Fundación Vía Libre

enero a diciembre

vía libre

¿Qué sucedió en el 2020?

Una recopilación de los editoriales de Fundación Vía Libre

Por Bea Busaniche
Presidente de Fundación Vía Libre

Contenidos

Enero

¡Gracias por acompañarnos en esta nueva edición de nuestro boletín mensual! ¡En este enero de inusual actividad en Argentina, queremos desearles un feliz año 2020!

Febrero

En defensa de la libertad de expresión

Marzo

Desde Vía Libre celebramos los anuncios del Presidente Alberto Fernández sobre la reforma de los servicios de inteligencia.

Abril

El Estado de Derecho es el camino

Ciberpatrullaje en la pandemia

Mayo

El derecho de autor ante la emergencia y el aislamiento

Sobre los límites en el uso de la tarjeta SUBE y el control del sistema de transportes en la pandemia

Junio

Trump vs. Twitter: ¿Alguien puede pensar en los usuarios?

Inteligencia Ilegal. Por un Nunca Más de los sótanos de la democracia

Julio

Ciberpatrullaje: Se conformó la mesa consultiva de seguimiento del protocolo del Ministerio de Seguridad

Identificación biométrica para exámenes en Universidades Nacionales: ¿Otra solución en busca de problemas?

Agosto

La Agencia de Protección de Datos Personales recomienda suspender la práctica de 'Ciberpatrullaje'

Algunos apuntes preliminares sobre la acción judicial de CFK contra Google

Hacia una política pública de protección de activos digitales en Argentina

Un indispensable debate sobre los servicios de telefonía e Internet en Argentina

Septiembre

La geopolítica de Tik Tok. ¿Hacia dónde van las políticas de Internet?

Historia clínica digital: ¿Por qué no?

Una vez más: urge una política de protección de los activos digitales en poder del Estado

Regulación del Reconocimiento Facial en la Ciudad Autónoma de Buenos Aires

Octubre

Volver a las fuentes. Hacia una política de autonomía basada en Software Libre

¿Será posible remediar la hiperconcentración del mercado de las Big Tech?

En defensa del derecho a cifrar

Reconocimiento Facial en Buenos Aires. ¡Nos ven la cara!

Noviembre

¿Puede un algoritmo dejarte sin empleo?

Historia Clínica Digital: Información sensible y altos riesgos

Allanar al mensajero

El voto electrónico no es seguro como el conteo tradicional en papel

Vía Libre cumple 20 años

Diciembre

10 de diciembre. Día Internacional de los Derechos Humanos

¿Y si Google dejara de funcionar?

Requisitos mínimos para una política de seguridad de la información en la Administración Pública Nacional

Anuario Vía Libre 2020

Enero

¡Gracias por acompañarnos en esta nueva edición de nuestro boletín mensual! ¡En este enero de inusual actividad en Argentina, queremos desearles un feliz año 2020!

VER EL NEWSLETTER COMPLETO

Con la asunción del nuevo gobierno argentino, el panorama para este año se plantea todavía abierto en cuestión de prioridades de agenda de temas y actividades. Sin embargo, es fundamental destacar uno de los apartados del discurso inaugural del Presidente Alberto Fernández sobre la reforma judicial y los servicios de inteligencia en Argentina.

Como integrantes de la Iniciativa Ciudadana para el Control de los Servicios de Inteligencia (ICCSI), desde 2012 venimos trabajando para poner límites a lo que el Presidente denominó "los sótanos de la democracia". El sistema democrático no puede tolerar ese tipo de ejercicio del poder basado en el oscurantismo, la extorsión y el manejo a discreción de uno de los poderes de la República como es el Poder Judicial, específicamente el fuero federal. En este sentido, desde la Fundación Vía Libre tenemos enormes expectativas y vamos a seguir de cerca las nuevas estrategias para resolver un problema que ningún gobierno de la democracia ha podido solucionar hasta la fecha.

Desde Vía libre le damos la bienvenida a la Dra. Cristina Caamaño a cargo de la intervención de la AFI. Conocemos a la funcionaria porque mantuvimos diversas reuniones con ella mientras estuvo a cargo de la oficina de escuchas. Durante su gestión visitamos y recorrimos las oficinas de la ex OJOTA (Oficina de escuchas judiciales) y tuvimos acceso a buena parte del complejo diagnóstico de situación en ese espacio. La tarea que Caamaño tiene a cargo hoy en día es todavía más compleja que aquella que llevó adelante en la oficina de escuchas y le deseamos el mayor de los éxitos en la misión de sanear los servicios de inteligencia para que cumplan con los principios fundamentales que deben cumplir en el marco del sistema democrático. Estaremos aquí para aportar en la medida de nuestras posibilidades y para criticar cuando sea necesario.

Entendemos que la reforma integral de los servicios de inteligencia requiere tiempo y una estrategia apropiada. Sin embargo, hay cuestiones urgentes que ya se pueden poner en práctica y que desde ICCSI demandamos como una primera medida: prohibir la intervención de la AFI en investigación criminal.

Sobre finales del gobierno de Cristina Fernández de Kirchner, cuando por ley se reformaron los servicios de inteligencia y se creó la Agencia Federal de Inteligencia (AFI), cuestionamos lo mismo que cuestionamos hoy: la llave que permitió en estos años mantener la connivencia de los servicios de inteligencia y la justicia. Advertimos sobre el problema serio que conlleva que la ley vigente no marque este límite con una clara y estricta separación funcional. Es ahí donde vemos hoy por hoy el primer punto de urgente resolución y por eso enviamos una nota a las nuevas autoridades para que tomen cartas inmediatas en este asunto.

Este no será el único asunto que nos mantenga ocupados durante este 2020. Diversos temas de agenda nos convocan y vamos a seguir trabajando en ellos durante este año.

Vemos con preocupación algunas ideas vinculadas a la reforma de la ley de propiedad intelectual en Argentina, factor que entendemos esencial para el desarrollo del país, por lo que vamos a sostener nuestro trabajo en promover un debate cada vez más amplio sobre regulaciones de propiedad intelectual desde una perspectiva progresista, que privilegie el acceso y participación en la cultura y ponga el foco en los incentivos apropiados para la creatividad. Vamos a fortalecer nuestras alianzas con el movimiento de bibliotecarios, archivistas y museos con quienes planeamos una agenda intensa de trabajo a fin de lograr una legislación que facilite y promueva el acceso y preservación de la cultura.

También se abren diversas agendas vinculadas con las regulaciones de la economía de las plataformas o la 'GIG economy'. Con la entrada en vigencia de las regulaciones laborales en California como ejemplo, entendemos inminente y urgente un debate que contenga y promueva los derechos laborales de aquellos que trabajan a través de empresas montadas casi exclusivamente en las aplicaciones. Los temas impositivos, de regulación laboral y de derechos no nos son ajenos en absoluto y seguiremos de cerca las iniciativas que está abriendo la nueva administración nacional. Se suma a todo esto el impacto cada vez más evidente del desarrollo de sistemas de inteligencia artificial sobre los cuales hemos estado y seguiremos trabajando.

Lo propio haremos con aquellas regulaciones vinculadas a libertad de expresión en la red y las iniciativas sobre discurso de odio, discriminación y autoregulación de las plataformas. Es cada vez más preocupante la restricción del discurso regulado por términos de uso y en definitiva sin las garantías de libertad de expresión plena, pero a su vez es crítico desarrollar un marco regulatorio para un sistema complejo donde se cruzan tensiones evidentes entre la regulación privada, la violencia en línea, la demanda de soluciones por parte de gobiernos y organizaciones de sociedad civil y la falta de respuestas satisfactorias frente a problemas complejos y colectivos como la discriminación y la violencia.

Finalmente, pero no menos importante, esperamos que en este año podamos trabajar en dotar a Argentina y la región de un marco jurídico de protección de datos personales efectivo y apropiado para los tiempos que corren.

El 2020 es un año muy especial para la Fundación Vía Libre: es el año de nuestro cumpleaños número 20. Es un hito para nuestra Fundación haber llegado hasta acá con una agenda compleja, diversa y en franco crecimiento desde hace años, haber respondido a una demanda pública de posicionamiento sobre temas conflictivos muchas veces, difíciles siempre y desafiantes por lo novedoso y complejo de los escenarios en los que nos toca no sólo actuar, sino incidir y formar opinión.

¡Por eso, en este 2020 más que nunca, les deseamos un excelente año y agradecemos infinitamente a quienes nos han ayudado a llegar hasta aquí!

Febrero

En defensa de la libertad de expresión

VER EL NEWSLETTER COMPLETO

En las últimas semanas, la empresa Twitter anunció nuevas reglas para la convivencia en ese espacio de debate que, a pesar de ser una plataforma privada, es una de las esferas más intensas del debate público. Digo intensas por no usar otros adjetivos, aunque bien podríamos hablar de que Twitter es la red donde el debate político es más ríspido, donde abundan las agresiones y las opiniones de todo color y tono, incluyendo las más indeseables e incómodas. La comunidad de usuarios de Twitter le ha dado esa impronta por razones que yo misma desconozco, pero que le han dado un perfil a esa red social. Es también, el lugar donde vemos ironías volar de un lado al otro, humor, sarcasmo y muchas otras prácticas del discurso humano (demasiado humano).

En su afán por "controlar el cumplimiento de nuestras reglas y garantizar la calidad y la seguridad de las conversaciones en Twitter" expresa la empresa en su comunicación sobre las nuevas reglas, la empresa amenaza romper ese clima de debate intenso que caracteriza ese espacio y pone en jaque algunos principios fundamentales de la libertad de expresión.

Dice Twitter: "Está prohibido compartir, con la intención de engañar, contenido multimedia falso o alterado que pueda dar lugar a daños graves. Asimismo, es posible que etiquetemos los Tweets que incluyen contenido multimedia falso y alterado para ayudar a los usuarios a comprender su autenticidad y para ofrecer más contexto."

Desde Vía Libre vemos con máxima preocupación esta tendencia, de la cual Twitter forma parte, de construir espacios seguros de debate sin definición clara y concreta de qué y cómo se construye esa mentada seguridad.

Las reglas que se plantean son por demás ambiguas y dejan lugar a arbitrariedades de todo tipo:

- Que el contenido audiovisual haya sido manipulado con intención de engañar.
- Que el contenido se comparta de manera engañosa.
- Que el contenido tenga impacto en la seguridad pública o provoque daños graves.

Las debidas explicaciones sobre cada uno de los factores a considerar dejan más dudas que certezas, ya que mantienen rasgos de ambigüedad problemáticos a la hora de dirimir la calidad de un discurso. En este sentido, otro factor de preocupación es que para que el contenido sea etiquetado y/o eliminado, no hace falta que reúna las tres condiciones sino que con una sola alcanza para recibir el llamado de atención.

¿Qué pasa con un contenido etiquetado? ¿Quién toma la decisión de etiquetarlo ¿Están en condiciones de aplicar mecanismos automatizados para identificar estos contenidos? y finalmente la gran pregunta: ¿Por qué consideramos indeseables estos contenidos?

Como ciudadanos, hemos tenido grandes dificultades para defender un derecho esencial como la libertad de expresión. Las sociedades no maduran ni prosperan escondiendo lo que no les gusta o consolidando un discurso único. No podemos caer en la trampa del consenso. Una voz, una sola disidente tiene derecho a existir y a ser protegida. La libertad siempre es la libertad de los que no piensan como nosotros.

Está en la madurez de nuestra sociedad lidiar con discursos abominables, engañosos o simplemente falsos. Esconderlos no soluciona los problemas, los magnífica y al final sabemos que la censura (pública o privada de contenidos) jamás ha sido solución a los problemas de la sociedad.

Para la empresa Twitter esto parece ser una decisión clave para no quedarse afuera de una tendencia que avanza tanto por parte de los Estados como de las grandes corporaciones de Internet. Para los ciudadanos, es un claro retroceso en una materia indispensable como la libertad de expresión en la red.

Marzo

Desde Vía Libre celebramos los anuncios del Presidente Alberto Fernández sobre la reforma de los servicios de inteligencia.

VER EL NEWSLETTER COMPLETO

Entre los anuncios realizados este 1 de marzo en el inicio de las sesiones ordinarias del Congreso Nacional se destaca una línea breve pero contundente pronunciada por el Presidente Fernández: la inminente firma de un Decreto de Necesidad y Urgencia para resolver uno de los temas más críticos y complejos en relación a los servicios de inteligencia.

Se trata de la modificación del artículo 4 inciso 1 de la ley 25.520 que expresa lo siguiente:

"ARTICULO 4° — Ningún organismo de inteligencia podrá:

1. Realizar tareas represivas, poseer facultades compulsivas, cumplir, por sí, funciones policiales ni de investigación criminal, salvo ante requerimiento específico realizado por autoridad judicial competente en el marco de una causa concreta sometida a su jurisdicción, o que se encuentre, para ello, autorizado por ley."

El anuncio del Presidente indica que, a partir de esta semana, será eliminada la excepción que habilita el requerimiento judicial, poniendo fin a una práctica histórica que ha marcado un rumbo equivocado de los servicios de inteligencia.

Dijo Fernández en la sesión que a partir de ahora quedará prohibido para los servicios de inteligencia "realizar tareas represivas, poseer facultades compulsivas, cumplir funciones policiales ni de investigación criminal" y punto, sin excepción ni mandato judicial de ningún tipo.

Esta es una vieja demanda de nuestra Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI). Es una pauta que está allí desde que se modificó la ley vigente durante el último año de la Presidencia de la Dra. Cristina Fernández de Kirchner y que criticamos enfáticamente en el momento de aquella reforma que dio origen a la AFI.

Los servicios de inteligencia no tienen que mantener relaciones con el poder judicial, no deben responder a éste ni deben intervenir en ningún tipo de tarea vinculada con la investigación criminal. Ese no es el rol de los servicios de inteligencia en una democracia. Para investigar delitos complejos y realizar ese tipo de investigaciones ajustadas a derecho se debe contar con una policía de investigaciones que trabaje bajo la órbita de un juez de garantías que asegure los principios fundamentales del debido proceso judicial.

Celebramos en su momento los anuncios hechos por el Presidente Fernández en la asunción de su mandato y entendemos que este anuncio no es un paso menor en ese camino, sino un avance indispensable para anticipar una reforma integral del sistema de inteligencia que ponga fin a prácticas reñidas con el sistema democrático.

En este sentido, desde la Fundación Vía Libre acompañamos y celebramos la decisión de modificar el artículo 4, inciso 1 de la Ley de Inteligencia anunciado en el inicio de las sesiones ordinarias.

Abril

El Estado de Derecho es el camino

VER EL NEWSLETTER COMPLETO

En estos días de aislamiento físico obligatorio, desde Vía Libre venimos haciendo diversas actividades que tienen que ver con nuestra agenda propia, pero que hoy está totalmente trastocada por la crisis global de Covid-19. No podemos estar ajenos a lo que ocurre en nuestro país, nuestra región y el mundo entero. En este sentido, identificamos al menos dos temas que tocan de cerca nuestro trabajo de los últimos 20 años: la protección del derecho a la privacidad de las personas y los aspectos vinculados a la propiedad intelectual.

En ambos casos, hemos estado trabajando con instituciones amigas para contribuir con información y ampliar el debate sobre la coyuntura que nos toca transitar. Lo seguiremos haciendo, así que sigan nuestras cuentas de redes sociales para enterarse de las próximas actividades.

En relación a los aspectos vinculados a la propiedad intelectual, nos satisface ver que son muchas las instituciones y gobiernos que están entendiendo la necesidad de poner los derechos fundamentales en materia de acceso a la salud por encima de la agenda de comercio y las regulaciones de propiedad intelectual vigentes. Así lo indican las principales declaraciones y lineamientos de derechos humanos e incluso la Organización Mundial de Comercio que, desde la 'Declaración de Doha sobre propiedad Intelectual y Salud Pública' reconoce con claridad la potestad de los Estados para establecer licencias obligatorias, importaciones paralelas y toda medida que sea necesaria para la atención de una emergencia sanitaria como la que atravesamos.

En ese sentido, es destacable informar que Argentina ya cuenta con este tema en su agenda. En la Ley de Solidaridad Social y Reactivación Productiva en el marco de la emergencia pública, aprobada sobre finales del 2019, lejos aún de la coyuntura actual de emergencia sanitaria, queda establecido que:

"Artículo 70.- Facúltase al Ministerio de Salud para establecer un mecanismo de monitoreo de precios de medicamentos e insumos del sector salud y de alternativas de importación directa y licencias compulsivas u obligatorias, frente a posibles problemas de disponibilidad o alzas injustificadas o irrazonables que afecten el acceso de la población a los mismos de manera que puedan poner en riesgo su salud.

Asimismo, facúltase al Ministerio de Salud para dictar las normas complementarias tendientes a implementar:

a) En acuerdo con el Instituto Nacional de Servicios Sociales para Jubilados y Pensionados, un listado de medicamentos e insumos a ser adquiridos por este organismo y por la Superintendencia de Servicios de Salud;

b) Precios de referencia de insumos y medicamentos esenciales por banda terapéutica;

c) Controles y dispositivos que promuevan la plena vigencia de la ley 25.649 de Especialidades Medicínales-Medicamentos Genéricos, con particular referencia a la prescripción y sustitución en la dispensación."

Es decir, Argentina cuenta ya con los instrumentos y la vocación política de aplicarlos en caso de necesidad.

En relación al segundo tema de nuestra agenda que preocupa sobremanera, la protección de datos y la privacidad de las personas, vemos allí un desafío mayúsculo en una sociedad que históricamente poco valora este derecho contemplado en todos los instrumentos de Derechos Humanos y que tiene rango constitucional en Argentina.

Junto a una larga lista de organizaciones globales, hemos acompañado una carta a gobiernos de todo el mundo sobre la protección de los derechos de las personas en este estado de excepción que estamos atravesando. El monitoreo que pueda eventualmente realizarse sobre personas portadoras del virus, inmigrantes, viajeros recién arribados, personas con síntomas de la enfermedad entre otros, deben ser considerados justamente medidas de excepción, limitadas en el tiempo, usadas sólo bajo estricta necesidad, implementadas en absoluta transparencia y eliminadas ni bien pase la razón que justificó su uso, con la consiguiente destrucción de registros que permitan o habiliten discriminación o afectación de derechos de las personas. Los datos personales médicos son datos sensibles y deben ser tramitados con total y absoluto cuidado y responsabilidad.

El hecho de que sociedades de máximo nivel de vigilancia hayan podido lidiar con la pandemia de forma eficiente torna aún más difícil instalar la legitimidad de un reclamo de privacidad que parece secundario ante la emergencia sanitaria. Sin embargo, plantear que existe una dicotomía insalvable entre el estado de derecho y la salud pública es una perversión tan seria como aquella instalada en 2001 y aún vigente sobre seguridad vs. privacidad.

No es posible pensar en ninguna opción en la cual se justifique la suspensión del estado de derecho para sortear la pandemia. Como sociedades, es indispensable asumir las responsabilidades que nos tocan para que no se profundicen aún más las medidas de excepción. La salud pública hoy es nuestra prioridad, ocupemos el lugar que nos toca.

Seamos responsables. Quedémonos en casa.

Un agradecimiento enorme a todas las personas que tienen que salir a trabajar porque su actividad es fundamental. Gracias y cuídense mucho. ¡Nuestro aplauso a ustedes!

