicionalmente cerradas a este tipo de trabajo empezaron a subirse al carro del desarrollo de código abierto, abriendo parte de su desarrollo a la comunidad, pero ignorando la parte ética en la que se centra el movimiento de software libre. Para estas grandes corporaciones, el modelo de colaboración resulta más eficiente, pero sólo hasta donde les conviene.

A medida que nuestras vidas se apoyan cada vez más en la tecnología, hay casos en los que prácticamente dependen de ella. Y si no prestamos atención a estos asuntos, como usuarios perdemos el control de lo que podemos hacer.

No sólo se "hackea" el software, sino que existen activistas detrás de un movimiento que impulsa el "derecho a reparar". Las empresas hacen lobby con los legisladores para evitar la creación de leyes que permitan a los usuarios reparar tanto teléfonos móviles como tractores. Los trabajadores del campo y aficionados a las computadoras han estado reparando sus máquinas por años, con o sin manuales o repuestos originales. Con estas nuevas leyes, las empresas se verían obligadas a vender repuestos y generar manuales para reparar los productos que fabrican y venden. De esta manera se le daría poder al usuario final, algo que los hackers intentan hacer de todas formas.

Un poco anarquistas, los hackers no confían en la autoridad. A diferencia de empresas y gobiernos, consideran la privacidad un derecho humano y así la defienden. Por lo tanto, luchan contra las prácticas de espionaje en las aplicaciones que recaudan datos personales de los usuarios indiscriminadamente. También prefieren sistemas distribuidos controlados por sus usuarios en vez de los silos centralizados de datos que son las redes sociales actuales.

Estas alternativas no son tan populares como las estándares de facto, que llevan inversiones millonarias por detrás. Pero existen y los hackers están trabajando en ellas.

Los programadores trabajamos en las interacciones de las personas con las máquinas, cada vez más presentes en la sociedad. Tenemos una responsabilidad de hacer que el código que escribimos y la tecnología que creamos no sólo haga su trabajo, sino que respete los derechos de las personas. Cualquier persona que se apropie de una tecnología o la intente modificar para que funcione a su gusto o la mejore es un potencial hacker.

Las computadoras pueden ayudarnos a hacer del mundo un lugar mejor. La alternativa es trabajar toda la vida para que hombres blancos con mucha plata tengan más plata. El mundo necesita más aspirantes a Steve Wozniak y menos a Steve Job. ■

¿Por qué la mayoría de los usuarios de internet usamos contraseñas tan inseguras?

Dr. Matias Dodel, investigador, Universidad Catolica del Uruguay

Existe una enorme diversidad de comportamientos o tácticas para protegerse en línea. Sin embargo, una y otra vez la predictibilidad de las contraseñas es considerada uno de los aspectos más críticos del problema sobre la ciber seguridad de los usuarios de internet (Carstens, 2009; Ur y otros, 2016).

Estudios recientes señalan algunas posibles aristas tras este fenómeno. Wash y otros (2016) encontraron que la reutilización de las contraseñas –uno de los principales problemas asociados a su predictibilidad– se incrementa con la complejidad de estas, así como en función de cuán frecuentemente son utilizadas.

Por otro lado, Ur y otros (2016) realizaron experimentos en los que compararon las contraseñas que los usuarios creen que son seguras con su fortaleza real en base a la cantidad de intentos necesarios para adivinarlas (en ataques de descifrado masivo o "de fuerza bruta"). Ur y otros (2015), utilizando una metodología más cualitativa, investigaron los procesos de creación de contraseñas. Ambos estudios encontraron que estos no son homogéneos entre los diferentes tipos de cuentas utilizadas (por ejemplo, bancos versus mails) y que varían de individuo a individuo.

En cuanto a posibles explicaciones acerca de las malas prácticas de creación de contraseñas, Ur y otros (2015; 2016) señalan la gran variación en la comprensión sobre cómo las contraseñas pueden ser atacadas. Ion y otros (2015) proponen que las percepciones problemáticas de los usuarios respecto de buenas prácticas de ciberseguridad se deben en gran parte a consejos de seguridad mal diseñados.