Abrazo a la distancia!

ciberpatrullaje en la pandemia

VER EL NEWSLETTER COMPLETO

¡Antes que nada, gracias por estar ahí leyendo! Verán que, a partir de hoy, nuestro boletín deja de ser mensual para pasar a ser quincenal. Sentimos la necesidad de mantener una comunicación más fluida y regular con quienes siguen el trabajo de nuestra fundación. Contrariamente a otros rubros que han entrado en un parate total con la cuarentena, el trabajo de Vía Libre se mantiene vigente y consideramos necesario incrementarlo en algunas de nuestras áreas específicas de trabajo. La defensa del Estado de Derecho es, sin dudas, una de esas áreas centrales.

Y si hablamos de Estado de Derecho, no podemos obviar un tema que nos parece indispensable seguir y mantener a la ciudadanía informada sobre lo que sucede: el "ciberpatrullaje" que sigue en marcha pese a las advertencias de todos los organismos de Derechos Humanos.

El viernes 17 de abril participamos de una reunión con la Ministra de Seguridad, Sabina Frederic. El encuentro se centró en la presentación de un borrador de protocolo para la implementación de las tareas de "ciberpatrullaje" que realizan las fuerzas de seguridad federales e incluso algunas provinciales. La Ministra nos explicó que actualmente están utilizando un protocolo que quedó vigente desde la gestión anterior, publicado en el año 2018, pero que la voluntad es reemplazarlo por uno nuevo para el cual se nos pidió colaboración.

Nuestra posición, como ya lo hemos dicho, es de total rechazo a este tipo de estrategias de vigilancia masiva. Sin el marco de una investigación criminal puntual, sin el control jurisdiccional apropiado y sin los límites que marca la ley, el ciberpatrullaje no es una práctica inocente y amigable de prevención: el ciberpatrullaje es inteligencia de fuente abierta y como toda forma de inteligencia está prohibida expresamente por ley.

La analogía que pretende emparentar el ciberpatrullaje al oficial de las fuerzas de seguridad que deambula por el espacio público y actúa cuando ve un hecho delictivo es absolutamente falaz. Quien hace la tarea de monitorear las redes no sólo no deambula por ahí inocentemente, es un oficial de las fuerzas que no se identifica como tal (primer elemento fundamental del accionar de las fuerzas de seguridad en cumplimiento de su tarea), que escucha conversaciones que pueden estar sucediendo en ese espacio semi-público como las redes sociales e internet y que sistematiza y analiza la información que recopila. Esa definición es la definición misma de hacer inteligencia.

En esta semana vamos a responder a la convocatoria del Ministerio de Seguridad a hacer comentarios sobre el borrador del protocolo que estamos analizando y junto a nuestras organizaciones colegas de la Iniciativa Ciudadana para el Control del Sistema de Inteligencia (ICCSI) vamos a presentar las objeciones que tenemos a la práctica y el protocolo.

Vivimos tiempos excepcionales donde muchos elementos fundamentales del Estado de Derecho están en suspenso. Sin ir más lejos, el derecho a la libre circulación está virtualmente suspendido en favor de otro derecho fundamental que tiene que ver con el derecho a la salud y las políticas sanitarias para la salud pública. Es un momento donde el Estado tiene que fortalecer más que nunca su relación con la ciudadanía. Es un momento en que las garantías deben ser extremadas.

La salida punitiva a la crisis, la utilización de la sanción penal ante la publicación de opiniones, incluso opiniones molestas, provocativas, y muy especialmente irónicas debe ser el último recurso en el marco de una situación social que requiere cuidar la paz social y fortalecer la confianza en las instituciones del Estado.

Lo sucedido con Kevin Guerra, a quien se le inició una causa penal por haber ironizado en Twitter, es inaceptable desde el punto de vista de la libertad de expresión. La figura de la "intimidación pública" aplicada en su caso y en otros similares ocurridos en las últimas horas es absolutamente exagerada, abusiva y, por lo tanto, repudiable como práctica en la cual no sólo han intervenido las fuerzas de seguridad sino y muy especialmente los fiscales y jueces que la han aplicado, cuando su rol fundamental es garantizar el Estado de Derecho y limitar cualquier atisbo de abuso policial e institucional.

Desde Vía Libre vamos a seguir trabajando intensamente este tema en estos días, junto con otros que nos convocan como la defensa del derecho a la privacidad y la intimidad, y el derecho de acceso pleno al conocimiento, la cultura y a gozar de los beneficios de la ciencia como dictan las normas internacionales de Derechos Humanos con rango constitucional.

¡Muchas gracias por estar ahí!

¡Cuídense mucho! ¡Nosotros seguimos trabajando desde casa!

Mayo

El derecho de autor ante la emergencia y el aislamiento

VER EL NEWSLETTER COMPLETO

Un grupo de Facebook de intercambio de lecturas, recomendaciones, sugerencias y si, por supuesto, .pdfs. Una comunidad de twitteras compartiendo lecturas en voz alta de grandes obras de la literatura. Estudiantes de todos los niveles pasándose capturas de páginas de libros que no llegaron a comprar y necesitan para sus cursadas. Docentes pasando bibliografía digitalizada a estudiantes.

El mundo de la pandemia se parece bastante a la peor pesadilla de aquellos que durante décadas nos llamaron 'piratas'.

Si algo ha desnudado esta situación (Además de las almas humanas, al decir de Albert Camus) es la necesidad urgente de salir del closet de la copia ilegal. Si, copiamos ilegalmente. Si, pasamos bibliografía a nuestros estudiantes. Si, leemos en voz alta. Si, recomendamos libros (y los pasamos en formato digital a otras personas). Si, somos delincuentes.

La copia no autorizada es un delito penal en Argentina. Así lo dicen los artículos 71 y 72 de la ley de propiedad intelectual vigente, la 11.723.

La Asociación de Bibliotecarios Graduados de la República Argentina consultó a la Dirección Nacional de Derechos de Autor si podía, en situación excepcional, hacer uso de las inexistentes flexibilidades disponibles para que las personas que trabajan en bibliotecas pudieran seguir cumpliendo su función central de disponibilizar el conocimiento, la cultura, los materiales de investigación, todo aquello que custodia y divulga una biblioteca.

La respuesta recibida no les sorprenderá: Las flexibilidades en materia de propiedad intelectual son posibles, pero esto sólo puede ser regulado por una ley aprobada en el Congreso. Ante la inexistencia de esa ley, la DNDA no puede por medio de resoluciones modificar el status quo vigente. Ante la inexistencia de una ley (que venimos pidiendo desde hace décadas), la política pública es ir a pedir permiso a las entidades que nuclean a los editores y otros titulares de derechos. Es decir, la política pública argentina sigue siendo consultar al sector privado que maneja la propiedad intelectual como si esto fuera efectivamente un asunto de privados y no un derecho fundamental que el Estado debe garantizar.

Por supuesto, como también era de esperar, la discusión en la emergencia se puso difícil y en algunos casos agresiva. Desde Vía Libre repudiamos toda forma de agresión a cualquiera de las partes de este debate.

Es indispensable entender que si un autor o autora pide en un grupo que no se comparta su obra, insultar no es la salida.

Lamentablemente, la experiencia nos dice que este debate se juega más en las tripas que en la evidencia y que tristemente, el sector más vulnerable de la cadena productiva de la propiedad intelectual tiene una perspectiva complicada. La gran mayoría (no vamos a generalizar) se ha formado en el tema escuchando el discurso de la industria cultural. Es fácil pensar que los responsables de que los autores no ganen un sustento digno con su obra somos los que copiamos sus libros sin permiso. Nada más alejado de la realidad.

No hay evidencia alguna que permita afirmar que los libros que se divulgan de manera digital no autorizada perjudican las ventas de ejemplares impresos. Es más, suele ocurrir que aquellos libros que más se comparten son efectivamente los que más se venden. Las ventas de libros dependen más del estado de situación de la economía en general que de la posibilidad o no de reproducirlos digitalmente y compartirlos.

Los países con industrias editoriales más sólidas son, justamente, aquellos en los que hay más y mejores flexibilidades al derecho de autor. Sin ir más lejos, EEUU y Europa cuentan con un número importante de flexibilidades a favor de bibliotecas, estudiantes, investigadores, personas con discapacidades e incluso cláusulas que habilitan ciertos usos comerciales amparadas en el uso justo de una obra.

La sistemática negativa de las cámaras del sector editorial, así como las entidades de gestión colectiva a dar una discusión rigurosa y bien fundada sobre las tres patas fundamentales del derecho a la cultura y su protección por la vía legal nos han traído a este momento en el cual la ciudadanía reivindica su derecho a leer, su derecho a estudiar, su derecho a compartir.

La ley de propiedad intelectual es tan estricta en Argentina que nadie está en condiciones ciertas de respetarla a rajatabla. La pandemia nos puso cara a cara frente a esta realidad. Y los autores que demandan que no compartan sus obras no son personas a las que haya que insultar, son personas con las que antes que nada, tenemos que aprender a conversar. Bienvenida/os al debate... Los que llevamos décadas tratando de construir una política pública de derechos culturales tenemos mucho para aportar.

Sobre los límites en el uso de la tarjeta SUBE y el control del sistema de transportes en la pandemia

VER EL NEWSLETTER COMPLETO

En los últimos días nos hemos visto desbordados de noticias y anticipos de medidas de acción para contener el avance de la pandemia de COVID-19. Sabemos que los gobiernos de todo nivel, desde el nacional hasta los gobiernos locales, están trabajando intensamente en arbitrar las medidas más apropiadas para contener el avance de los casos por un lado y flexibilizar algunas actividades por el otro. Desde nuestro lugar, estamos cooperando en la medida de nuestras posibilidades en todo lo que tiene que ver con las aplicaciones de tecnologías, el debate sobre propiedad intelectual y la protección de datos personales en todo nivel.

Es desde este lugar que queremos fijar posición frente a dos medidas que se barajan en las últimas horas y que tienen que ver con el uso de la tarjeta SUBE en el transporte público y los turnos para abordar los trenes interurbanos que unen la Ciudad Autónoma de Buenos Aires con diversos municipios del AMBA.

Sabemos y comprendemos plenamente que uno de los problemas centrales que hay que atacar es el hacinamiento en el transporte público y por

lo tanto es indispensable reservar su uso a las tareas esenciales. Sin embargo, consideramos desproporcionada la iniciativa tendiente a bloquear el uso de la tarjeta SUBE para quienes no califiquen en ese grupo.

Desde que se habilitó el uso de la tarjeta SUBE hace casi una década, advertimos enfáticamente que la nominación de las tarjetas de transporte suponía una amenaza a la privacidad y la libre circulación de las personas. Se nos tildó de exagerados, de paranoicos, entre muchos otros calificativos que no nos interesa ni recordar. Sin embargo, el tiempo nos dio la razón. La base de datos de la tarjeta SUBE se filtró y se hizo prácticamente pública varias veces. Pero no sólo hubo problemas de seguridad en el cuidado de los datos personales de los usuarios. El allanamiento del domicilio de Javier Smaldone en CABA nos ofreció la oportunidad de ver cómo se arma una causa a una persona para tratar de vincularla con un hecho delictivo con el que no tuvo nada que ver. En el expediente que el propio Javier hizo público se ve a las claras cómo las fuerzas de seguridad solicitaron los registros de la tarjeta SUBE para trazar sus movimientos. Este es sólo un caso conocido por nosotros. No dudamos de la existencia de otros similares, ya que parece ser una acción bastante común en este tipo de investigaciones.

Una vez más vamos a repetir casi como un mantra la expresión acuñada por Shoshana Zuboff: 'Toda tecnología que pueda ser usada para la vigilancia, será usada para la vigilancia'. Nominar la SUBE es una mala idea, es un problema de privacidad y tiene consecuencias sobre la libertad y los derechos de las personas. Lamentablemente, la cadena siempre se corta por lo más delgado y son los sectores populares, el personal de casas particulares, las y los beneficiarios de programas sociales, las y los niños, niñas y adolescentes que usan boletos escolares, los que no pueden darse el lujo de cuidar su privacidad y están obligados a nominar la tarjeta. Cuidar la privacidad es costoso y un lujo imposible para buena parte de la ciudadanía en sociedades desiguales.

La propuesta de bloquear la tarjeta para quienes no son personal esencial se inscribe en esta misma línea de acciones desproporcionadas que afectan al sector más vulnerable de nuestras sociedades: mujeres que deban salir en busca de ayuda ante un caso de violencia, personas que deben viajar a buscar medicación o insumos básicos, personas con problemas de salud que no se atienden en la emergencia de un centro médico pero que requieren una visita médica regular que no pueden suspender, trabajadores informales, empleados de sectores no esenciales que se vean obligados a asistir a sus trabajos sin que sus empleadores prevean otros medios de transporte. Si, entendemos la necesidad de descongestionar los servicios de transporte público. Si, entendemos la urgencia de tomar medidas para contener la diseminación de casos que además está impactando severamente en esas mismas poblaciones en situaciones extremas de vulnerabilidad.

Lamentablemente vivimos en un momento de la historia en el que ante cualquier problema la primera solución siempre parece ser una app o un recurso informatizado. Muchas veces este tipo de propuestas generan más problemas que las supuestas soluciones que prometen y en ese afán de 'hacer algo' perdemos de vista otras potenciales soluciones más prácticas pero menos marketineras.

En su momento, se justificó la incorporación de la SUBE afirmando que la información recolectada iba a servir para mejorar todo el sistema de transporte público, ya que se iba a contar con muchos datos que permitirían rediseñar frecuencias, fortalecer áreas críticas y mejorar el régimen de subsidios. Nada de esto ocurrió y años después de implementada la medida seguimos sufriendo las mismas flaquezas del sistema.

No todos tenemos cajeros automáticos, mercados y farmacias en cercanía. No todos tenemos un auto estacionado en la puerta o recursos para pagar un taxi. No todos tenemos quién nos haga las compras o gestione nuestras necesidades fundamentales en estos días de aislamiento social obligatorio. El colapso del transporte público es otro de los temas críticos indispensables a resolver y que la crisis de COVID-19 no hace más que poner una vez más sobre la mesa.

La nominación de la SUBE y la captura masiva de datos de cada persona que viaja demostró ser ineficiente para fortalecer y mejorar el sistema. Bloquear el uso de la tarjeta ante esta crisis no parece ser la excepción a esta regla.

Junio

Trump vs. Twitter: ¿Alguien puede pensar en los usuarios?

VER EL NEWSLETTER COMPLETO

Se viven días convulsionados en los EEUU, donde el número de víctimas fatales por la pandemia de Covid 19 supera largamente las 100.000 personas con un impacto económico sin precedentes desde la crisis del 29. En paralelo, el brutal asesinato de George Floyd despertó una ola de protestas que, mientras compartimos esta comunicación, se sigue alimentando de violencia, represión, amenazas y decenas de miles de personas en las calles de las ciudades de todo el país al grito de #BlackLivesMatter. En paralelo, una campaña electoral con miras a las elecciones presidenciales de Noviembre. Es en este contexto que debemos analizar el decreto ejecutivo (Executive Order) de Donald Trump sobre regulación de contenidos en redes sociales.

En primer lugar, es importante mencionar que la Orden Ejecutiva tiene algunos elementos valiosos en relación a su valor declarativo. A esta altura, ¿Quién podría discutir la afirmación de que las regulaciones de puerto seguro (la Sección 230 de la CDA) no están allí para permitir a un puñado de compañías controlar los espacios vitales del intercambio de debates o para habilitarlas a usar su poder de censura para silenciar ciertos puntos de vista?

El documento de Trump está plagado de afirmaciones vinculadas a la Primera Enmienda de la Constitución de los EEUU y el derecho sagrado a la libertad de expresión como fundamento de la democracia en los EEUU. Sin embargo, no hay mucho más que una acción declarativa allí donde es evidente que la misma estructura constitucional de los EEUU impide al presidente la modificación o la interpretación de una ley con este mecanismo.

El problema está sobre la mesa y es indispensable atenderlo. Las plataformas ejercen cierto tipo de control sobre la producción de los usuarios en diferentes niveles, formas y con diferentes mecanismos bajo el mandato de la CDA Sección 230. Vayamos por partes.

Las plataformas gozan de la protección (denominada inmunidad o puerto seguro) de la Ley para la Decencia en las Comunicaciones (CDA) que en su sección 230 establece que las empresas no serán responsables por los contenidos generados por los usuarios. Esta medida apunta justamente a proteger el discurso público de cualquier incentivo a la censura que podría significar la atribución de responsabilidad a las empresas. Si las empresas son responsables por lo que hacen las personas que las usan, la censura sería moneda corriente.

Sin embargo, bajo la cláusula del 'buen samaritano' que actúa de buena fe, la misma sección 230 habilita a las empresas a ejercer cierto tipo de control sobre discurso que se considere violento, indeseable, discriminatorio aún en casos en los que esté efectivamente protegido por las garantías de libertad de expresión. Acá es donde aparece el problema central de este asunto: en los usos que las plataformas han hecho de esta cláusula que les permite dar de baja contenidos y suspender usuarios que vulneren los términos de uso.

Trump protesta porque entiende que las empresas, y en particular Twitter, han operado para invisibilizar el discurso conservador y enfureció cuando la plataforma marcó como 'información engañosa' varias de sus publicaciones y les dio contexto a partir de mecanismos de 'fact checking'. Además, la empresa Twitter marcó como 'exaltación de la violencia' un mensaje del presidente. Ese mensaje no fue borrado en función del interés público que supone el mensaje de un presidente. Vale recordar que este no fue el mismo trato propinado al Presidente Jair Bolsonaro, de Brasil, a quien directamente le eliminaron algunas de sus publicaciones por contenidos violentos.

La reacción de Trump es tratar de retirar las inmunidades y hacer a las plataformas directamente responsables como

editores. Ahí es donde está el problema central de una supuesta solución que sólo terminará de apuntalar un problema que es evidente.

Es importante mencionar que la OE de Trump no tiene la capacidad de modificar la regulación vigente, la Sección 230 de la CDA. Tampoco tiene potestades en la interpretación de la norma, atribución exclusiva de los tribunales. También es clave agregar que Trump ordena a los órganos reguladores desarrollar medidas en este sentido. Esos órganos reguladores como la FCC son autónomos del poder ejecutivo, por lo que Trump no tiene mandato para ordenarles esto. Si puede avanzar sobre la cuestión de los gastos que el Estado Federal realiza en derivar publicidad a través de esas plataformas y allí aparece un tema interesante a revisar: la pauta publicitaria y los fondos que van del sector público al privado en áreas de comunicación.

Más allá de esto, es indispensable analizar esta situación con el problema real sobre la mesa: En la puja entre Twitter y Trump, nadie está pensando en proteger la libertad de expresión de los usuarios que se encuentran regularmente con situaciones de asimetría en relación a la baja de contenidos, advertencias y suspensión de cuentas por diversos motivos (mayormente por violaciones a otra regulación norteamericana, la Digital Millenium Copyright Act - DMCA por su sigla en Inglés).

Las plataformas no son la esfera pública. Son una esfera privada que se ha convertido en un espacio indispensable del debate público, que moldean en función del modelo de negocios que cada una de ellas tenga y que generalmente se basa en la economía de la atención y la asignación de avisos publicitarios según perfiles.

Desde múltiples sectores se le viene pidiendo a las plataformas que ejerzan más y más ese control, ya sea para frenar el discurso violento, la discriminación, el acoso hacia las mujeres o las campañas de desinformación. Es en esa línea que las plataformas usan cada vez más las cláusulas de la CDA que las habilitan.

Atribuirles responsabilidad objetiva a las plataformas y eliminar la inmunidad de la que gozan sólo puede servir como incentivo a más controles y censura privada, ya que ninguna empresa podrá sostener un negocio en el cual deba hacerse cargo económicamente cada vez que un usuario vulnera un derecho, ofende a alguien o viola una regulación vigente en algún lugar del mundo. Esa estrategia no hará más que profundizar un problema que ya de por si es difícil de abordar.

Donde sí se puede tratar de arbitrar alguna medida es en la regulación de las pautas que habilitan a las plataformas a dar de baja discursos, expresiones, opiniones y participaciones de los usuarios, asegurando que nada de esto se realice sin debida notificación, de forma proporcional, con mecanismos de transparencia y defensa así como con extremos cuidados de no eliminar discurso que efectivamente esté protegido por los principios de libertad de expresión.

A la luz de cómo se ha desarrollado el debate, esta es una tensión en la que ni Twitter ni Trump parecen estar pensando. En este debate sobre las regulaciones de contenidos de las plataformas de Internet es hora de reclamar que cualquier decisión que se tome sea hecha en función del eslabón más débil de la cadena y en protección de esa esfera de comunicación en la que finalmente lo más importante somos nosotros, los usuarios.

Inteligencia ilegal. Por un Nunca Más de los sótanos de la democracia

VER EL NEWSLETTER COMPLETO

Como seguramente ya saben, tres integrantes de nuestra organización forman parte de la lista de más de 500 personas fichadas en el marco de la participación en eventos internacionales como la Ministerial de la OMC en 2017 y la reunión del G20 en 2018. Entre esas fichas aparecen nombres de periodistas, académicos/as y miembros de organizaciones de la sociedad civil que se acreditaron a alguno de estos dos eventos.

En primer lugar, queremos agradecer el apoyo de las personas e instituciones que manifestaron su solidaridad frente a la situación vivida. Hacemos lo propio con los y las colegas cuyas fichas aparecieron en la AFI y que gracias a la gestión de la intervención ya se encuentran en poder de la justicia. En ese sentido, planeamos darle seguimiento a la causa que instruye actualmente la fiscal Paloma Ochoa y que tramita ante el juzgado del Dr. Martinez De Giorgi.

Sin embargo, esta no es la única de las causas abiertas en las cuales queda en evidencia la actuación de los organismos de inteligencia. A diario vemos novedades que incluyen espionaje y seguimiento de integrantes de todas las fuerzas políticas y periodistas en el ejercicio de sus funciones que han sufrido vigilancia ilegal por parte de espías que reportaban al poder político. Hay todavía quienes relativizan esta situación con afirmaciones tales como que 'esto siempre fue así'. Es posible que con mayor o menor torpeza e impunidad, los servicios de inteligencia hayan sido sistemáticamente utilizados para intervenir en la vida política del país. También es conocida la alianza espuria de servicios de inteligencia, tribunales federales y un sector de periodismo siempre ávido de poner al aire noticias escandalosas, operaciones y escuchas ilegales. Reconocer la historia no puede jamás ser una forma de legitimarla, sino que es la base para decir Nunca Más.

La Iniciativa Ciudadana para el Control de los Sistemas de Inteligencia nació hace muchos años para dar cuenta de esta problemática que impacta de lleno en la democracia argentina. Es, sin dudas, la gran deuda que tenemos como país con el Estado de Derecho.

Más allá de la necesidad urgente de avanzar con las causas judiciales y exponer las responsabilidades políticas del más alto nivel en estas operatorias claramente ilegales, es indispensable dar un debate serio y profundo sobre los servicios de inteligencia en Argentina.

¿Para qué queremos un sistema de inteligencia? ¿Cuáles son las funciones propias de un sistema de inteligencia en democracia? ¿Qué rol cumple cada área de los sistemas de inteligencia en el Estado? ¿Cómo se establece un sistema efectivo de control y transparencia? ¿Cómo se establece un sistema de rendición de cuentas apropiados? ¿Cómo hacemos para sanear las operaciones espurias y reconvertir estos sistemas en algo realmente profesional y útil al sistema democrático en su conjunto y no a la fuerza política que ocasionalmente ocupe la casa de gobierno?

Son muchas las preguntas ante una oportunidad única en la cual Vía Libre va a participar activamente. Es hora de diseñar una reforma profunda y establecer mecanismos sólidos de control para que los sistemas de inteligencia sirvan al país y no sean usados para espiar a la ciudadanía.

Es clave además establecer pautas claras de limitación del secreto. Es inadmisible que la oficina de Acceso a la Información Pública a cargo de la protección de datos personales, la justicia ante la cual se interpusieron recursos de acceso a la información y habeas data y la bicameral de control de servicios de inteligencia fracasaran una tras otra en establecer límites a la AFI y en proteger los derechos de la ciudadanía ante la recopilación ilegal de información. Pautas estrictas de limitación de secreto y desclasificación de archivos deben ser parte de una nueva legislación que otorgue transparencia al sistema de inteligencia.

A su vez, es urgente que se establezcan mecanismos de control y transparencia más allá de la AFI, a todas las fuerzas de seguridad que tienen roles de investigación, para que se ajusten al debido proceso judicial y al Estado de Derecho.

Si bien la AFI hizo inteligencia ilegal que incluyó datos personales e información privada de cada una de las personas fichadas, no hay una diferencia tan grande entre el fichaje que se hizo de periodistas, académico/as e integrantes de la sociedad civil y las pautas de inteligencia de fuentes abiertas establecidas en el protocolo de ciberpatrullaje vigente. Son diversas áreas de una misma tendencia que es indispensable limitar y controlar a fin de garantizar a la ciudadanía su derecho a la intimidad, a pensar diferente, a organizarse y protestar y a expresarse en absoluta libertad.

Julio

Ciberpatrullaje: Se conformó la mesa consultiva de seguimiento del protocolo del Ministerio de Seguridad

VER EL NEWSLETTER COMPLETO

El 1 de Julio pasado se reunió por primera vez la Mesa Consultiva de seguimiento de las tareas que las fuerzas de seguridad federales realizan en el marco del protocolo de prevención del delito en fuentes abiertas (Resolución 144/2020). Desde Fundación Vía Libre, una vez más, queremos manifestar nuestro desacuerdo con la implementación de medidas de vigilancia en fuentes abiertas y la necesidad de ajustar las tareas al marco legal vigente.

Sin ánimo de reeditar una discusión semántica sobre si el patrullaje de redes sociales es o no inteligencia, son notables las características que nos llevan a reafirmar que este tipo de medidas no son asimilables a la recorrida que un oficial realiza en la esfera pública en prevención del delito y que esto tiene más que ver con la posibilidad de pararse a escuchar, tomar fotografías y hacer registros de información que, aún realizados en un ámbito de acceso público constituye una tarea de recopilación y análisis de información, es decir, una tarea de inteligencia y que por lo tanto debe ser instruida en el marco de una investigación judicial con pleno control jurisdiccional.

Dicho esto, y aún frente a nuestro desacuerdo con la medida, queremos destacar que el Ministerio de Seguridad conformó la mesa de seguimiento del protocolo con una convocatoria a diversas organizaciones de la Sociedad Civil entre las que se cuenta también Fundación Vía Libre junto a colegas como Ilsed, CELS, Amnistía Argentina, la Comisión Provincial por la Memoria y a la que ahora se han sumado además integrantes de la Oficina de Protección de datos personales de la Agencia de Acceso a la Información Pública. En la mesa participan también delegados del Poder Legislativo. El miércoles pasado estuvieron presentes en la reunión los diputados nacionales Cristian Ritondo (por el PRO) y Paula Penacca (Frente de Todos). Faltó la presencia de delegados del Senado Nacional que aún no fueron designados para este fin.

Varias cuestiones importantes que vale la pena compartir con ustedes en este espacio: En primer lugar, se mencionó con gran énfasis que el protocolo tiene fecha de prescripción y que no hay plan de mantener estas políticas más allá de la emergencia sanitaria de Covid 19. En este sentido, el protocolo está atado al Decreto que establece la emergencia sanitaria en su fecha de caducidad.

En segundo lugar, frente al interés de varios integrantes de la mesa en conocer casos específicos, el Ministerio prometió para la próxima reunión un informe de gestión que de cuenta de los casos en los cuales el protocolo fue puesto en acción en casos concretos. Desde ya, es importante recordar que desde las organizaciones de la Sociedad Civil exigimos explicaciones sobre el caso puntual de un periodista de la provincia de Chaco a quien se inició un expediente por la distribución en redes de una noticia falsa.

En tercer lugar, se nos informó que se está trabajando en un programa de formación para las fuerzas de seguridad orientado especialmente a una implementación del Protocolo 144/20 ajustado a derecho, que incluya sensibilización en el uso de redes sociales.

Por otro lado, también se debatió la problemática de las policías provinciales, ya que es preocupante el accionar de estas fuerzas que están por fuera de este protocolo. En ese sentido, el MinSeg indicó que mantuvieron diversas reuniones de trabajo con las fuerzas provinciales a las que se les presentó el protocolo y sus lineamientos fundamentales.

El tema que aún no tiene una respuesta clara y que una vez más preguntamos es la utilización de tecnologías para la tarea de patrullaje de redes sociales. Se nos indicó que en el marco de esta gestión no se realizó ninguna compra de sistemas dedicados a esto y que si se está utilizando alguna tecnología, la misma habría sido adquirida en la gestión anterior y se nos informará sobre el tema en las próximas reuniones. Es decir, no tenemos ninguna respuesta concreta sobre el uso o no de tecnologías para el monitoreo de redes sociales.

Finalmente, es importante mencionar que la presencia de legisladores en la mesa consultiva obedece además al interés en desarrollar legislación para regular esta práctica. Frente a cualquier iniciativa de este tipo, desde nuestra organización tenemos claro que lo que hace falta es una regulación protectora de los derechos de la ciudadanía que implemente de manera transversal y efectiva las garantías apropiadas para la defensa del derecho humano a la intimidad de las personas en todo el territorio nacional.

Una vez más, desde Vía Libre queremos dejar plenamente asentado que mantenemos nuestra posición crítica a esta política y que junto con las organizaciones de la sociedad civil con las que habitualmente trabajamos en estos temas no avalamos la práctica. Nuestra presencia en la mesa consultiva no constituye apoyo ni acuerdo alguno a esta iniciativa, aunque entendemos que es la mejor estrategia que podemos desarrollar para contribuir al conocimiento público de la problemática y aportar a que se realicen ajustes, mejoras y finalmente aportar a la construcción de un sistema de prevención del delito que no vulnere los derechos fundamentales a la privacidad, el debido proceso y que no socave el derecho a la libertad de expresión.

Desde este y otros espacios de comunicación de nuestra Fundación haremos los esfuerzos que estén a nuestro alcance para llevar las preocupaciones de la ciudadanía que nos acompaña en nuestro ideario a la mesa consultiva y al mismo tiempo divulgar y compartir públicamente los avances que se produzcan en el marco de la implementación del protocolo 144/2020 del Ministerio de Seguridad.

Identificación biométrica para exámenes en Universidades Nacionales: ¿Otra solución en busca de problemas?

VER EL NEWSLETTER COMPLETO

La pandemia de Covid19 sigue trayendo efectos colaterales además de las dramáticas situaciones sanitarias, económicas y sociales en la que cada país está tratando de sobrellevar una coyuntura de absoluta excepcionalidad que desafía a todos los sectores de la vida pública y privada. Uno de los efectos colaterales más notables es la adopción y legitimación pública de sistemas de vigilancia y control social cada vez más amplios e invasivos.

Los sistemas educativos sufren estos impactos de forma directa, con suspensión de actividades en todo nivel, con millones de niños, niñas y adolescentes fuera de las aulas en todo el mundo y con un sistema de educación superior que se encontró obligado a diseñar políticas de transformación digital en un contexto de incertidumbre y urgencia. En Argentina, a todo este contexto se suma una profunda crisis económica y la dificultad de llegar a todas las personas afectadas de forma equitativa.

En este contexto, las Universidades Nacionales se encontraron con panoramas disímiles a la hora de avanzar con la transformación digital no prevista. Con el correr de los meses y el alejamiento constante de cualquier certeza sobre las fechas de examen que deberían administrar en estos meses de Julio/Agosto, los centros académicos del país comenzaron a plantearse cómo evaluar a los y las estudiantes en la modalidad remota.

Fue la Universidad Nacional de Córdoba la primera en dar un paso en la contratación de Software para evaluaciones a la empresa privada Respondus, tras lo cual se generó un fuerte debate al interior de esa casa de estudios sobre las implicancias en términos de derechos de estudiantes y docentes.

Respondus es un sistema de reconocimiento facial que sirve a su vez como herramienta de control para

validar la identidad de los/as estudiantes en contexto de examen, pero a su vez se presenta como mecanismo para detectar e impedir el fraude en los exámenes. El sistema graba el rostro y el entorno de los estudiantes y procesa algorítmicamente las grabaciones para identificar potenciales 'conductas sospechosas.'

El sistema funciona exclusivamente en sistemas operativos Windows y OSX, no funciona en dispositivos móviles ni en computadoras o tabletas cuyo sistema operativo sea libre o diferente de los previstos. También requiere que la computadora donde se administra cuente con una cámara de buena definición para la evaluación.

Peor aún es el mecanismo que utiliza este software para su evaluación. Respondus utiliza un navegador web propio que bloquea la evaluación dentro de este entorno y obliga a cerrar cualquier otra aplicación que los estudiantes puedan tener abierta en paralelo. Además, utiliza un sistema que monitorea la actividad de sus usuarios en el momento del examen.

A esto se suma la promesa de detectar si el rostro de quien lo utiliza cambia durante el transcurso de la grabación, el sistema registra audio y sonido, que en el caso actual de Aislamiento Social Preventivo y Obligatorio implica la captura del contexto de hogar de los y las estudiantes, con todo lo que esto implica en términos de privacidad.

Respondus accede a información biométrica, rostro, cuerpo, rasgos, reacciones, gestos, hace seguimiento y construye - ¿aprende? - cómo identificar potenciales fraudes durante el examen.

Este sistema es privativo, nadie más que la empresa conoce cómo funciona, no se puede auditar, no cumple con las pautas apropiadas de protección de datos de las y los estudiantes y es seriamente invasivo de la privacidad de las personas. Además, fue adquirido para un fin que de una forma u otra rompe el contrato social del sistema educativo universitario: la confianza entre docentes y estudiantes.

Desde este espacio acompañamos a las organizaciones y personas que desde la Universidad Nacional de Córdoba están haciendo el esfuerzo de abrir una discusión seria sobre esta práctica típica del 'solucionismo' tecnológico que avanza en la compra de supuestas soluciones desproporcionadas para la tarea que se pretende realizar, abusivas en relación a los datos personales y la privacidad e innecesarias desde el punto de vista de la ética y el contrato social de nuestras universidades públicas.

En paralelo, y con implicancias serias también, el Consejo Interuniversitario Nacional (CIN) presentó un acuerdo de cooperación con el Renaper y el Ministerio del Interior para la incorporación de un sistema de reconocimiento facial para la identificación biométrica de los y las estudiantes en instancia de exámenes finales en las Universidades Nacionales.

Este sistema, a diferencia de Respondus, es provisto por el estado y trabaja sobre la base de datos del Renaper para validar identidad. Si bien este sistema no es invasivo como Respondus, es importante mencionar que los sistemas de reconocimiento facial siguen siendo problemáticos en términos de proporcionalidad y necesidad y que avanzar con tecnologías de este tipo sin un correcto análisis resguardo de la privacidad de las personas es un problema serio en el actual contexto en que aún no hay una política clara de protección de los activos digitales en poder del Estado Argentino.

Desde el año 2011, cuando la ex Presidenta Cristina Fernández de Kirchner realizó el lanzamiento del sistema SIBIOS, en Fundación Vía Libre venimos alertando sobre la necesidad de establecer mecanismos de evaluación serios sobre la necesidad y la custodia de los datos de la ciudadanía. Desde entonces, en todo el mundo, se han dado avances y retrocesos en la materia.

Los sistemas de reconocimiento facial están hoy en el centro de la escena en muchas democracias del mundo, en particular en Europa y especialmente en los EEUU donde se ha demostrado que estos sistemas refuerzan los estereotipos de la exclusión, amenazan los derechos civiles y socavan los principios de la defensa de la privacidad de las personas.

Una vez más observamos que aún con buenas intenciones, con la necesidad de dar una respuesta urgente a la crisis desatada por la pandemia de Covid19 y su severo impacto en el sistema educativo, las decisiones de políticas públicas priorizan la adopción de tecnologías sin apropiada evaluación de impacto y políticas de seguridad como si la incorporación de este tipo de sistemas fuera inocua.

Argentina se debe aún varios debates sobre estos temas. En principio, sobre la incorporación de tecnologías de vigilancia y su consecuente naturalización en diversas esferas de la vida pública como el sistema educativo. Y finalmente, una discusión sobre la debida protección y las políticas de seguridad de los activos digitales en manos del Estado Argentino. Ambos temas son centrales para la agenda de trabajo de Fundación Vía Libre, por lo que esperamos contribuir en ampliar y consolidar políticas públicas que requieren urgente discusión.

Agosto

La Agencia de Protección de Datos Personales recomienda suspender la práctica de 'Ciberpatrullaje'

VER EL NEWSLETTER COMPLETO

En la primera reunión de la mesa consultiva sobre el protocolo General para la Prevención Policial del Delito con uso de Fuentes Digitales Abiertas, conocido públicamente como protocolo de 'ciberpatrullaje', diversas organizaciones de la sociedad civil y especialistas invitados instamos al Ministerio a suspender la práctica hasta tanto se corrobore la necesidad, proporcionalidad y utilidad de la mentada actividad que se pretendía regular, a la vez que celebramos la derogación del protocolo vigente desde 2018 que había habilitado una serie de acciones contrarias a la libertad de expresión como el conocido caso de Javier Smaldone.

En ese encuentro realizado en la primera semana de julio de este año, la Agencia de Acceso a la Información Pública que tiene bajo su órbita el área de protección de datos personales prometió presentar un dictamen sobre el protocolo y la práctica de inteligencia de fuente abierta.

Merced a una solicitud de acceso a la información pública, desde la Fundación Vía Libre accedimos al dictamen sobre la adecuación del Protocolo realizada por la Agencia de Acceso a la Información Pública y remitido al Ministerio de Seguridad el 23 de Julio pasado.

El documento detallado aborda varios aspectos que deberían haber sido considerados antes de la puesta en marcha del protocolo y que merecen suma atención.

En primer lugar establecen la vinculación innegable del protocolo con la ley de protección de datos personales vigente en Argentina al expresar que "Dado que la finalidad del Protocolo es realizar tareas de prevención del delito en el espacio cibernético, y que para determinar si una persona cometió o no un delito las Fuerzas Policiales van a consultar, recolectar, ceder y/o almacenar información referida a la conducta de personas determinadas -es decir, datos personales-, no cabe duda que el Protocolo se encuentra sometido a la regulación de la Ley N° 25.326."

Hecha esa aclaración, cabe preguntarse entonces si cumple realmente con los mandatos de la norma vigente en Argentina. Veamos...

El segundo aspecto que evalúa el dictamen es la legalidad de la práctica como tal, que en principio no parece colisionar con la ley de protección de datos: "... en el caso objeto de análisis el MSG parecería realizar sus operaciones de tratamiento bajo las bases legales de los apartados (a) y (b) del artículo 5, inciso 2 la Ley No 25.326, que establecen, respectivamente, que "[n]o será necesario el consentimiento [del titular de los datos] cuando: a) Los datos se obtengan de fuentes de acceso público irrestricto; b) Se recaben para el ejercicio de funciones propias de los poderes del Estado o en virtud de una obligación legal".