Sucede que, generalmente, los consejos o campañas de ciberseguirdad destinadas a usuarios de internet no contemplan los aspectos cognitivos y conductuales del comportamiento humano (Ion y otros, 2015) ni las diferencias e inequidades entre los internautas (Dodel y Mesch, 2018). Por ejemplo, abocarse a restringir el uso de internet o de determinados sitios para reducir riesgos puede parecer tentador, pero no sólo que los expertos en seguridad no la califican como una práctica efectiva (Ion y otros, 2015), sino que también es muy probable que limite el desarrollo y las oportunidades de los usuarios en la web.

Sin embargo, existe una serie de buenas prácticas menos dañinas que podrían ser relativamente costo-eficiente para usuarios con algo de colaboración de los desarrolladores. A modo de ejemplo, quisiera señalar dos propuestas interesantes.

En primer lugar, aumentar la usabilidad de programas que requieren conocimientos más técnicos (gestiones de contraseña o sistema de doble autenticación, por ejemplo) al incrustarlos en los sistemas operativos o transformarlos en soluciones de instalación única/permanente como actualmente sucede con los antivirus.

En segundo lugar, mejorar los contadores de fuerza de contraseñas parece crítico. En la actualidad estos señalan únicamente si los *passwords* son fuertes o débiles, pero los usuarios pueden no ser conscientes de los motivos por los cuales la contraseña que ingresaron es predecible o débil (Ion y otros, 2015; Ur y otros, 2016). Más allá de si utilizan mayúsculas y caracteres especiales, otros aspectos como la inclusión de términos comunes (por ejemplo, *dios* o *amor*) o el ingreso de una cadena de caracteres predecible (por ejemplo, "123", "qwe" o "=?¡") no se ven reflejados en estos contadores. ■

Referencias:

Carstens, D. S. (2009). "Human and social aspects of password authentication" en Gupta, M. y Sharman, R. (eds.) *Social and human elements of information security: Emerging trends and countermeasures.* Hershey: IGI Global.
Dodel, M. y Mesch, G. (2018). "Inequality in Digital Skills and the Adoption of Online Safety Behavior". *Information, Communication & Society,* 21(5).
Ion, I.; Reeder, R. y Consolvo, S. (2015). "'... No one Can Hack My Mind': Comparing Expert and Non-Expert Security Practices", en *Proceedings of the Symposium on Usable Privacy and Security (SOUPS).*
Ur, B. y otros (2015). "'I added '!' at the end to make it secure': Observing password creation in the lab", en *Proceedings of the Symposium on Usable Privacy and Security (SOUPS).*
Ur, B. y otros (2016). "Do Users' Perceptions of Password Security Match Reality?", en *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.*
Wash, R. y otros (2016). "Understanding password choices: How frequently entered passwords are re-used across websites", en *Proceedings of the Symposium on Usable Privacy and Security (SOUPS).*

Aparicio Abella

CIBERSEGURIDAD

Algunos piques

Ing. Mateo Martinez, confundador de Charrua

Venimos de un 2017 sumamente agitado en temas de ciberseguridad, en el que hemos visto el crecimiento del *ransomware* (*malware* para secuestro de datos). Lamentablemente, el pronóstico para 2018 no es mucho más alentador: se esperan muchos más ataques enfocados en celulares y tablets personales que en dispositivos corporativos, como sucedió el año pasado.

Existe además un alto crecimiento en la adopción de dispositivos hogareños (*Internet of things*, en inglés) que también serán un objetivo fácil para los atacantes. Cuando hablamos de atacantes, nos referimos a delincuentes que se aprovechan de la tecnología. La Real Academia Española, a finales de 2017, aceptó finalmente la palabra *hacker* con su verdadero significado: "experto en sistemas de seguridad y computación", en lugar del mal utilizado "pirata informático", como había sido definida en 2014, cuando ingresó como palabra a dicha academia.