Sin embargo, esto no habilita a que el MinSeg incumpla las demás obligaciones que surgen de la ley de protección de datos, especialmente el derecho de información, modificación, seguridad de la información, eliminación y todo lo que tiene que ver con el procesamiento de esos datos recolectados. En particular, no queda claro según el documento si entre los datos recolectados se incluye o no datos sensibles, cuya protección especial debe necesariamente ser garantizada por cualquier oficina pública.

En tercer lugar, el protocolo se establece para atender la situación excepcional de la crisis provocada por la

pandemia de Covid 19 y fija validez sólo por el período de vigencia del decreto de emergencia sanitaria. Sin embargo, a la hora de evaluar los delitos que se integran como potenciales justificaciones, buena parte de ellos carecen de relación directa con la situación sanitaria. "Esto pareciera indicar que la finalidad del tratamiento podría ser demasiado amplia, y debería restringirse únicamente a aquellos casos en los que una intrusión a la privacidad sea estrictamente necesaria para alcanzar el objetivo propuesto por el MSG. Por lo anteriormente expuesto,la AAIP estima que, en principio, la finalidad del Protocolo resulta muy amplia y por ello debería estudiarse su restricción."

'El artículo 4 del Protocolo (Procedimiento estandarizado y definición de indicadores delictivos) establece que a los fines de realizar las tareas de prevención "[…] la SECRETARÍA DE SEGURIDAD Y POLÍTICA CRIMINAL dispondrá el procedimiento estandarizado y la definición de los indicadores delictivos que orientarán la actividad preventora de los cuerpos policiales y fuerzas de seguridad en el marco de la política criminal del MINISTERIO DE SEGURIDAD durante la emergencia pública en materia sanitaria […]".' Los y las integrantes de la Mesa Consultiva de seguimiento todavía no tenemos ninguna noticia sobre la definición de los indicadores delictivos que orienten la actividad.

Hacemos nuestro el pertinente reclamo de la AAIP en el sentido de que "el Protocolo no especifica cómo las tareas de prevención realizadas por el MSG funcionarán en la práctica; ni en particular (i) que categorías de datos se recolectarán, (ii) cómo se asegurará que la información recopilada sea fiable, y (iii) qué consecuencias tendrá el tratamiento de los datos para sus titulares."

El principio de información al titular de los datos es clave para el real cumplimiento de la normativa. En este sentido, hay una seria falencia en el protocolo ya que más allá de la legalidad y justificación del tratamiento, falla a la hora de cumplir debidamente el artículo 6 de la ley 25.326 que manda proveer información al titular de los datos para que este pueda ejercer plenamente sus derechos de acceso, rectificación, supresión y la posibilidad de iniciar un reclamo administrativo en caso de corresponder. Entonces, la AAIP expresa que "Protocolo deberá prever de qué manera el MSG informará a la ciudadanía sobre el tratamiento de sus datos, y en particular, a través de qué medios podrán ejercer sus derechos."

Por otro lado, es indispensable que el protocolo clarifique la situación relacionada con la retención y destrucción de los datos que no cumplan con una finalidad establecida. En este caso, el documento del MinSeg establece el principio de destrucción del material 'prevenido no judicializado', pero no aclara cuál es el plazo para esta revisión, no establece ningún programa de revisión periódica para evaluar la pertinencia y necesidad de los datos ni por cuánto tiempo serán almacenados. Esa es otra demanda muy pertinente de la oficina de protección de datos.

Un tema aparte es la posibilidad de que los datos sean recolectados y procesados mediante la utilización de algún tipo de sistema automatizado de tratamiento de esos datos. La autoridad de aplicación de la norma de protección de datos en argentina ya se ha expedido sobre el particular en su Resolución AAIP N° 4/2019 al establecer que "en caso que el responsable de la base de datos tome decisiones basadas únicamente en el tratamiento automatizado de datos que le produzcan al titular de los datos efectos jurídicos perniciosos o lo afecten significativamente de forma negativa, el titular de los datos tendrá derecho a solicitar al responsable de la base de datos una explicación sobre la lógica aplicada en aquella decisión, de conformidad con el artículo 15, inciso 1 de la Ley No 25.326."

Y aquí llegamos a otro punto seriamente conflictivo del protocolo y la política del MinSeg. En todas las reuniones, en todos los documentos presentados a las autoridades, desde Fundación Vía Libre repetimos la pregunta sobre qué tecnologías está utilizando el Ministerio de Seguridad para ejercer la tarea de ciberpatrullaje. Nunca recibimos respuestas apropiadas, salvo la promesa de una respuesta en la próxima reunión prevista para el 1 de septiembre del corriente año. No hay tampoco información apropiada sobre las medidas de salvaguarda de la información recolectada, ninguna evaluación de impacto ni un plan de seguridad de la información recolectada.

Desde Vía Libre compartimos la preocupación de la AAIP y hacemos nuestra la recomendación de que se suspenda la aplicación de las tareas de prevención del delito con uso de Fuentes Digitales Abiertas hasta tanto se clarifiquen y cumplan debidamente los principios establecidos en el marco de la Ley de Protección de datos personales vigente en todo el territorio nacional.

Algunos apuntes preliminares sobre la acción judicial de CFK contra Google

VER EL NEWSLETTER COMPLETO

Como seguramente ya saben, la Vicepresidenta de la Nación Cristina Fernández de Kirchner inició una acción judicial para poner sobre la mesa la responsabilidad que la empresa Google tiene (o no) en la publicación de un contenido que, en el ordenamiento jurídico argentino podría ser definido como una calumnia.

¿Qué dice la ley sobre las calumnias? "Calumniar es acusar a otro falsamente de haber cometido un delito. No será delito si los dichos guardan relación con un asunto de interés público". (Fuente: Código Penal)

El caso reviste enorme importancia por diversos motivos. En primer lugar, porque llega a poner sobre la mesa uno de los temas que se vienen discutiendo desde hace años en Argentina y que, más allá de algunos casos judiciales como Taringa (Fuero penal, con fallo favorable a Taringa) y Rodriguez c/ Google y Yahoo (Civil, con fallo de CSJN favorable a Google) no tiene un correlato en la legislación vigente, al menos en la cuestión de responsabilidad de intermediarios. Si algo queda en claro a partir de estos casos, y esto es un consenso entre la comunidad académica que estudia estos temas, es que el asunto tiene vínculo directo e ineludible con la doctrina de libertad de expresión.

En segundo lugar, es importante distinguir que, si bien Google se ampara en la declaración de que su sistema es un algoritmo que ordena y presenta información producida por terceros, en el caso de referencia, el punto de conflicto no es estrictamente el resultado del buscador sino lo que se denomina Caja de Conocimiento (un espacio entre los resultados de las búsquedas que apunta a sintetizar para facilitar el acceso a información rápida sobre el tópico que se indaga). La cuestión aquí es cómo y con qué criterios se arma esa caja de conocimiento que se destaca en los resultados que arroja el buscador.

Vamos a revisar paso a paso qué pasó y qué podemos esperar de esta acción judicial.

El 17 de mayo de 2020, ante la búsqueda de Cristina Fernández de Kirchner en el sistema, la caja de conocimiento presentaba su perfil con el cargo de "Ladrona de la Nación Argentina" en lugar del correspondiente Vice Presidenta de la Nación Argentina. En ese caso, la fuente de la cual Google toma el dato es Wikidata (uno de los diversos proyectos de la Fundación Wikimedia, que sostiene y administra la enciclopedia Wikipedia). Wikidata es un proyecto de datos abiertos, que así como sus proyectos hermanos, tiene la característica de que cualquier persona puede editarlo y volcar y modificar información allí. De hecho, como funciona como cualquier wiki, es posible hoy reconstruir el periplo del vandalismo.

Pocos meses después, la presentación de CFK apunta a dos cuestiones clave: La primera, a solicitar una pericia sobre los servidores de Google (Argentina e Internacional) para que indiquen cómo se construye ese resultado (tema aparte, esto seguramente dará lugar a algún pleito de propiedad intelectual) y cuánto tiempo, cuántas visualizaciones y por lo tanto, qué impacto público tuvo la instalación del vandalismo en la caja de conocimientos. En este caso, se trata de evaluar el potencial daño de la publicación supuestamente injuriosa (digo supuestamente, porque una injuria debe ser intencional, y resta probar si hubo intención de Google de cometer esta injuria).

Vale mencionar también que la causa iniciada por CFK no es penal, sino civil. Busca saber cómo se construyen los resultados de las búsquedas, evaluar el potencial daño y en consecuencia recibir una reparación pecuniaria por daños contra su honra y reputación.

¿Qué plantea el escrito presentado por los abogados de CFK?

Acá entramos en un tema de gran complejidad, porque el escrito no utiliza la doctrina de responsabilidad de intermediarios sino la ley de defensa del consumidor, según la cual, Google no habría cumplido con el debido servicio a su usuaria CFK. En este sentido, más allá de la estrategia judicial de utilizar una norma que deja en cabeza de la empresa probar que hizo todo lo que diligentemente debía hacer y protege especialmente al consumidor, será difícil probar que el contrato de adhesión de usuarios finales incluya la obligación de velar por lo que terceros opinan y publican sobre una persona. Nada de eso se incluye en la ley de defensa del consumidor.

El otro marco regulatorio al que apela la demanda es el marco civil de daños y la obligación de contener la pobibilidad de que esto ocurra. Ir en este sentido obligaría a revisar la sentencia de Rodriguez c/ Google que consagró, en defensa de la libertad de expresión, que el buscador no tiene obligación de monitorear y controlar lo que otros publican.

Dirán entonces que Google es autor (tal como expresó el abogado de CFK en diversas notas de prensa). Si Google es el autor de la calumnia entonces no tiene ningún sentido ponerse a discutir sobre responsabilidad de intermediarios (si es autor no es intermediario) o defensa del consumidor. Es un caso simple y llano de calumnias e injurias. En este sentido, si esto es así, habrá que aplicar la doctrina habitual de calumnias e injurias y recordar que los y las personas en la función pública gozan de menores niveles de protección que las personas de a pie por lo que la demanda no parece que tenga posibilidad de prosperar.

Más allá de esto, que podría resolverse dentro de muchos años, el caso pone ante la mirada pública un tema central en relación a la protección de la libertad de expresión y la responsabilidad de las plataformas de redes sociales donde esos derechos se ejercen en un ambiente controlado por un sector privado hiperconcentrado y bajo sus reglas.

Una buena consecuencia de este caso sería, a mi modo de ver, la posibilidad de exigir y conseguir mayor transparencia sobre la edición que las plataformas hacen a la hora de mostrar resultados, sugerir enlaces y presentar contenidos a sus usuarios. Si hay algo que debemos tratar de conseguir es más y mejores recursos para proteger la libertad de expresión en estos entornos de los cuales depende buena parte de la esfera pública hoy.
Una consecuencia indeseable sería que se establezca responsabilidad objetiva sobre las empresas, lo que implicaría un daño concreto a la libertad de expresión de sus usuarios, ya que si las plataformas son responsables actuarán de forma preventiva dando de baja contenidos de forma sistemática para evitar nuevas demandas. Si esta opción es la que prospera, habrá que ver qué decisión toma la empresa: editar y controlar todo lo que se difunde o su contracara, la única opción que la dejaría en el puerto seguro de no tener responsabilidad: no intervenir en la circulación de cualquier cosa, no priorizar ni ejercer moderación, sin algoritmos que administren y sin eliminación de contenidos potencialmente dañosos, es decir, habrá que acostumbrarse al todo vale y dejar de pedir intervención de las empresas para controlar discursos indeseables.

Si se concluye que hay responsabilidad editorial, habrá que ver cómo se resuelve una causa de este tipo ya que pondría a una firma como Google en el mismo marco legal que cualquier medio de comunicación con responsabilidad sobre lo que publica. Si prima este criterio, por qué no iría luego la funcionaria contra otros medios de comunicación que publican a diario acusaciones y adjetivos de mucho peor tenor, incluyendo diarios, programas televisivos, revistas y cualquier otro medio con responsabilidad editorial. No lo hace, porque es claro que eso constituiría un ataque a la libertad de expresión.

Veremos, con el correr de los días, hacía dónde va esta demanda. Mientras tanto, seguiremos debatiendo con la libertad de expresión como valor a defender, en particular en temas de interés público como este.

Hacia una política pública de protección de activos digitales en Argentina

VER EL NEWSLETTER COMPLETO

Hace pocos días circuló una noticia de esas que tienen muy bajo impacto en los medios de comunicación y que le interesa a un pequeño sector de 'nerds' de la seguridad y la privacidad. Una base de datos con el registro de más de 115.000 argentinos que aplicaron para permisos de circulación en el contexto del Aislamiento Social Preventivo y Obligatorio (ASPO) fue expuesta en la web sin ningún tipo de seguridad, clave o mecanismo de autenticación de acceso. Los datos filtrados incluían nombres, DNI, identificación tributaria así como las razones por la cual estaban solicitando el permiso de circulación. Como es lógico, los trabajadores esenciales fueron los más expuestos, aunque también quedaron a la vista los permisos excepcionales. La base de datos expuesta pertenece a la Provincia de San Juan y el Ministerio de Salud de la Nación.

La base desprotegida de esta forma fue detectada por el investigador de seguridad Bob Diachenko de Comparitech el 25 de Julio pasado. De inmediato, el investigador alertó al Ministerio de Salud de La Nación. La cronología de los sucesos sería desopilante si no fuera dramática. La base de datos fue indexada el 12 de Julio, el 25 fue hallada por Diachenko, quien inmediatamente dio la alerta a los responsables de la base. El 28 de Julio, la base de datos fue dada de baja, pero luego fue puesta en línea nuevamente sin explicación ni cuidados. El investigador envió otra alerta, esta vez a la autoridad de ciberseguridad de la nación, quienes inmediatamente respondieron con un reconocimiento del incidente y con una comunicación a los responsables. El 29 de Julio, la base de datos fue dada de baja nuevamente.

La base filtrada contenía registros de 115.271 argentinos con datos tales como género, DNI y CUIT, fecha de nacimiento, fotografía, dirección de correo electrónico, número telefónico, correo electrónico laboral y en más de 33000 casos la copia del permiso de circulación solicitado, incluyendo datos de empleador, lugar, teléfono, el tipo de negocio a los que el solicitante puede ir, si es personal médico o no, entre mucha otra información privada administrada en la base de datos del Gobierno de San Juan.

Este es uno de tantos casos de negligencia en la administración de bases de datos y activos digitales en poder del Estado. Es un caso más en el que queda de manifiesto la falta de una política integral de protección de activos digitales que el Estado debe custodiar de manera apropiada y con máximos niveles de responsabilidad.

La construcción de esa política de protección de activos digitales es una de las tareas más complejas y desafiantes de este presente. Requiere compromiso no sólo de la sociedad civil involucrada, la comunidad de seguridad de la información (Infosec) sino y muy especialmente un trabajo sostenido de la Administración Pública Nacional, que pueda construir una política de Estado que trascienda las gestiones de gobierno.

La definición de esas políticas debe ser liderada por el área de ciberseguridad que en el actual organigrama del Estado depende de la Secretaría de Innovación Pública, pero debe tener la capacidad de ejercer un mandato férreo sobre todas las oficinas del Estado que construyen y administran bases de datos con información que los y las ciudadanas debemos proporcionar a las diferentes oficinas públicas para el cumplimiento de su misión. Se trata no sólo de tener una política en los papeles, sino de tener la capacidad de que esa política sea apropiada y respetada por todas las instancias del Estado, incluyendo en un país federal como el nuestro, por los responsables de bases de datos en las administraciones provinciales y municipales de todo el país.

La filtración de datos que abre esta columna no es la primera ni será la última, pero la tomamos como ejemplo para dar cuenta de un fenómeno que pasa prácticamente inadvertido para la ciudadanía y del cual las administraciones públicas no se hacen cargo. Es más, lo más habitual en nuestro país es que las cuestiones vinculadas con la 'ciberseguridad' tengan una impronta más punitiva que preventiva, más policial que de seguridad informática, más orientada a reportar y denunciar culpables (con la consiguiente persecución penal asociada) que en generar cadenas de responsabilidades sobre los y las funcionarias a cargo de gestionar los datos de la ciudadanía.

Cada tanto se genera una noticia policial (como el sonado caso de La Gorra Leaks) en el cual la prensa experta en policiales da voz a la versión oficial que suele buscar culpables afuera para tapar así sus propias responsabilidades en la administración de un bien bajo su custodia, pero que no les pertenece: la información de la ciudadanía. El caso La Gorra es emblemático, porque reúne todos los condimentos del horror: Autoridades políticas de seguridad y fuerzas federales absolutamente negligentes con información sensible, una filtración de datos de policías en terreno, sus familias, datos de testigos, escuchas telefónicas, denuncias, etc filtradas por la desidia irresponsable de quienes no son capaces de resguardar su propia seguridad de la información, ataque a la comunidad de Infosec que dio cuenta del incidente y finalmente la apertura de causas penales armadas contra quienes de forma atinada explicaron lo sucedido y dejaron al descubierto la propia torpeza de los funcionarios involucrados.

Amenazar a los practicantes de la seguridad de la información con artilugios penales nunca puede ser una salida a los problemas de seguridad.

Desde hace muchos años en Fundación Vía Libre venimos trabajando con la comunidad de Infosec para alertar sobre la problemática de la seguridad de la información, sobre los riesgos y amenazas de construir una doctrina puramente penal y punitiva, sobre la pésima influencia de ciertos sectores proclives a firmar cualquier lineamiento de 'ciberseguridad' y 'cibercrimen' que baje de organismos internacionales sin escuchar ni atender debidamente la voz de la comunidad de Infosec local, que es sólida, variada y rica en talentos y experiencia.

Infinidad de veces dijimos que la seguridad de la información no depende de la creación de más tipos penales, y que en buena medida no tener un protocolo de acción es la causa fundamental de este tipo de filtraciones. Infinidad de veces tratamos de establecer el principio precautorio sobre los datos recopilados por las Administraciones Públicas de todo nivel, con magro éxito.

Esa manía de extraer datos para casi cualquier cosa, sin análisis de legalidad, necesidad y proporcionalidad y sin evaluación de amenazas y riesgos de las bases de datos nos ha dejado en una situación en la cual los ciudadanos podemos tomar todos los recaudos con nuestros datos, pero es el propio Estado el que toma a la ligera la seguridad de esa información que, insisto, no les pertenece y tiene obligación de custodiar.

El caso de San Juan nos sirve una vez más para advertir que sin una política de seguridad y protección de los activos digitales en poder del Estado Argentino, no hay reforma penal, inclusión de cibercrímenes de toda índole o firma de tratados internacionales como el convenio de Budapest que sirva para lidiar con una situación histórica de negligencia y desidia de quienes deben asegurar el respeto por la privacidad de la ciudadanía.

Es indispensable dotar a la oficina de Ciberseguridad de las capacidades técnicas, humanas, presupuestarias e institucionales que le permitan diseñar, promover y hacer cumplir un protocolo apropiado para la protección de los activos digitales en manos del Estado. A medida que el Estado avanza en la conformación de bases de datos de todo tipo y en todo nivel, esta necesidad se vuelve más urgente.

Desde Fundación Vía Libre estamos dispuestos a trabajar codo a codo con las autoridades a cargo del área y con la comunidad de Infosec para cumplir este objetivo que debería ser central para construir una política pública apropiada que proteja la seguridad de los activos del Estado y especialmente los datos de la ciudadanía que tiene pleno derecho a reivindicar una garantía mínima para su privacidad.

Un indispensable debate sobre los servicios de telefonía e Internet en Argentina

VER EL NEWSLETTER COMPLETO

La noche del viernes se caracterizó por la sorpresa generada por la serie de Tweets del Presidente de la Nación en los que explicaba la resolución emitida mediante el Decreto 690/2020 que declara los servicios TIC como servicio público en competencia. Es sabido que el contexto de pandemia puso sobre la mesa una situación de profunda inequidad en el acceso a tecnologías de información y comunicación que se tornan hoy indispensables para el pleno ejercicio de derechos fundamentales entre los que se destacan no sólo la libertad de expresión y de acceso a la información, sino en esta coyuntura el derecho esencial a la educación y al trabajo.

Es importante mencionar que no compartimos la metodología del DNU para tramitar un tema tan complejo como la regulación de Telecomunicaciónes, sin embargo comprendemos no sólo el apremio sino además la dificultad que plantea un tema como este a la hora de construir consensos. Las telecomunicaciones son un terreno de ardua disputa de intereses, con jugadores poderosos de la construcción de opinión pública, que lamentablemente lleva años de discusión sin que Argentina pueda darse una regulación de telecomunicaciones moderna y apropiada para subsanar los históricos problemas de costos, calidad de servicios y concentración que arrastramos hace décadas.

El decreto no trae grandes novedades, sino que repone algunas previsiones que habían sido incorporadas originalmente en la Ley Argentina Digital, sancionada en 2014, modificada por el ex Presidente Mauricio Macri como una de sus primeras medidas de gobierno. Tan crucial es el tema, que Macri dedicó a esta cuestión el decreto 267/2015, a muy pocas horas de asumir la presidencia.

Como ya mencionaron varios académicos durante el fin de semana, la declaración de servicio público para la telefonía móvil y los denominados servicios TIC implica una consagración del derecho fundamental a comunicar, razón por la cual en su momento, la propia CIDH intervino para instar a la gestión anterior a reponer los derechos adquiridos por la ciudadanía y borrados de un plumazo con el decreto 267.

Argentina no sólo tiene un servicio de Internet deficiente y caro, sino y especialmente, concentrado y extremadamente desigual.

Esta iniciativa, que debería ser tratada pronto en el Congreso, repone parte de esos aspectos, y en particular recupera para el Estado ciertas potestades regulatorias propias de un sistema de servicio público, que valga la aclaración, dista mucho de ser una estatización o una toma de control público de las empresas privadas (como algunos sectores trataron de hacer creer al público incauto durante el fin de semana).

El flamante DNU establece que los servicios TIC son servicios públicos esenciales y estratégicos en competencia. Esto significa que las empresas licenciatarias pueden fijar precios "justos y razonables que deberán cubrir los costos de la explotación, tender a la prestación eficiente y a un margen razonable de operación", pero que la autoridad de aplicación tendrá un rol clave a la hora de regularlos.

Los servicios de telefonía móvil serán a partir de ahora servicios públicos bajo la regulación de ENACOM. Muchos legisladores de diversa extracción política venían presentando proyectos en ese sentido, ya que la telefonía fija es servicio público desde la privatización de Entel en la década del 90. No parece haber justificación para diferenciar los servicios móviles de la regulacion general de la telefonía.

Más allá de nuestro acuerdo general con el espíritu del decreto, desde Vía Libre entendemos que las regulaciones de telecomunicaciones requieren un debate amplio y consensos sólidos que permitan construir servicios públicos a la altura de la importancia que este sector tiene para el pleno ejercicio de derechos de la ciudadanía.

En el año 2014, frente al Senado Nacional, sostuvimos la indispensable necesidad de actualizar el marco regulatorio de las Telecomunicaciones en Argentina. En aquel entonces, y mientras se debatía el proyecto de Argentina Digital fuimos enfáticos en la necesidad de tener una regulación ajustada a la importancia del campo, alejada de cualquier doctrina de la seguridad nacional como la imperante en la vieja ley de 1972, cuando los servicios móviles y de Internet estaban todavía muy lejos de llegar a la ciudadanía.

El debate de Argentina Digital constituyó una oportunidad importante para dar ese debate, pero la ley resultante estaba plagada de inexactitudes y problemas que todavía se arrastran. La difusa definición de Servicios TIC hace que hoy, por ejemplo, nadie tenga del todo claro si la TV paga o la TV satelital están incluidas como servicio público en competencia o no. También queda de manifiesto el problema severo de mezclar en una misma ley la regulación de infraestructura y la regulación de contenidos. Los servicios TIC no son sólo los servicios móviles y de Internet, un sin fin de aplicaciones y otros servicios aparecen asociados a esa figura y regulados de la misma forma que las grandes empresas de telecomunicaciones.

Al igual que en 2014 hacemos nuestra la intención de consagrar como servicio público estos servicios esenciales para el pleno ejercicio de otros derechos, la necesidad de garantizar servicios asequibles a toda la ciudadanía, la urgente aplicación de una política que potencie y mejore el alcance de la conectividad a todos los sectores, especialmente los más relegados social, económica y geográficamente.

Finalmente, vamos a repetir exactamente lo que dijimos en 2014 en ocasión del debate sobre Argentina Digital, una ley que junto a la Ley de Servicios de Comunicación Audiovisual fue desguazada por Decreto por la gestión de Mauricio Macri en un clarísimo retroceso de una situación que estaba lejos de ser la ideal para la ciudadanía de Argentina.

El DNU emitido este viernes, firmado por todo el gabinete nacional, demuestra que la política de telecomunicaciones no es ajena al interés de esta gestión. Sin embargo, es fundamental la planificación de una política pública que no sólo se construya en consensos sino que sea resiliente más allá de las diferentes administraciones.

Persisten aún problemas heredados de Argentina Digital: Una autoridad de aplicación con un nivel de discrecionalidad alto que da lugar a los vaivenes de los que hemos sido testigos en los últimos años, una ausencia total de autoridades de control independiente, profesional, colegiada, un contexto de alta concentración de prestadores de servicios, con una integración vertical y un poder de mercado que impacta en forma sistemática en todos los aspectos, incluyendo no sólo los derechos del consumidor sino en libertad de expresión y derecho de la competencia.

Finalmente, el Decreto viene a reponer los magros avances obtenidos en la ley de 2014 y vuelve a echar luz sobre la necesidad de que nuestro país pueda dotarse de una regulación de telecomunicaciones moderna, garante de derechos, promotora de la competencia y la innovación y fundamentalmente apropiada para los tiempos que corren.

Septiembre

La geopolítica de Tik Tok. ¿Hacia dónde van las políticas de Internet?

VER EL NEWSLETTER COMPLETO

Hace varias semanas que venimos pensando en compartir algunas ideas e impresiones sobre la escalada de Donald Trump contra Tik Tok y WeChat y las tecnológicas chinas en general. Esto se enmarca en un contexto más amplio que se divulgó hace pocos días y que constituye una iniciativa que promete tener un impacto serio en la regulación / funcionamiento de Internet tal como la conocemos hoy.

Hace muy pocas semanas, Donald Trump y su Secretario de Estado Mike Pompeo presentaron el programa "The Clean Network" o "La Red Limpia" por su traducción al español.

Se trata, según Pompeo, de un abordaje amplio para custodiar la privacidad de los ciudadanos de los EEUU y la información sensible y confidencial de las compañías de ese país de las intrusiones "agresivas de actores maliciosos" tales como (op cit) el Partido Comunista Chino (CCP). Pompeo anunció el lanzamiento de cinco líneas de acción para proteger las telecomunicaciones críticas y las infraestructuras tecnológicas de los EEUU:

Carriers limpios: para asegurar que ningún carrier chino se conecte con las redes de telecomunicaciones de los EEUU.

Tiendas limpias: para remover aplicaciones no confiables de los proveedores de servicios de los EEUU (aquí se incluye el proyecto impedir la descarga de Tik Tok y WeChat desde las tiendas de las compañías norteamericanas).

Apps limpias: para evitar que proveedores de teléfonos chinos traigan pre instaladas o permitan la instalación de apps de empresas norteamericanas a las que se fuerza así a no hacer negocios con proveedores de origen chino.

Nube limpia: para evitar que la información de los ciudadanos norteamericanos y la propiedad intelectual de las compañías de ese país, incluyendo información sobre tratamientos y vacunas de Covid19 sean sustraídas o accedidas por adversarios que mantienen servicios en la nube (incluyen aquí a empañías como Alibaba, Baidu o Tencent).

Cables limpios: para asegurar que los cables submarinos que conectan EEUU con el resto del mundo no sean interceptados por los servicios de inteligencia del Partido Comunista Chino a gran escala.
Según el funcionario de la Administración Trump, más de 30 países y territorios y las principales empresas de telecomunicaciones del mundo asumieron el compromiso de hacer negocios exclusivamente usando proveedores confiables en sus redes limpias.

En una rápida reacción al anuncio, el académico Milton Muller expresó su repudio a tales medidas, indicando que usar las leyes de emergencia y de seguridad nacional para este tipo de cuestiones no sólo es desproporcionado, sino que va a redundar en problemas muy serios para las propias compañías norteamericanas que se supone busca proteger.

Estas medidas tiran por tierra la larga doctrina de libre comercio de la cual EEUU se ha beneficiado por décadas. Calificar a las empresas chinas como una amenaza a la seguridad nacional no es otra cosa que evitar cualquier control legislativo que pueda haber sobre las medidas y establecer de facto un sistema proteccionista que además, pretende imponer a sus países aliados.

En este sentido, la declaración de Trump sobre Tik Tok y WeChat al momento de emitir las sendas órdenes ejecutivas que interpuso para prohibir su utilización en territorio norteamericano a menos que sean compradas por capitales locales contiene un nivel de cinismo que ya no sorprende. Todos los actos de los que acusa a estas compañías son exactamente los mismos que sabemos que pueden hacer las empresas de los EEUU.

Richard Hill, experto internacional en telecomunicaciones, consultor de la UIT e integrante colega de varias redes como JustNet Coalition y Our World is Not For Sale se preguntaba en estos días si la política de Trump no constituye una puerta a que los países que no sigan al pie de la letra los mandatos de los EEUU empiecen a aplicar esos mismos parámetros hacia las compañías de los EEUU.

Actualmente, es importante recordar que el gobierno de los EEUU puede, con orden judicial, acceder a la información personal de sus ciudadanos procesada por las compañías bajo su marco legal, aunque sus datacenters se encuentren fuera del país (Cloud Act). Además, pueden acceder sin orden judicial, a los datos de ciudadanos extranjeros residentes en cualquier lugar del mundo.

El camino adoptado por la administración Trump no deja mucho margen de acción a los países que decidan de manera soberana no alinearse con ellos en este intento de polarizar cada vez más las relaciones internacionales. Recordemos además que hace pocas semanas, la Corte de Justicia Europea declaró inválido el EU-US Privacy Shield porque consideró que la ley norteamericana no es compatible con los derechos fundamentales consagrados en la UE al no proveer adecuada protección a los datos personales de sus ciudadanos. ¿Qué hará Europa frente a este panorama? Probablemente, esperar a ver el resultado de las elecciones de Noviembre en los EEUU.

La escalada de Trump contra las empresas del gigante asiático abre un período que bien podríamos caracterizar con aquella milenaria maldición china: 'Ojalá vivas tiempos interesantes".

Países periféricos con poca capacidad de acción en relación a la agenda de Internet Governance en particular o de Comercio Internacional en general no podemos perder de vista estos escenarios de la geopolítica que marcan tendencias, rumbos y requieren de estrategias apropiadas para su abordaje. Leer lo que ocurre a nivel internacional es clave en esta coyuntura en la que la polarización creciente no es sólo un tema de la política doméstica sino de las relaciones internacionales en general.

Estos temas de política internacional no están aislados de otros que están ocurriendo hoy mismo como la elección del próximo presidente del Banco Interamericano de Desarrollo (BID) o las negociaciones de la agenda de comercio de la OMC. La política de Trump para la 'Red Limpia' constituye un problema serio para la política global y la posibilidad de construir una gestión más amplia y democrática de Internet, gestión en la cual nuestra región está sistemáticamente ausente. Esto no es casual. No sólo se trata de construir las capacidades para incidir en un mundo de gran complejidad, sino y muy especialmente, de tener una política de estado definida para temas centrales como la gestión y regulación de Internet, agenda en la cual Argentina ha tenido más vaivenes que objetivos claros.

¿Quién está analizando esto en Argentina hoy?
En la agenda local no sólo deberíamos incluir los debates sobre la responsabilidad de los intermediarios que tanta repercusión generan sino también discusiones clave sobre aspectos centrales vinculados a la propiedad intelectual, formar capacidades para incidir en la esfera técnica de las regulaciones como la IETF (donde tienen lugar buena parte de los entredichos de la política internacional bajo un oscuro velo de jerga técnica), trabajar en la construcción y tendido de infraestructura apropiada, actualizar la regulación de protección de datos y privacidad, promover las capacidades locales para la innovación así como adoptar políticas de larga data de apoyo al desarrollo de software libre.

Históricamente, el rol argentino en las discusiones globales sobre políticas de internet ha sido de magro a nulo. Quizás sea hora de construir un foro para pensar qué políticas de internet necesitamos, qué regulaciones vamos a diseñar, qué alianzas vamos a tejer y qué objetivos nos vamos a dar en un contexto en el que no deberíamos caer en la polarización creciente, sino en el que vamos a tener que articular acciones que nos permitan construir y consolidar políticas de Internet que cumplan plenamente con los Derechos Humanos.

Historia clínica digital: ¿Por qué no?

VER EL NEWSLETTER COMPLETO

La semana pasada, las comisiones de Salud y Sistemas, Medios de Comunicación y Libertad de Expresión dieron dictamen conjunto favorable a un **proyecto de creación de una Historia Clínica Digital** para toda la población argentina.

El dictamen reúne proyectos previos presentados por los senadores Roberto Basualdo, Silvia García Larraburu, Silvia Elías de Perez, Antonio Rodas y Maurice Closs en un dictamen conjunto que recomiendan acompañar y aprobar en el recinto bajo el título de "Programa federal único de informatización y digitalización de historias clínicas de la República Argentina", cuyo artículo 1 establece la creación del programa en forma progresiva para la conformación de un sistema único de historias clínicas electrónicas.

En primer lugar, no queda claro que los autores del proyecto hayan hecho un análisis apropiado que ponga en tensión los supuestos beneficios y objetivos del proyecto frente a los riesgos y complejidades que se abren en esta potencial 'solución'. Una vez más, como tantas veces, vemos buenas intenciones para establecer un sistema que puede tener alguna utilidad, sin sopesar los problemas graves que se pueden generar a partir de su implementación.

Nos recuerda a los viejos debates que hemos dado y seguiremos dando sobre voto electrónico: creer que si pongo tecnología soluciono algo sin prever absolutamente nada de las complejidades que se abren y las voces de alerta que necesariamente se deben atender. Una vez más, el solucionismo tecnológico en su más pura expresión.

En primer lugar, ningún especialista en seguridad de los sistemas de información fue convocado a participar de la redacción y debate de la medida que se propone implementar. Por lo que pudimos seguir del debate realizado en forma remota, no se ha presentado ninguna evaluación de impacto ni de potenciales riesgos derivados de la creación de una base de datos centralizada de esta magnitud.

En segundo lugar, si bien el texto del dictamen es explícito al decir que se debe respetar el marco legal de la regulación de protección de datos personales (Ley 25.326) no parece tener la debida adecuación a esa norma. Esa ley es especialmente protectora de los datos de salud, considerados datos sensibles que requieren consideraciones mucho más rigurosas que el resto de los datos personales.

En tercer lugar, el dictamen aprobado establece la obligatoriedad de la integración a la base de datos, con lo que borra de un plumazo uno de los derechos fundamentales de la ley de protección de datos personales vigente a la fecha, el derecho a ser eliminado de una base de datos. El proyecto reconoce que el paciente es titular de los datos y que tiene derecho a conocer la información en su Historia Clínica Electrónica. Pero ante esta obligación impone luego un salto al vacío del pensamiento mágico: 'El almacenamiento, actualización y uso se efectúa en estrictas condiciones de seguridad, integridad, autenticidad, confiabilidad, exactitud, inteligibilidad, conservación, disponibilidad y acceso". Un verdadero acto de fe.

Finalmente, redefine el concepto de consentimiento informado y lo retira de la voluntad de los y las pacientes, al establecer que 'forman parte de los consentimientos informados, las hojas de indicaciones médicas y/o profesionales, las planillas de enfermería, los protocolos quirúrgicos, las prescripciones dietarias, certificados de vacunación, los estudios y prácticas realizadas, rechazadas o abandonadas'.

Esto no sólo constituye un abuso en términos de derecho a la intimidad de las personas, sino y fundamentalmente un avance inadmisible sobre el derecho constitucional de habeas data al delegar el consentimiento de los y las pacientes a los proveedores del sistema de salud.

La creación de esta base de datos es peligrosa, invasiva y abusiva. Está basada en objetivos que no quedan claros y no provee ninguna certeza, ni mucho menos resguardos mínimos necesarios de seguridad de la información sensible que pretende administrar.

No hace falta agregar mucho al mandato de que en 24 meses se diseñe un software que pueda estar accesible desde todos los efectores de salud en todo el país. ¿Saben ustedes qué capacidad de infraestructura, equipamiento y desarrollo hace falta para montar esto en ese plazo?

El valor en términos económicos de una base de datos de este tenor implica a su vez una tentación muy grande en término de accesos indebidos. Es importante recordar que la trayectoria del Estado argentino a la hora de preservar los datos de la ciudadanía dista mucho de ser confiable.

Una vez más, desde este espacio, nos oponemos a la construcción de bases de datos centralizadas que contengan datos sensibles de la sociedad sin considerar mínimamente el principio precautorio de una actividad que a todas luces genera más riesgo para la privacidad de la ciudadanía y una reducción inadmisible de los consagrados derechos de habeas data que beneficios para un sistema de salud que claramente hoy se encuentra ampliamente sobrepasado en su capacidad.

La seguridad informática no es un acto de fe. Una base de datos no está segura porque el texto de una ley así lo afirme. La seguridad de la información en poder del estado debe ser una política pública sólida cuya construcción en Argentina todavía está en estado embrionario. Mientras tanto, exponer los datos de la ciudadanía y vulnerar su privacidad no debería ser admisible por más buenas intenciones que el legislador pretenda incorporar en sus proyectos de ley.

Una vez más: urge una política de protección de los activos digitales en poder del Estado

VER EL NEWSLETTER COMPLETO

El ataque sufrido por los sistemas de la Dirección Nacional de Migraciones (DNM) pone una vez más de relieve la importancia de una política pública de protección de activos digitales. No vamos a dedicar mucho de esta columna al caso en particular, que ya ha sido narrado en nuestro sitio web y reportado por buena parte de la prensa nacional, sino al contexto en el que se presenta y los lineamientos que consideramos esenciales para que sucesos de este tipo no se repitan.

Resulta indispensable mencionar que en casos donde se producen filtraciones de información bajo gestión del Estado, las acciones de investigación policial y las causas penales que pudieran abrirse no reparan el daño. Es más, en la mayoría de los casos conocidos, jamás se llega a detectar, identificar y mucho menos condenar a los reales responsables de los ataques. Pero aún así, el daño ya está hecho. Cuando se trata de filtración de información personal, datos sensibles, datos confidenciales de oficinas públicas y de la ciudadanía, no hay reparación posible.