¿Cómo los ciudadanos podemos protegernos ante estas amenazas? Si bien la tecnología avanza, los dispositivos evolucionan y su uso también, los cuidados mínimos son relativamente simples:

1. No cliquear en links no esperados.
2. No descargar aplicaciones de sitios de dudosa reputación.
3. No formar parte de cadenas de correos.
4. No creer en las estafas propuestas en internet (boleto de lotería, fortunas familiares, estafa nigeriana, etcétera).
5. Si es gratis, el producto somos nosotros.

Este último punto nos lleva a pensar también en cómo debemos cuidar nuestra privacidad en internet. Las redes sociales han creado un ambiente donde se ha perdido, en cierta forma, la privacidad, y muchas veces se expone información innecesaria, como la fecha de nuestras vacaciones, nuestros horarios habituales, la cantidad de personas que habitan en una casa, el posicionamiento por GPS en las fotografías, la ubicación actual, entre otros aspectos que terminan vulnerando la privacidad. Es hora de tomar conciencia y tener precauciones, como se hace fuera del mundo cibernético. En cuanto a los niños, lo fundamental es extender hacia internet los cuidados y enseñanzas de no hablar con desconocidos, no brindar información y cuidar la intimidad.

Pasando al ámbito de organizaciones y empresas, será un año de cambios sustanciales en aspectos de ciberseguridad. Esta dejará de ser una opción y de tomarse como un seguro frente a potenciales riesgos, ya que será casi obligatorio contar con medidas de seguridad contra ataques cibernéticos; por lo tanto, se recomienda generar simulacros de incidentes, definir cómo se actuará frente a una crisis que impacte en el negocio y planificar su recuperación.

El pronóstico para 2018 es que los ataques serán del tipo *fileless,* es decir, no necesitarán que un usuario ejecute un archivo, sino que se aprovecharán de las vulnerabilidades de los sistemas para acceder a las organizaciones.

Sumado a esto, las técnicas de inteligencia artificial y *machine learning* empiezan a incorporarse a las técnicas de los atacantes, generando una gran desventaja para las organizaciones que no cuentan con protección adecuada. Por lo tanto, se hacen necesarias soluciones que analicen y generen perfiles de los atacantes y que puedan tomar decisiones inteligentes a la hora de lograr defensas efectivas. ■

LEGISLACIÓN SOBRE DELITOS EN LA RED

¿Qué es ser un delincuente en la era digital?

Dr. Fabrizio Scrollini, investigador a cargo de Datysoc

¿Es lo mismo que ser un delincuente común? ¿Cómo debería regularse el fenómeno del ciber-delito si es que tal cosa existe? ¿Es lo mismo organizar una protesta en línea que atacar los servidores de una planta de energía? ¿Y puede esta regulación actuar en contra de la innovación? En un momento crucial para el crecimiento de Uruguay en el desarrollo de las TIC y la conversión del país en un polo tecnológico en la región, la tipificación sobre los delitos informáticos resurge constantemente, más aún teniendo en cuenta la puesta en funcionamiento de la reforma del Código de Proceso Penal y, en un futuro, del Código Penal.

¿Dónde estamos?

Uruguay lidera en múltiples rankings de gobierno electrónico a nivel global. Sin embargo, hay un área donde desde hace ya unos años se señala un debe: los delitos informáticos. Por ejemplo, el informe "Ciberseguridad: ¿estamos preparados en América Latina y el Caribe?", elaborado conjuntamente por la Organización de los Estados Americanos y el Banco Interamericano de Desarrollo, sitúa a Uruguay por debajo del nivel "formativo" de madurez en delincuencia cibernética, investigación jurídica y divulgación responsable de información, muy por debajo de su promedio general en el índice. Si bien existen algunos delitos que pueden ser considerados como "informáticos", estos se encuentran desperdigados en varias normas y siempre se señala desde el exterior la falta de esa preciada Ley de Delitos Informáticos. Pese a que el Parlamento ha estudiado diversos proyectos provenientes del Poder Ejecutivo y de los legisladores de la oposición, ninguno logró prosperar en su camino.

¿Hacia dónde se quiere ir?