Por eso, nuestra posición en relación a la seguridad de los activos digitales en poder del Estado es diametralmente opuesta a la que parece ser la norma de sentido común y la respuesta de diversos sectores, incluyendo el Ministerio de Seguridad de la Nación. La política de cibercrimen, ciberdelito y ciberseguridad planteada en el marco de la Resolución 977/2019, aprobada en la gestión anterior y vigente a la fecha, es no sólo desatinada sino insuficiente y estéril para el objetivo de proteger la información que gestiona la Administración Pública Nacional.

Una política de seguridad de la información no es, ni debe ser, una política policial ni sostenida por las fuerzas de seguridad. Debe ser una política de prevención basada en protocolos de acción, estrategias de mitigación, prevención de daños y ataques que fije lineamientos rigurosos a toda la administración pública. Esta política no debe estar en manos de las fuerzas federales ni de las policías de ningún tipo, ya que no se trata de una mirada estrictamente criminal y punitiva del problema.

Existe en Argentina, en el marco de la Jefatura de Gabinete de Ministros, un área dedicada a la ciberseguridad. En el actual organigrama estatal, es ese el lugar desde el que deben partir las políticas y protocolos de custodia y protección de los activos digitales. Este es el escenario actual de Argentina. En un escenario ideal deberíamos, con carácter de urgencia, delinear una institucionalidad más sólida y estratégica que lleve adelante esta tarea.

A la hora de imaginar una política adecuada, evaluar modelos exitosos es el primer paso a seguir. Es por eso que nos permitimos poner como ejemplo a la Bundesamt

für Sicherheit in der Informationstechnik (BSI), la Oficina Federal de Seguridad de la Información de Alemania. Se trata de un cuerpo profesional de trabajo en seguridad informática que marca la pauta y fija las condiciones bajo las cuales se procesa la información en el Estado alemán. Esta oficina, altamente especializada y con capacidades institucionales transversales a todo el gobierno alemán, establece y monitorea todos los aspectos centrales de la gestión de información en la Administración Pública Federal, incluyendo las aplicaciones y dispositivos que usan las máximas autoridades del Estado. Su objetivo es promover la seguridad de la información para todo el país, no sólo para el Estado, sino para la ciudadanía y el sector privado. Trabaja en coordinación y cooperación con el sector privado y los practicantes de la seguridad de la información en Alemania.

Por supuesto es imposible comparar la coyuntura alemana con la nuestra. La BSI cuenta con una planta profesional permanente, un presupuesto enorme y una dedicación de recursos que le permite trabajar en investigación, desarrollo y prevención como política de Estado. No es la única agencia de este tipo. Francia cuenta con la Agence nationale de la sécurité des systèmes d'information, con un presupuesto de más de 100 millones de Euros y más de 500 empleados en su planta permanente. España, por su parte, cuenta con el Instituto Nacional de Ciberseguridad (InCIBe).

Esto no pretende ser un mero relato de lo que sucede en países con muchos más recursos que los nuestros. Pero si queremos enfatizar que es necesario contar con políticas de protección de la información, especialmente a nivel Estado, y que estas políticas no pueden ser minimizadas ni postergadas. El evento de Migraciones es elocuente por sí mismo, pero no es el único. Hace pocas semanas dimos cuenta en este espacio de la filtración de datos de 115.000 argentinos registrados en las bases de datos del gobierno de San Juan, víctimas de la negligencia de un Estado provincial que no dispuso ninguna medida de resguardo a esos datos.

Hace pocos días, además, junto a un equipo de amigos de la Fundación, dimos la voz de alerta sobre la precariedad en la seguridad de la app de covid 19 de la Provincia de Salta. Nuestra buena relación con el CERT y con el área de Ciberseguridad nos permitió levantar una alerta con la esperanza de haber contribuido a hacer un rápido control de daños.

Ahora bien, no es posible ni aceptable publicar apps llenas de agujeros de seguridad. No es admisible que el Estado ponga en riesgo un bien que no le pertenece, los datos de la ciudadanía. No es admisible que Argentina, que cuenta con una pujante comunidad de Infosec, no cuente con una política pública en este sentido.

No es admisible que todo lo que se construya alrededor de la seguridad de la información tenga la impronta de las fuerzas federales de seguridad, que con el escandaloso caso La Gorra Leaks dejó de manifiesto no sólo que carece de cualquier competencia para lidiar con el tema en materia preventiva, sino que carece además de la voluntad de investigar a los reales responsables tras allanar perejiles y miembros de la comunidad de infosec por el mero hecho de haber informado públicamente sobre esos sucesos.

Si finalmente, como parece ser, se impone la doctrina heredada de la gestión de Patricia Bullrich al frente del Ministerio de Seguridad, vamos a estar un paso más lejos de construir una política pública sólida, razonable y apropiada para proteger la seguridad de los activos digitales en Argentina. Los y las argentinas estaremos en mayor riesgo, definitivamente, no menos.

Regulación del Reconocimiento Facial en la Ciudad Autónoma de Buenos Aires

VER EL NEWSLETTER COMPLETO

El jueves 17 de Septiembre, en Reunión de Comisión de Seguridad de la Legislatura de la Ciudad Autónoma de Buenos Aires dio tratamiento al proyecto de modificación del Sistema Integral de Seguridad Pública, integrando los sistemas de reconocimiento facial. Se trata del **expediente 1686-D-2020** para modificar la Ley N° 5.688, bajo la firma de la legisladora Claudia Neira, Claudio Ferreño, Victoria Montenegro y Santiago Roberto, todos integrantes del Bloque del Frente de Todos en la Legislatura.

El proyecto de referencia tiene como aspiración establecer un marco regulatorio al sistema de reconocimiento facial que el poder ejecutivo de la Ciudad Autónoma de Buenos Aires implementó por simple resolución y compra directa de las tecnologías aplicadas. En estos momentos, el uso del sistema se encuentra suspendido a raiz de la pandemia de Covid 19, pero es vocación del gobierno de la Ciudad volver a implementarlo y renovar la compra de estos sistemas ni bien se restaure la normalidad post-pandemia.

Diversas organizaciones, entre ellas colegas como AccessNow, Asociación por los Derechos Civiles (ADC), Centro de Estudios Legales y Sociales (CELS) y el Observatorio de Derecho Informático Argentino (ODIA) nos hemos reunido para llevar adelante acciones conjuntas para contribuir al debate abierto en la legislatura. En este sentido, **entregamos diversos documentos a la comisión de Seguridad que fueron integrados al trámite parlamentario y leídos en el marco de la reunión del jueves pasado.**

Entendemos y apreciamos la buena voluntad del Frente de Todos de tratar de desarrollar un marco regulatorio para el uso de estas tecnología, pero entendemos que los problemas que esto conlleva están lejos de resolverse con la norma propuesta. Antes de plantear una regulación que habilite su uso es urgente dar una discusión de fondo y preguntarnos: ¿es aceptable instalar tecnologías de esta naturaleza en la esfera pública?

La respuesta unánime de nuestras organizaciones es no. Es imposible abordar un tema de tal gravedad con una posición resignada y de acompañamiento tal como la que planteó la Diputada Neira en la sesión del jueves pasado. A tal punto no parece haber conciencia del impacto de estas tecnologías, que sólo a instancia de lo solicitado por las organizaciones, las y los legisladores entendieron que la ley debía ser girada además a la Comisión de Derechos Humanos, Garantías y Antidiscriminación. Nota aparte merece el hecho de que una de las firmantes del proyecto es a su vez presidenta de esa comisión que debe necesariamente tramitar este tema.

¿Por qué no se entiende que las tecnologías de reconocimiento facial implican un peligro tan severo a la propia seguridad y Derechos Humanos de las personas que transitan por la Ciudad de Buenos Aires? La noción de que las tecnologías aplicadas a la seguridad son indispensables, que son apropiadas y que son eficientes debe ser uno de los mitos mejor instalados en la conciencia colectiva, incluyendo de quienes deben tomar decisiones informadas y basadas en evidencias.

Existe numerosa documentación que pone de relieve los problemas de este tipo de implementaciones, pero en la reunión de comisión todo se redujo a comentarios sobre lo necesario del uso de tecnologías y el equilibrio entre seguridad y Derechos Humanos, sin considerar que vulneran los Derechos Humanos es una forma grave de inseguridad. No hay que buscar un equilibrio allí: hay que respetar los Derechos Humanos, entre los cuales la seguridad de cada persona es parte intrínseca.

Desde las organizaciones solicitamos la ampliación del debate, contribuimos con documentos con argumentos y evidencias y propusimos que se regulen estas tecnologías, pero al estilo San Francisco o Boston: con una moratoria o simple y llana prohibición. Hicimos nuestras las **palabras del Relator de Privacidad de ONU**, quien invocó la urgente necesidad de realizar una evaluación de impacto en el derecho a la privacidad antes de implementar este tipo de tecnologías, en referencia a su uso en la Ciudad de Buenos Aires.

Es por eso, que desde Vía Libre recomendamos seguir con atención estos temas, ya que si bien esta iniciativa tiene lugar en la Ciudad de Buenos Aires, una vez que se legitima y normaliza, su réplica en otras ciudades y distritos no tarda en llegar.

Las tecnologías de reconocimiento facial son invasivas de la privacidad, son inexactas, se basan en sistemas de inteligencia artificial que, con resultados elaborados a base de estadísticas, redundan en una profundización de diversas formas de sesgos y discriminación, con impacto directo en el debido proceso, la privacidad, la presunción de inocencia, la libre circulación por el espacio público y la libre asociación y reunión.

Otro tema se abrió a partir de la reunión: la funcionaria del área de seguridad que estuvo presente en la sesión explicó que además se compraron sistemas para prevenir conductas sospechosas (como el merodeo) y para el análisis forense de los registros de CCTV requeridos en el marco de alguna investigación judicial.

Los sistemas de predicción de conductas son extremadamente peligrosos y poco sabemos sobre lo que se ha comprado e instalado en la Ciudad de Buenos Aires. Aprobar una regulación como la que plantea el FdT, aunque pretenda fijar cotas a los sistemas, termina legitimando una práctica que desde los sectores comprometidos con los Derechos Humanos deberíamos cuestionar.

Seguiremos trabajando estos temas, seguiremos participando de las sesiones y articulando con colegas de otras organizaciones para prevenir y alertar sobre los peligros de este tipo de tecnologías en la esfera social.

Octubre

Volver a las fuentes. Hacia una política de autonomía basada en Software Libre

VER EL NEWSLETTER COMPLETO

Ayer 4 de octubre se cumplieron 35 años de la fundación de la Free Software Foundation, una organización creada en los años 80 por Richard Stallman, a quien le debemos buena parte del desarrollo de una filosofía de autonomía y libertad vinculada al software. Nunca está demás recordar ese concepto que da origen a buena parte del recorrido de nuestra organización también, el software libre se trata de la libertad de las personas frente a los programas de computación, libertad de usarlo para cualquier propósito, de estudiar cómo está escrito y adaptarlo a las propias necesidades, libertad de hacer y distribuir copias, libertad de distribuir y compartir esas obras derivadas de ese software.

Este concepto simple y práctico establece una forma de mirar el mundo de las computadoras que es indispensable recordar, reconocer y recuperar a la luz del estado actual del debate sobre las tecnologías que determinan cada vez más la vida social.

La celebración de un nuevo aniversario de la Free Software Foundation nos ofrece una oportunidad interesante para recuperar algunos conceptos elementales que se desprenden de aquella definición de software libre que tantas veces hemos repetido a lo largo de los últimos **20 años en Vía Libre**. No se trata sólo de programas de cómputo, sino y fundamentalmente, de establecer nuevas formas de pensar la regulación del conocimiento.

Es por eso que cualquier discusión sobre software libre nos lleva irremediablemente a hablar de propiedad intelectual, porque la concepción filosófica del software libre se basa justamente en debatir la problemática vigente de los actuales sistemas de gestión y apropiación de bienes intangibles. En una mirada que se adelantó a lo que vendría después, el movimiento de software libre construyó un paradigma de conocimiento centrado en la libertad y la autonomía de las personas en directa relación con la construcción colectiva de conocimiento. No se trata de libertades individuales estrictamente, sino de asegurar libertades que sólo son factibles en la colectividad.

En tiempos de Covid 19, con la masiva penetración de las tecnologías de información y comunicación y la necesidad urgente de informatizar la gran mayoría de las relaciones humanas, desde los afectos hasta la educación y el trabajo, la necesidad de reconstruir y promover un activismo centrado en los valores del software libre se torna urgente.

Esos valores son los que nos permiten afirmar que el interés público siempre debe estar por encima de los intereses particulares sostenidos en sistemas de propiedad intelectual que son fuertemente restrictivos, como la ley 11.723 de Argentina y tantas otras legislaciones que no contemplan flexibilidades indispensables en los tiempos que corren: bibliotecas, estudiantes de todo nivel, investigadores académicos, docentes universitarios, personas con diversos tipos de discapacidades y miles de personas que necesitan acceso y sólo pueden tenerlo incumpliendo la ley. Esta situación nos insta a repensar la regulación de propiedad intelectual desde una perspectiva de bien público.

Pero los conceptos filosóficos que aprendimos quienes nos formamos en la concepción del software libre van aún más allá y es por eso que se torna ineludible referirlos a otras áreas sustantivas de la vida social hoy. Mientras escuchamos como tendencia una reivindicación de la soberanía tecnológica para nuestros países, en particular para nuestra región, vemos con desazón que la hegemonía del software privativo sigue siendo la norma.

Los mismos modelos de servicios presentados como gratuitos para determinados sectores clave de la vida pública (vale citar el acuerdo de la Universidad de Buenos Aires para el uso de Teams en todas sus facultades) siguen vigentes, como aquella recordada Alianza por la Educación que en el año 2003 el Ministerio de Educación de Argentina firmó con la empresa fundada por Bill Gates. A eso se suman las alianzas con nuevos actores, como el convenio que la Universidad Nacional de Córdoba firmó con Google para proveer servicios de video llamada para las clases por una módica suma de dólares impagable para un presupuesto en crisis. La historia se repite y nada cambia, sólo pasan los años y las oportunidades se diluyen entre nuestras manos. Eso sí, el discurso de la soberanía sigue firme sin que se debata en profundidad qué significa en el campo de las tecnologías de la información y comunicación.

El discurso de la soberanía tecnológica promete convertirse en uno más de tantos significantes vacíos si no se adoptan políticas públicas de largo plazo que permitan desarrollar dos aspectos esenciales sin los cuales la soberanía no es más que una palabra de moda afín con algunas líneas ideológicas: Desarrollo de Autonomía y Desarrollo de Capacidades. No existe soberanía sin desarrollo de capacidades, sin la cual, la autonomía será difícil de alcanzar a nivel tanto social como individual.

El concepto de soberanía puede parecer tentador en un contexto global en el cual el modelo de la internet controlada y fragmentada de China aparece como el futuro, en el que la estrategia de la 'Clean Network' del Departamento de Estado de los EEUU promete fijar barreras comerciales y de conexión con el mundo y donde la fragmentación de la red promete ser ese futuro en el cual se vuelve a pensar en el control por parte de los Estados Nacionales, lo que en muchos casos redundará en censura y control por parte de estados reñidos con los Derechos Humanos. Sin embargo, no hay que caer en la trampa de que toda regulación por parte de los Estados redundará en mecanismos de censura y control necesariamente. La regulación del Estado es indispensable para garantizar el pleno ejercicio de los Derechos Humanos, del Estado depende la consolidación y defensa de esos derechos y por lo tanto, no se puede abdicar de la responsabilidad. Menuda contradicción aparece por delante.

¿Queremos una Internet regulada por cada estado, fragmentada, controlada? O ¿Queremos una "Internet Libre" (entre comillas) donde los Estados renuncian a su rol de regulador y dejan librada al mercado la gestión de una de las infraestructuras centrales de la vida pública?

Las preguntas son deliberadamente tramposas y suponen una dicotomía que, no por falsa, es menos usada. No queremos una Internet en la cual el Estado sea el único regente pero tampoco una red dominada por un puñado de corporaciones que sólo responden a sus accionistas. Pero para salir de esa falsa dicotomía es menester construir capacidades reales que nos permitan desarrollar y consolidar espacios de autonomía. En ese sentido, es urgente pensar políticas que aborden al menos tres temas nodales: las regulaciones de propiedad intelectual, las políticas de defensa de la competencia y los estándares de los cuales depende la interoperabilidad.

El Software Libre nos ha enseñado mucho en esa materia, nos ha enseñado que es indispensable construir un modelo de propiedad intelectual flexible y abierto que posibilite el desarrollo, el aprendizaje, la participación y el pleno control sobre el conocimiento producido. A su vez, nos recuerda y enfatiza que la interoperabilidad es un elemento central para que contemos con las libertades plenas para dirimir qué tecnologías queremos adoptar, desarrollar, usar y compartir. A eso es clave analizar la problemática de la concentración, los monopolios y las políticas de defensa de la competencia que han perdido fuerza en las últimas décadas y permitido el crecimiento monumental de corporaciones en todos los ámbitos de la economía global, no sólo en la industria tecnológica que podemos afirmar es una hija más de estos procesos de hiperconcentración del capital.

No se trata de cerrar las fronteras en un campo que es eminentemente global, sino de contar con las herramientas básicas que nos permitan discernir estratégicamente en los conflictos y promover la autonomía con un urgente fortalecimiento de las capacidades locales, nacionales, regionales.

El movimiento de Software Libre lleva años trabajando lentamente en esos pasos. Sin Estados que adopten medidas apropiadas en este sentido, la autonomía en materia tecnológica será cada vez más difícil de alcanzar.

Saludamos a la Free Software Foundation en sus 35 años de existencia. Todavía falta mucho, muchísimo para cumplir aquella misión de promover software libre para una sociedad libre.

¿Será posible remediar la hiperconcentración del mercado de las Big Tech?

VER EL NEWSLETTER COMPLETO

A esta altura de los debates por la regulación de las grandes plataformas, parece inevitable pensar que se debe implementar algún tipo de regulación para solucionar los múltiples problemas que se han puesto sobre la mesa en los últimos años. Se trata de problemas de diversa índole y naturaleza y que implican una complejidad de difícil abordaje si se piensa en una única solución a los temas vinculados con libertad de expresión, gobernanza de contenidos, protección de la privacidad y los datos personales, desinformación y discursos de odio, defensa del consumidor y un largo etcétera que atraviesa la discusión sobre las grandes plataformas de lo que se conoce como GAFA (Google, Amazon, Facebook, Apple).

Desde hace algún tiempo venimos sosteniendo en este espacio que la regulación no sólo debe ser inteligente, sino que tiene que ser apropiada para no generar más daños ni consolidar los problemas derivados de la hiperconcentración. En ese sentido, hacemos nuestra la posición de Cory Doctorow en su **artículo 'How to Destroy Surveillance Capitalism"**.

En ese documento, Doctorow aborda los dos problemas centrales que nos han traído hasta aquí y en los que coincidimos: el relajamiento extremo de las políticas antitrust que han impactado la economía de los EEUU desde el gobierno de Reagan en adelante, generando mega corporaciones y billonarios que concentran como nunca mercados y riquezas y por otro lado las políticas de propiedad intelectual que han contribuido a sostener esos monopolios y frenar la innovación y la capacidad de competir en esos mismos mercados. El surgimiento de las Big Tech no es otra cosa que una consecuencia más de ese proceso que impacta a todos los sectores de la economía.