Uno de los principales problemas que enfrentan los proyectos presentados es que se basan en soluciones extranjeras, que pueden haber servido para la realidad de otros países pero no necesariamente sirvan para el nuestro. Sin embargo, resulta difícil conocer exactamente cuál es nuestra realidad cuando no existen cifras oficiales sobre el tema, ni se han realizado estudios criminológicos que permitan identificar las características de autores y víctimas de este tipo de conductas.

De esta forma, la preocupación por legislar lleva a buscar a tientas en el derecho penal soluciones, colocando la carreta por delante de los bueyes. El derecho penal es la última herramienta disponible, que sólo actúa cuando los demás mecanismos de prevención social han fallado. Pretender encontrar en él las soluciones es el primero de los problemas a resolver. La industria de la seguridad es generalmente reticente a revelar qué tipo de incidentes y qué daños se han causado, e irónicamente ese secretismo es el que termina poniendo más en riesgo a todo el sistema.

Por ejemplo, una mala técnica legislativa puede llegar a criminalizar conductas legítimas y especialmente protegidas como pueden ser las parodias en redes sociales o el hackeo de sombrero gris, aquel que tiene como fin comprobar vulnerabilidades de un sistema y reportarlas para su solución. El ya conocido caso del hackeo al Sistema de Transporte Metropolitano o el potencial reporte de vulnerabilidad de una aplicación bancaria, podrían ser considerados delitos, cuando en realidad son formas de poner en alerta a los administradores de estos sistemas, sin generar daños. Una mala regulación puede poner en riesgo la seguridad de todas las partes. Por otro lado, ninguno de los proyectos menciona la divulgación responsable de información, los famosos *whistleblowers*, lo que podría llevar a mejores prácticas de transparencia, sin miedo a represiones o revanchismos. Y tampoco los proyectos refieren a protocolos acerca de cómo llevar adelante denuncias.

Próxima estación: ¿Budapest?

El Convenio de Cibercrimen del Consejo de Europa, conocido como Convenio de Budapest, es la referencia a nivel global para la persecución de este tipo de delitos. Sumarse a Budapest no significa trasladar automáticamente un conjunto de normas rígidas que no puedan ser modificadas. Dentro de cada uno de los tipos penales, la redacción de Budapest otorga un margen de elección a los legisladores de cada país, de forma tal que la norma se vuelve más o menos punitiva, es decir, más o menos gente adentro de la cárcel.