Si escuchamos la voz de las áreas de policy de las grandes compañías y vemos las comunicaciones oficiales que han emitido en los últimos años, hay un nuevo llamado a viva voz a los gobiernos: '¡¡¡regúlenme!!!' parece ser el pedido de empresas como Facebook y Google. Esto se debe a que las regulaciones que admiten ahora para supuestamente solucionar los problemas creados por las campañas de desinformación, la violación de propiedad intelectual y la diseminación de discurso de odio las obligan a tomar medidas que son altamente costosas, desarrollar tecnologías de control de contenidos, expandir la contratación de ejércitos de revisores de contenidos y establecer reglas de control estricto sobre lo que los usuarios publican en sus plataformas. Con una arquitectura de este tipo obligada para todos los jugadores de la industria, la posible emergencia de competidores es tendiente a nula.

Ahora Facebook aparece con una **serie de recomendaciones regulatorias o legislativas para combatir las operaciones de influencia** que parecen escritas por un censor profesional. Sin definir en qué consiste una Operación de Influencia, la empresa se atreve a decir que los reguladores deben incluso emitir tipos penales nuevos para perseguir a las personas que se involucran en ese tipo de acciones.

Cualquier estrategia es válida a la hora de plantear soluciones falsas al problema de fondo: la concentración. Este documento de Facebook no aparece fuera de contexto.

La semana pasada, el Comité Antitrust del Congreso norteamericano, liderado por el Congresista David Cicilline publicó lo que a nuestro modo de ver constituye la pieza fundamental de la trama regulatoria para las Big Tech, el primer y principal documento que da en la tecla, un reporte que es fruto de la investigación de 16 meses llevada adelante sobre Google, Facebook, Amazon y Apple.

El documento plantea la urgente necesidad de reforzar los marcos de regulación anti monopolios y recupera el rol clave del Congreso en la definición de políticas públicas para los EEUU. Si este informe tiene el impacto que merece, estamos ante las puertas de un documento clave para reestructurar no sólo el mercado de las Big Tech, sino todo el modelo de la economía de los EEUU.

El documento de más de 450 páginas está **disponible en línea** y es una lectura obligada para quienes estamos pensando regulaciones sobre Internet.

Entre las recomendaciones que plantea el documento se destacan:

a) Restaurar las condiciones de competencia en la economía digital:

- Separaciones estructurales y prohibiciones de ciertas plataformas dominantes de operar en líneas comerciales adyacentes;
- Requisitos de no discriminación, que prohíban a las plataformas dominantes promover la autopreferencia y les exijan que ofrezcan condiciones iguales para productos y servicios iguales;
- Interoperabilidad y portabilidad de datos, exigiendo a las plataformas dominantes que establezcan condiciones de compatibilidad de sus servicios con múltiples redes y que promuevan que la información sea fácilmente trasladable entre ellas;
- Prohibición presunta contra futuras fusiones y adquisiciones por parte de las plataformas dominantes;
- Puerto seguro para los editores de noticias para salvaguardar una prensa diversa y libre y
- Prohibición de toda forma de abusos de poder de negociación, prohibiendo que las plataformas dominantes participen en prácticas de contratación que se deriven de su posición dominante en el mercado y requiriendo protecciones del debido proceso para individuos y empresas que dependen de las plataformas dominantes;

b) Fortalecimiento de las leyes antimonopolio:

- Reafirmar los objetivos antimonopolio de las leyes de defensa de la competencia y su centralidad para garantizar una democracia sana y vibrante;
- Fortalecer la Sección 7 de la Clayton Act, incluyendo la restauración de presunciones y reglas claras, la protección de competidores incipientes, y el fortalecimiento de la ley sobre fusiones verticales;
- Fortalecimiento de la Sección 2 de la Sherman Act, incluyendo la prohibición del abuso de posición dominante y la clarificación de las prohibiciones de apalancamiento, precios depredatorios, negación de servicios e instalaciones esenciales, rechazo a negociar, vinculación y autopreferencia y diseño de productos anticompetitivos;
- Tomar medidas adicionales para el fortalecimiento de la observancia de estas leyes en general, incluyendo los antecedentes jurisprudenciales problemáticos;

c) Revisar los mecanismos de observancia de las leyes antimonopolio:

- Restaurar las agencias federales para que tengan plena capacidad operativa, mediante la activación de sanciones civiles y otras medidas de alivio para las reglas de "métodos desleales de competencia", requiriendo que la Comisión Federal de Comercio participe en la recopilación regular de datos sobre concentración, mejorando la transparencia pública y la responsabilidad de las agencias, requiriendo fusiones regulares retrospectivas, codificando prohibiciones más estrictas en la puerta giratoria y aumentando los presupuestos de la FTC y la División Antimonopolio;
- Fortalecimiento de la aplicación privada, mediante la eliminación de obstáculos tales como cláusulas de arbitraje forzoso, límites a la formación de acciones colectivas, estándares creados judicialmente que restringen lo que constituye una lesión antimonopolio y estándares de alegato indebidamente altos.

La agenda de la responsabilidad de las empresas intermediarias sobre lo que hacen, dicen y publican sus usuarios parece haber copado todo debate sobre la regulación. Hacer que las empresas sean responsables, tengan el deber de monitorear y controlar lo que circula por sus redes, no sólo genera un incentivo a la censura privada cada vez más presente en esas plataformas con el consiguiente impacto sobre la libertad de expresión sino que desvía completamente el punto nodal del problema y contribuye a fortalecer la posición dominante de mercado de las mismas. Seamos honestos: pretender que paguen compensaciones pecuniarias por contenidos que publican sus usuarios es apenas un cosquilleo para las cuentas de estas empresas y genera un ecosistema en el que nadie querrá invertir y generales competencia.

Por eso ahora Facebook sale con su estrategia voluntaria de control de discurso de odio, desinformación y todas las plagas del lejano oeste en que supuestamente se ha convertido Internet. Mientras nos entretenemos en debatir responsabilidades, juicios y causas en los diversos tribunales, las soluciones efectivas empiezan a hacerse visibles. El Informe del Comité dirigido por el Congresista David Cicciline es un aporte sustantivo en la buena senda.

En defensa del derecho a cifrar

VER EL NEWSLETTER COMPLETO

El 11 de Octubre pasado, los gobiernos de las 'Five Eyes Nations' (Australia, Canadá, Nueva Zelanda, Reino Unido y los Estados Unidos) más Japón e India **firmaron una declaración exigiendo la instalación de backdoors en todos los sistemas de cifrado punto a punto disponibles.**

Después de una larga perorata sobre cuánto les importa la privacidad de las personas y el rol clave del cifrado punto a punto para proteger la información personal, la propiedad intelectual, los secretos industriales, la privacidad y la ciberseguridad, el grupo de países firmantes solicitó a las grandes empresas de tecnología que implementen mecanismos para quebrar estos sistemas de cifrado tras enmarcar el asunto en un tema de seguridad pública.

Aseguran que estas implementaciones suponen desafíos a la seguridad pública y apelan a los clásicos y ya remanidos argumentos de que quebrar el cifrado es clave para proteger a los sectores más vulnerables de nuestra sociedad. Si, el clásico "¿alguien puede pensar en los niños?"

Implican en su texto, además, que no sólo la ciudadanía está en riesgo sino también las empresas de tecnología ya que ellas mismas se ven imposibilitadas de responder en los casos en los que se "violan sus términos de servicios".

La declaración finaliza desafiando la afirmación de que la "seguridad pública no puede ser protegida sin comprometer la privacidad o la ciberseguridad" y aseguran contar con recursos e ideas capaces de proteger todos estos importantes valores para nuestras sociedades. A su vez, prometen trabajar con el sector privado en soluciones a esta problemática que parece no tener una salida sencilla.

Desde hace muchos años, se vienen elaborando estrategias para minimizar las capacidades de cifrar las comunicaciones, siempre con el argumento de la seguridad pública. Hace años que venimos diciendo que no se debe considerar que para ganar seguridad se debe vulnerar la privacidad de las personas, porque la mera pérdida de un derecho como es la intimidad y la confidencialidad de las comunicaciones implica un hecho de inseguridad.

La seguridad implica necesariamente la preservación de derechos, por lo que es inexplicable que todavía se considere que para ofrecer una falsa promesa de seguridad se deba ceder un derecho sustantivo y esencial como la privacidad. El derecho a cifrar es una reivindicación que sostenemos y nos parece indispensable promover y proteger.

¿Por qué reivindicamos que se debe preservar y defender el derecho al cifrado en las comunicaciones?

En primer lugar, en el mundo digital, las comunicaciones son esencialmente inseguras. Internet no fue diseñada para la privacidad por lo que, en líneas generales, debemos partir siempre del supuesto de que todo lo que intercambiamos a través de la red sin medidas apropiadas de privacidad es o puede volverse público. Las posibilidades de terceros de acceder a nuestras comunicaciones son enormes y el usuario promedio no suele tener mucha conciencia sobre la necesidad de proteger sus comunicaciones. Por esto es importante que los servicios más populares hayan incluido el cifrado de punto a punto entre sus prestaciones sin que los usuarios tengamos que arbitrar configuraciones que puedan sumar complejidad.

El derecho a la intimidad es un derecho humano reconocido por nuestra constitución, por los tratados internacionales de Derechos Humanos y por lo tanto, la ciudadanía debe contar con la posibilidad de custodiar ese derecho de forma apropiada, sin injerencias arbitrarias en su vida privada (Artículo 19 de la CN).

La violación de las comunicaciones sólo es factible como medida excepcional, bajo principios de legalidad, necesidad y proporcionalidad y bajo el marco de la legislación vigente, que debe ser adecuada a principios constitucionales. Pero esa excepcionalidad no debe traducirse en medidas generales que minimicen las capacidades de todas las personas de resguardar sus derechos. Podríamos decir que pedir una puerta trasera a todos los dispositivos, es como exigir la llave de todos los domicilios por si alguna vez tengo que allanar la casa de alguien en el marco de una investigación criminal.

La comunicación de estos siete países forma parte de un proceso largo que tiene la pretensión de introducir puertas traseras a los sistemas de cifrado, tendencia de la que forman parte otras instancias previas que tuvieron al cifrado como punto de ataque por parte de gobiernos y servicios de inteligencia.

En este sentido, es indispensable recordar que ya pesan restricciones a la exportación y la inclusión del cifrado en convenios internacionales como el Arreglo de Wassenaar, un tratado internacional contra la exportación de armas de guerra del que Argentina es firmante.

El Arreglo de Wassenaar también está plagado de buenas intenciones, se constituyó para contribuir a la seguridad y estabilidad de las relaciones internacionales mediante la promoción de la transparencia y la responsabilidad en la transferencia de armas y productos tecnológicos de uso dual, para prevenir que las mismas lleguen a manos de terroristas. Con estos argumentos se integran a **esta lista** de elementos de circulación internacional restringida, que requieren autorización por parte de los estados para su exportación, numerosos desarrollos tecnológicos comúnmente utilizados en seguridad informática, especialmente diversos algoritmos de cifrado.

Es indispensable que prestemos atención a esta iniciativa de estos siete países que pretenden socavar las capacidades de la ciudadanía de proteger su privacidad con una de las pocas herramientas que contribuyen a cuidar este derecho fundamental.

Proteger y reivindicar el cifrado punto a punto es un paso más, aunque seguramente no será el último, en defensa del derecho a la intimidad.

Reconocimiento Facial en Buenos Aires. ¡Nos ven la cara!

VER EL NEWSLETTER COMPLETO

El jueves pasado la legislatura porteña aprobó la reforma de la Ley 5688 del Sistema Integral de Seguridad Pública, una norma que regula las políticas de seguridad de persecución penal entre las que se encuentra el sistema de cámaras de videovigilancia en el espacio público. Junto a organizaciones colegas como Access Now, Amnistía Internacional, Asociación por los Derechos Civiles, Centro de Estudios Legales y Sociales, DATAS y el Observatorio de Derecho Informático Argentino presentamos numerosas objeciones e hicimos todo lo que estuvo a nuestro alcance para tratar de profundizar el debate y llamar la atención sobre los problemas que supone la instalación de sistemas de reconocimiento facial en la esfera pública. Enviamos una nota a los legisladores e hicimos pública nuestra posición, pedimos que se gire curso a la comisión de Derechos Humanos y Garantías y no tuvimos éxito, no logramos siquiera que los legisladores habilitaran un espacio amplio para exponer sobre un tema que no sólo se discute en nuestro país sino que está en la agenda de Derechos Humanos en muchos países del mundo.

Como menciona nuestra carta a la legislatura, la incorporación de esta tecnología presenta múltiples afectaciones para el ejercicio de los derechos humanos, entre ellos, la privacidad, la libertad de expresión, la libertad de reunión y asociación, la libre circulación por el espacio público, la no discriminación y la presunción de inocencia y el debido proceso.

Paradójicamente, las organizaciones estábamos esperando que se reuniera la Comisión de Derechos Humanos, Garantías y Antidiscriminación para dar un volumen más sustantivo al debate sobre el impacto de estas tecnologías pero el giro a esa comisión fue suspendido sorpresivamente.

Así, con dictamen en las comisiones de Seguridad y de Justicia, el proyecto fue a recinto y fue aprobado con la mayoría propia del bloque oficialista, al que se sumó el bloque de Evolución.

La sesión fue muy extraña. Para quienes no pudieron verla, está **disponible en nuestro canal de Youtube.**

Vale la pena empezar por el hecho de que el proyecto fue presentado y llevaba la firma de tres legisladores del Frente de Todos, que tras las numerosas críticas emitidas al proyecto decidió votar en contra del mismo. Es importante rescatar esta actitud como un gesto positivo por parte de esta fuerza que tras el gravísimo error cometido decidió revertir su acompañamiento. Esperamos que esto sirva de aprendizaje y experiencia ya que las y los legisladores saben que cuentan con este grupo de organizaciones diversas que podemos asistir a la hora de regular temas que impactan en los DDHH.

No es aceptable seguir legislando sin saber. En temas de seguridad y garantías, eludir la visión desde los Derechos Humanos es una forma de claudicación que lamentamos profundamente, ya que las tecnologías no son inocuas y son a su vez vectores de ideología que impactan de lleno en la vida social. No se puede aceptar el discurso que establece que la vigilancia generalizada puede ser un recurso apropiado para lidiar con problemas diversos tales como la búsqueda de personas prófugas de la justicia.

Ahora nos queda la preocupación enorme de ver cómo se restaura este sistema que ya se estuvo usando en la Ciudad de Buenos Aires y que ahora, a raíz de la pandemia, se encuentra suspendido. No faltará mucho para que el negocio se vuelva a poner en marcha, porque hablemos con propiedad, esto es un negocio que alimenta la industria de las tecnologías de la seguridad. Ese negocio se nutre de buena prensa, funcionarios ávidos de soluciones mágicas, marketineras y modernas y una sociedad mayormente afín a una mirada punitiva que demanda seguridad a cualquier precio.

El bloque evolución, que criticó duramente el proyecto en las comisiones, pero votó favorablemente en el recinto, negoció la incorporación de una comisión de seguimiento y control de esta implementación. Será difícil dar seguimiento apropiado, porque es común que estas empresas proveedoras de servicios de este tipo no entreguen jamás el código fuente ni acceso a sus datasets de entrenamiento de los algoritmos de reconocimiento facial que implementan. Tampoco será fácil obtener información fidedigna, porque lo que indican los funcionarios es poco creíble. En reuniones mantenidas con funcionarios y legisladores oficialistas nos encontramos con que se sostienen discursos de dudosa verosimilitud, afirmaciones tales como que el sistema arroja 'cero falsos positivos' o que nuestro sistema es más moderno y eficiente que el usado en Londres o Shangai son algunas de las cosas que hemos oído en las últimas reuniones.

En la reunión de Comisión de Seguridad se dijo incluso que se están implementando tres sistemas: el de reconocimiento facial para la captura de prófugos, el de investigación forense y el predictivo. Este último es un sistema dedicado a identificar de manera automatizada conductas anómalas para levantar alertas de intervención policial. Se lo justifica diciendo que el sistema podrá detectar un auto a contramano en una autopista como hecho anómalo, pero nada sabemos sobre el entrenamiento de esa IA y qué cosas pasarán a ser anómalas y requieran intervención policial.

Estas tecnologías tienen un doble problema. Si funcionan mal, afectan la vida de muchas personas que son erróneamente identificadas, demoradas y en algunos casos incluso detenidas por su fisonomía. Si funcionan bien, generan un estado represivo, de vigilancia indigna de un sistema democrático respetuoso de las libertades civiles.

Por eso, repetimos lo que venimos diciendo hace meses: 'Al reconocimiento facial no se lo regula, se lo prohíbe'.

Noviembre

¿Puede un algoritmo dejarte sin empleo?

VER EL NEWSLETTER COMPLETO

Muchas preguntas surgen a partir de la incorporación a la vida social de cada vez más procesos mediados por sistemas automatizados de toma de decisiones. Las preguntas sobre el empleo están a la orden del día, ya que es una de las áreas donde el impacto de estas tecnologías tiene consecuencias más notables. Desde la automatización para la selección de curriculums pasando por la gestión y evaluación de actividades laborales, los algoritmos se insertan cada vez más en la vida laboral de las personas.

La semana pasada, **un grupo de ex trabajadores choferes de Uber iniciaron una demanda legal contra la compañía para eliminar el algoritmo que según ellos causó su despido**. Según indicaron, los tribunales deberán evaluar por primera vez una norma que está contenida en el Reglamento General de Protección de Datos de la Unión Europea en su artículo 22. Este artículo regula las decisiones individuales automatizadas, incluyendo la elaboración de perfiles y establece el derecho de toda persona interesada en no ser objeto de una decisión basada únicamente en el tratamiento automatizado de datos que produzca efectos jurídicos en él o lo afecte significativamente de modo similar.

Estamos ante un caso importante en la jurisprudencia europea, porque es la primera vez que este articulado se pone en pleito en fuero judicial. Los choferes de origen británico accionaron legalmente en Holanda, sede donde la firma Uber tiene radicados sus centros de datos. Por supuesto, Uber indicó que las cuentas de estos choferes fueron desactivadas sólo después de que hubiera una revisión manual por parte de humanos, pero es difícil definir si esto es así. Ahí radica la complejidad del caso. **(Véase la demanda completa en el sitio de los abogados holandeses que la llevan adelante)**

El sindicato de mensajeros y trabajadores de aplicaciones (ADCU) indicó que desde el 2018 registraron alrededor de mil casos de personas que fueron acusadas de actividad fraudulenta e inmediatamente suspendidos de la aplicación sin derecho a apelación. Esto se diferencia notablemente de las normas laborales que regulan la actividad del sector en Inglaterra, donde los transportistas y choferes que son despedidos de un empleo tienen que ser reportados ante la oficina de transportes de Londres, donde pueden explicar su situación y justificar por qué deben mantener sus licencias. En el caso de Uber esto no ocurre así y los choferes ignoran de plano que los ha llevado a la suspensión.

La intención legal del sindicato y los abogados con los que trabajan es establecer una acción de clase, llevar el tema al Tribunal de Justicia Europeo y constituir un precedente que proteja los derechos de los y las trabajadoras que dependen de la aplicación para su sostén cotidiano. Es la primera vez que se pone sobre la mesa de un tribunal el artículo 22 de la GDPR.

Es importante destacar que en Argentina, las regulaciones también deberían protegernos de este tipo de tratamiento automatizado de datos y que poco sabemos todavía de cómo poner en acción salvaguardas de ese tipo. Tenemos algunos instrumentos que nos permitirían accionar, y en particular, indagar a las empresas sobre la gestión de nuestros datos personales.

Tenemos derecho a saber qué datos recolectan, qué usos le dan a esos datos que recolectan, corregir esos datos, modificarlos, eliminarlos y ejercer plenamente los derechos que nos reconoce el Principio de Habeas Data de la Constitución Nacional de 1994 y las leyes vigentes de protección de datos personales.