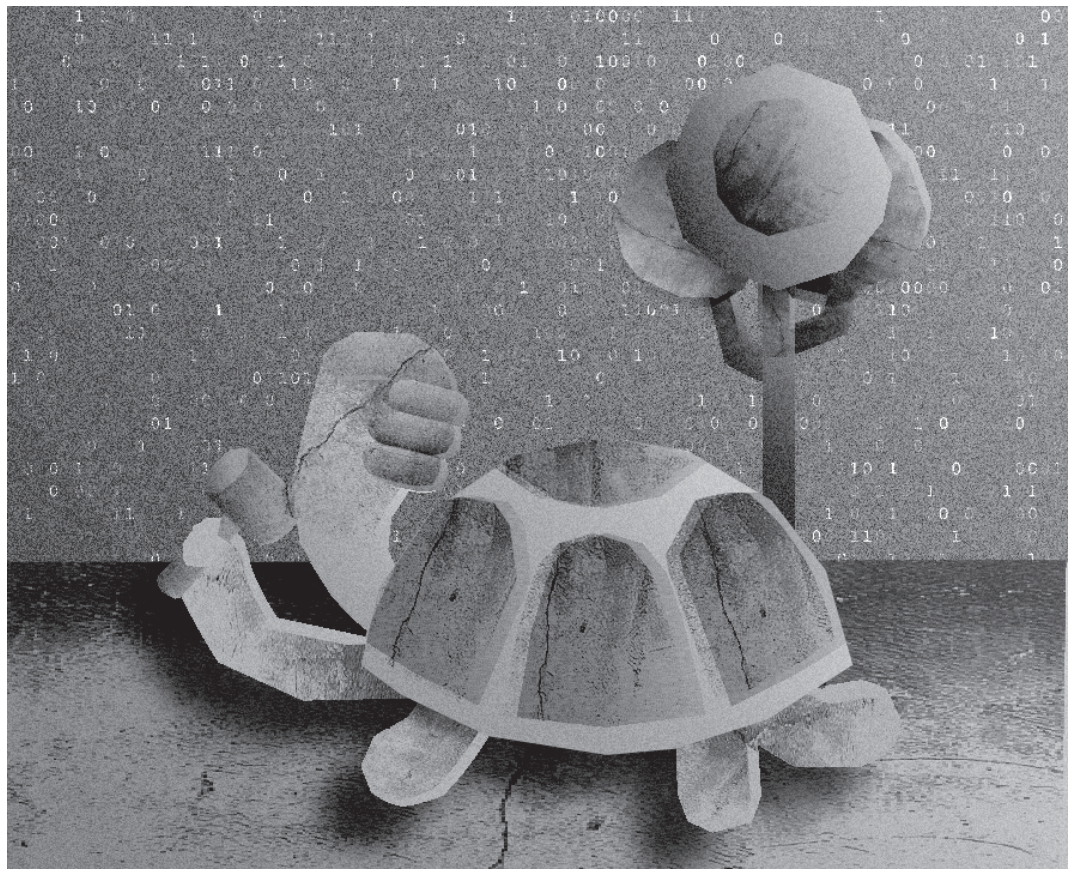
Por otra parte, el Convenio de Budapest no sólo incluye delitos, sino también normas procesales, las más discutidas dentro del Convenio. Un desbalance a favor de la seguridad por sobre las garantías de los ciudadanos es en donde los países han puesto más reservas a la hora de ratificar. ¿Pueden o deben los gobiernos grabar todas sus actividades en línea? Y de ser así, ¿cuándo? ¿Qué límites tienen? La injerencia de terceros países dentro de prácticas locales, que pueden perjudicar derechos como la privacidad, resulta una discusión que aún estamos muy lejos de dar si pretendemos continuar por este camino. Por otro lado, Budapest fue pensado para un mundo anterior a las revelaciones de Edward Snowden y la compra por parte de varios gobiernos de herramientas de espionaje, así como para un mundo donde el tráfico de datos personales transfronterizos era mera especulación.

Reflexiones para el camino

Hasta ahora, los proyectos presentados enfocan sus baterías en la criminalización de conductas cometidas a través de internet o contra algún sistema informático, o bien plantean trasladar las normas de Budapest automáticamente, sin coherencia con nuestro ordenamiento jurídico. La adhesión al Convenio de Cibercrimen debe ser una decisión estudiada, evaluando individualmente cada una de las normas, evitando la adopción en bloque sólo para cumplir con listas internacionales.

Tal vez la regulación debería ser encarada desde una perspectiva más amplia, que contemple derechos humanos, y no desde la prohibición, menos aún una prohibición de tipo penal. Brasil ha abierto el camino a través de su Marco Civil de Derechos Digitales, una especie de Constitución en la que Gobierno, Técnicos y Sociedad Civil sentaron las bases sobre las que se apoyará la regulación de las redes en ese país. Dicho de otra forma, en lugar de pensar en las patologías y conductas posiblemente ilegales (que las hay) uno podría comenzar a discutir los derechos y cómo protegerlos en línea, naturalmente utilizando el derecho penal y la evidencia disponible para generar regulación que pueda cumplirse. ■

Este texto se basa en una invesitgacion del Dr. Matias Jackson para Datysoc en el 2017



Luciana Peinado

la diaria

Redacción: 2900 0808
Treinta y Tres 1479 Montevideo, Uruguay
ladiaria@ladiaria.com.uy
twitter.com/ladiaria

Dirección: Lucas Silva | Diseño: Luciana Peinado | Textos: Fernando Briano, Patricia Díaz, Matías Dodel, Lorena Echeverry, Mariana Fossatti, Tomás Laurenzo, Mateo Martínez, Fabrizio Srollini, Ana Tuduri | Corrección: Victoria Olivari | Ilustraciones: Aparicio Abella, Luciana Peinado

DATA&SOC

Con el apoyo de: OPEN SOCIETY FOUNDATIONS