En el mundo de los derechos laborales hay todavía un largo trayecto por recorrer para que trabajadores y trabajadoras vinculadas a la economía de plataformas gocen de los derechos correspondientes en materia laboral. El caso abierto en Holanda promete ser largo, complejo y sobre todo muy interesante, ya que habrá que analizar cómo se toman las decisiones mediadas por algoritmos, cuáles son los argumentos para el despido de estas personas y cómo se respetan los derechos laborales en una economía basada más en la precarización que en la innovación.

Historia Clínica Digital: Información sensible y altos riesgos

VER EL NEWSLETTER COMPLETO

El 5 de noviembre pasado, el Jefe de Gabinete de Ministros anunció el plan de telemedicina junto al Ministro de Salud Ginés González García. "El programa prevé una inversión de 5 mil millones de pesos y contempla la creación de la historia clínica única, la receta electrónica, los datos en la nube y la telemedicina" detalló Cafiero en la **presentación de la iniciativa**. El programa es indistinguible del que **presentó en 2019 el ex secretario de salud Adolfo Rubinstein**.

Una vez más, en materia de aplicación de tecnologías a la vida pública nos encontramos con continuidades que ya no sorprenden. La visión de las tecnologías sigue siendo la misma, en particular en áreas en las cuales la utilización de datos de las personas es particularmente sensible (Salud y Seguridad).

Hace meses venimos sosteniendo que es una mala idea armar una base de datos centralizada de la historia clínica de cada persona. Los antecedentes en materia de protección de datos y custodia de los activos digitales no nos dan ninguna razón para confiar en que esos datos sensibles estarán a buen resguardo.

Expresamente la regulación de protección de datos personales establece que la información de salud entra en la categoría de datos sensibles. En su artículo 2do. la **Ley 25326** establece que son Datos sensibles los "Datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual".

La misma normativa establece la prohibición de constituir bases de datos de este tipo salvo cuando medien razones de interés general autorizadas por ley. Lamentablemente, el Congreso ha hecho avanzar un proyecto en este mismo sentido. Es claro que hay acuerdos entre las fuerzas políticas mayoritarias para avanzar en esta política que pone en severo riesgo los datos de la población.

Los datos de salud son fundamentales en la vida privada de las personas, ya que conllevan información que puede ser usada de forma discriminatoria, dañina y suponer situaciones de riesgo para las personas afectadas. No se trata sólo de la eventual publicidad de esos datos sino y fundamentalmente de la posibilidad de que esos datos sean usados en contra de sus titulares.

Este tipo de información tiene un valor económico incalculable. Compañías aseguradoras, empresas de medicina prepaga y por supuesto las grandes empresas cosechadoras de datos personales ven en estas bases de datos un valor incalculable que les permitirían por ejemplo, segmentar ofertas, brindar servicios de selección de personal, generar conocimientos y hacer prospectiva sobre determinadas poblaciones, entre múltiples otros usos potenciados hoy por el uso de sistemas de inteligencia artificial.

La creación de una base de datos centralizada de este tipo es sin dudas un punto de ataque muy tentador para cualquier negocio. A eso debemos sumar la baja calidad de la gestión de los datos personales en Argentina. La experiencia reciente del ataque sobre la base de datos de Migraciones debería alcanzar para alertar sobre los riesgos de una base de este tipo. Antes de avanzar con los datos en la nube y otras expresiones vacías de puro marketing (solucionismo tecnológico en su más pura expresión), el Estado debería informar con claridad qué estándares de seguridad, qué impacto en Derechos Humanos y Privacidad, qué tecnologías evaluaron a la hora de avanzar. Pero claro, el discurso tecnoutópico es más ameno y efectista.

De hecho, el actual gobierno puede prometer y jurar que jamás entregará esta base de datos a terceros ni la usará en desmedro de la ciudadanía, pero no puede comprometerse sobre lo que hagan futuros gobiernos. Esa idea de que mi gobierno es bueno y no va a hacer nada malo con los datos es inaceptable. Vale recordar que en la reciente sanción de la regulación de uso de sistemas de reconocimiento facial en la Ciudad Autónoma de Buenos Aires, los legisladores del PRO se enorgullecieron de mencionar que esta política es una continuidad y una aplicación más del lanzamiento que Cristina Fernández de Kirchner hizo en noviembre de 2011 del sistema SIBIOS, la base de datos biométrica para la seguridad. Una absoluta vergüenza.

A esto podemos agregar que los antecedentes internacionales no son auspiciosos. En 2013 el Reino Unido lanzó Care.data, una iniciativa del sistema de salud inglés que centraliza la información de salud de sus pacientes. **La experiencia demostró una inadecuada protección de la anonimización de la información de los pacientes y conflictos notables con los médicos a cargo, falta de un entendimiento claro de las reglas del consentimiento informado y mínimo control sobre las ventas de la información.**

A esto se suma el acuerdo de cooperación entre la Royal Free London NHS Foundation Trust y la firma DeepMind Technologies Limited, una subsidiria de Alphabet Inc. en 2016. La idea del acuerdo fue entregar la información para el entrenamiento de algoritmos que permitieran un manejo apropiado de las enfermedades de riñón. Por supuesto, hubo problemas de privacidad, de transferencia de los datasets derivados de la información poblacional a grandes empresas privadas de prospectiva suponen serios desafíos a los tomadores de políticas públicas y la industria **(Powles, et al)**.

Finalmente, los tecno solucionistas de turno olvidan un principio fundamental: La autodeterminación informativa.

El artículo 7 de la ley de protección de datos personales lo expresa enfáticamente: "Ninguna persona puede ser obligada a proporcionar datos sensibles".

Desde Fundación Vía Libre esperamos que la actual gestión revise esta decisión y analice las implicancias de una política tan riesgosa en materia de derechos fundamentales, revise sus protocolos de administración y gestión de datos personales y comprenda que en materia de impacto sobre derecho a la autodeterminación informativa es indispensable aplicar evaluaciones previas y un principio precautorio.

Una vez filtrada una base de datos de este tipo, el daño ya está hecho. La autonomía de nuestros datos es un derecho y el estado debe cumplir su obligación de protección.

Allanar al mensajero

VER EL NEWSLETTER COMPLETO

El tratamiento que la justicia argentina le da a los reportes de vulnerabilidades en seguridad de la información es insostenible, arbitrario, injusto y totalmente contraproducente. Sin ánimo de generalizar, es hora de abordar este problema de forma profesional y rigurosa, porque las consecuencias de estos procedimientos no sólo son catastróficas para las personas involucradas, sino que traen graves problemas para toda la ciudadanía. No dimensionar esto es el primer y más recurrente error.

No es la primera vez que en estas páginas abordamos la urgente necesidad de proteger a quienes se dedican a la seguridad de la información en Argentina. Esta demanda no es casual, se sostiene en que de manera recurrente la justicia ordena allanar domicilios de investigadores y practicantes de infosec por el mero hecho de reportar vulnerabilidades.

Los casos se repiten uno tras otro y la consecuencia directa es el desincentivo total al reporte responsable, la criminalización de una práctica indispensable en las sociedades actuales y la falta total de investigación rigurosa sobre los reales responsables de las grietas de seguridad, que casualmente, siempre salen impunes.

Este fin de semana nos enteramos de un nuevo hecho que merece todo nuestro repudio y solidaridad con el investigador allanado y su familia.

Adrián Ruiz, especialista en informática que reportó en octubre la exposición de datos de 54 mil personas en la web de Caminos de la Sierra, empresa estatal que gestiona la Red de Acceso a Córdoba (RAC), recibió este viernes pasado a las 7 de la mañana un allanamiento en su domicilio. Ruiz identificó la vulnerabilidad al ingresar a su propia cuenta de usuario del sistema de pago electrónico. En su navegador detectó que si cambiaba la url - cosa que puede hacer cualquier persona sin demasiados conocimientos técnicos - se podía acceder a una carpeta general de archivos con información privada de las personas que usan el sistema.

En esa base estaban expuestos los datos de 54.214 clientes con nombre, apellido, número de documento, tarjeta de crédito y débito, patentes de sus autos, horarios de tránsito y sentido de paso en el peaje, correo electrónico, teléfono, domicilio, facturas de infracciones, recibos de pago, archivos de clientes morosos y registro de millones de pasos por peajes desde febrero a septiembre de este año, tal como **reporta el periodista Juan Pablo Carranza en La Voz del Interior.**

Ruiz no tocó esos archivos y de inmediato dio la voz de alerta a la empresa responsable de la gestión de los mismos. Esto es una práctica habitual y suele ser bien recibida por empresas que tienen interés real en proteger los datos que administran. No es el caso de Caminos de las Sierras. La empresa no dio respuesta a la alerta ni tomó recaudo alguno sobre los datos. Ante la preocupación por tal suceso, Ruiz acudió a la prensa.

La comunicación de este tipo de hechos a la prensa suele ser el último recurso, a veces desesperado, ante la falta total de responsabilidad de las empresas y organismos que deben custodiar datos de la ciudadanía. Exponer el hecho es la única forma de lograr que alguien se tome en serio la tarea de mantener la seguridad de la información con la que cuentan estos servicios. Vale mencionar que tras la publicación del hecho, Ruiz se puso a disposición de la empresa para colaborar en la solución del problema que había detectado y se reunió con los equipos técnicos para mostrarles exactamente cuál era el inconveniente. La empresa salió del paso diciendo que los datos estaban ya bajo resguardo. Pero luego fueron a la justicia e iniciaron una causa penal por un hecho del que sólo la empresa es culpable.

Este viernes, Ruiz fue allanado en su domicilio por la Justicia Provincial y por solicitud del fiscal especializado en cibercrimen Franco Pilnik. El allanamiento duró 8 horas y fue una pesadilla para Ruiz y su familia. Según indicaron fuentes cercanas al especialista, los policías que llegaron a su domicilio peritaron sus equipos en busca de la información supuestamente bajada de la base de datos de la RAC.

Todo lo que no se debe hacer y todo lo que está mal está presente en este caso.

En primer lugar, hablamos de una empresa estatal negligente con los datos que recopila, ya que la vulnerabilidad reportada por Ruiz es básica y carente de cualquier sofisticación. Nadie sabe además, desde cuándo esos datos estaban expuestos, por lo que la magnitud del impacto es imposible de medir. La primera y mayor responsabilidad aquí está en cabeza de la propia empresa, cuya negligencia extrema deja en riesgo los datos - y con ellos la privacidad y la seguridad - de más de 54 mil usuarios de sus servicios.

Es indispensable que las autoridades de protección de datos personales cuenten con mayores mecanismos de investigación y acción contra empresas negligentes que no cumplen protocolos mínimos de custodia de los datos. Sin una autoridad de aplicación de la ley de protección de datos, y con la total impunidad que les da ponerse en un lugar de víctimas en lugar de hacerse cargo de sus responsabilidades, las empresas y reparticiones públicas seguirán afectando gravemente la integridad de la información de la ciudadanía.

En segundo lugar, la propia empresa denuncia un ataque cuando se trata de una típica situación de negligencia. En lugar de agradecer el reporte y resolverlo, la denuncia penal de un hecho que es pura y exclusiva responsabilidad de la empresa es un despropósito.

En tercer lugar, una fiscalía y un juez que hacen lugar a una investigación en la que claramente no hay delito alguno. De hecho, si hubiera algún delito (cosa que habría que revisar en detalle), debería investigarse el accionar negligente de la propia empresa. Lo que hizo Ruiz no debería calificarse de delito bajo ninguna circunstancia, sin embargo el acceso indebido a los sistemas de información es considerado un delito desde la **reforma del código penal que incorporó los denominados delitos informáticos en 2008**.

Ya en aquellos años, desde Fundación Vía Libre nos opusimos a la creación de figuras penales abiertas que pudieran poner en riesgo la tarea de investigación de vulnerabilidades y de infosec. Temíamos que ocurriera lo que efectivamente está ocurriendo ahora. Muchos abogados nos salieron al cruce diciendo que la aplicación del tipo penal iba a ser hecha por juristas que entenderían las diferencias entre reportar una vulnerabilidad y atacar un sistema informático, pero lo que está ocurriendo en demasiadas oportunidades nos da la razón. Fiscalías supuestamente especializadas en delitos informáticos avanzan sobre investigadores de infosec sin las mínimas salvaguardas, avanzan sobre sus vidas privadas, allanan sus domicilios e incautan sus instrumentos de trabajo sin fundamento alguno. El Caso Smaldone es un gran ejemplo. Hace un año lo allanaron, detuvieron por varias horas y expropiaron todos sus equipos de trabajo sin siquiera imputarlo por delito alguno.

El Código Penal sanciona el acceso por cualquier medio, sin la debida autorización o excediendo la que posea, a un sistema informático de acceso restringido. La pena se agrava cuando el acceso fuese en perjuicio de un sistema o dato informático de un organismo público estatal o de un proveedor de servicios públicos o de servicios financieros.

En este caso, la vulnerabilidad reportada por Ruiz estaba ahí, a la vista de cualquier persona que fuera mínimamente perspicaz. ¿Podemos afirmar que un sistema que está abierto totalmente por negligencia de una empresa es un sistema de acceso restringido? Por supuesto que Ruiz no tenía autorización para ver esos archivos, pero ¿qué es lo que corresponde hacer ante un hallazgo de este tipo? Por supuesto, reportarlo y contribuir en la solución del problema.

Lo que están logrando empresas, fiscales de delitos informáticos y jueces que allanan al mensajero es desincentivar el reporte de vulnerabilidades, una tarea fundamental en una sociedad donde intercambiamos datos permanentemente y la seguridad de los mismos es una cuestión central.

Al próximo investigador y practicante de infosec que encuentre una vulnerabilidad como esta no le van a quedar ganas de reportar, y los datos de la ciudadanía seguirán expuestos una y otra vez por negligencia y arbitrariedad.
¿Imaginen si cada vez que un periodista investiga y encuentra un hecho de corrupción es allanado por sospechas de complicidad o se lo acusa por el hecho reportado? La tarea de Infosec necesita ser protegida, garantizada y promovida porque de ella depende la seguridad de la información. El reporte de vulnerabilidades debe ser garantizado tanto como protegemos la libertad de expresión y la atención apropiada de los reportes debe ser una exigencia a todas las empresas y organismos públicos que gestionan datos de la ciudadanía.

El efecto intimidatorio de estos allanamientos tiene consecuencias nefastas y deben ser considerados ataques por parte del Estado a la libertad de expresión y al acceso a la información. Fiscales y jueces que cubren con complicidad a empresas negligentes no nos brindan seguridad, sólo garantizan impunidad a los verdaderos responsables y castigan una tarea fundamental como la práctica de la seguridad de la información.

El voto electrónico no es seguro como el conteo tradicional en papel

VER EL NEWSLETTER COMPLETO

En las últimas horas hemos escuchado esta declaración muchas veces. No se trata de volver a repetir lo que desde Vía Libre enfatizamos hace más de 17 años sino de encender cualquier medio de comunicación y escuchar declaraciones de altos funcionarios de la administración Trump y líderes de opinión que se niegan a confiar en el sistema electoral de los EEUU. Más allá del resultado electoral en ese país, esta enfática afirmación hecha por el columnista conservador Tucker Carlson en Fox News, retuiteada inmediatamente por el Presidente Donald Trump en su popular cuenta de esa red social, debería llevarnos a una inmediata reflexión.

Tras las elecciones del 3 de noviembre, la política norteamericana ha dado infinidad de notas que podrían ser desopilantes sobre el sistema de voto electrónico, si no fuera porque lo que se juega es el sistema electoral de uno de los países más poderosos del planeta.
En estos días, la empresa Smartmatic volvió al centro de la escena. Las acusaciones de fraude y manipulación electoral están a la orden del día. Cualquier declaración picante sirve para completar un cuadro en el que se apunta sin pudor a socavar la confianza en el sistema electoral. Sin tapujos, se escucha a políticos de alto nivel como Rudolf Giuliani esbozar teorías conspirativas de todo color, que incluyen una afirmación de gravedad institucional inusitada sobre la contratación de la firma de origen venezolano para manipular las elecciones presidenciales de 2019 en Argentina. Por más desopilante que suene, como en todo proceso de construcción de una campaña de desinformación, las mentiras se construyen sobre verdades parciales. Smartmatic fue contratada en forma poco transparente, no hubo auditorías suficientes ni apropiadas y se reportaron severas vulnerabilidades al sistema usado para el escrutinio provisorio. Lo fundamental es que la firma sólo pudo intervenir en ese proceso y no en el fondo de la elección, no intervino en la emisión y conteo definitivo y por lo tanto, su intervención jamás hubiera podido tener repercusión legal efectiva. Gracias a la gran comunidad de seguridad de sistemas de información y a la enorme acción de la campaña #NoAlVotoElectrónico en 2016, pudimos rescatar y sostener la credibilidad en nuestro sistema electoral.

Lo cierto de toda esta historia que atrapa a la opinión pública en los EEUU, es que este tipo de afirmaciones y declaraciones temerarias es posible porque Tucker Carlson tiene razón: no se puede confiar en las máquinas de votación. El sistema de votación electrónico no es tan seguro como el viejo y tradicional sistema de conteo manual. Lamentablemente, esta coyuntura no es la más apropiada para dar un debate sobre el sistema electoral de los EEUU, pero bien podríamos aprovechar la oportunidad para volver a discutir los instrumentos electorales en nuestro país y en la región.

Desde que se realizó la primera prueba piloto de voto electrónico en Ushuaia, en el año 2003, Argentina ha transitado idas y vueltas en la incorporación de tecnologías al proceso electoral. Ya desde entonces, en Vía Libre adoptamos una posición contraria a la votación mediada por computadoras, incluso en sistemas que arrojan comprobante en papel. Entendimos muy tempranamente, junto con buena parte de la comunidad global de seguridad de sistemas de información, que la mediación informática supone una caja negra en el proceso, importa numerosos riesgos nuevos para los que el sistema político y el aparato electoral no están preparados y supone una incapacidad casi absoluta de arbitrar medios apropiados para el control de la elección.

En una elección mediada por computadoras, las denuncias que puedan socavar el proceso electoral siempre van a ser verosímiles, ya que es imposible corroborar la integridad de la elección y garantizar el secreto del voto. En un escenario de este tipo, el sistema se presta para casi cualquier tipo de operación, legítima o no, que no podrá ser corroborada, pero tampoco desmentida. Este escenario socava el sistema democrático y es una de las razones por las cuales siempre insistimos con la negativa a votar con computadoras.

Argentina se debe un buen debate y la construcción de consensos apropiados para una reforma sólida del sistema electoral. Lamentablemente, el proyecto planteado por el gobierno de Mauricio Macri en el año 2016 fue más un capricho por la implementación de voto electrónico que una propuesta seria de solución a los problemas que tiene el sistema electoral argentino, problemas que sin dudas son menores comparados con los que se hubieran originado de avanzar la reforma electoral con votación electrónica.

El primer consenso al que deberíamos arribar es a no pretender arreglar lo que no está roto. El sistema electoral argentino, pese a una pequeña cantidad de denuncias infundadas o menores, no tiene problemas estructurales serios. Ninguna elección presidencial ha sido cuestionada desde el restablecimiento de la democracia. Las denuncias que hemos escuchado muchas veces tienen que ver con delitos electorales pero no con un fraude que impacte en el resultado de una votación. La más común y reiterada de las críticas al sistema electoral es la posibilidad del robo de boletas y el alto costo de reposición de las mismas. Ambas situaciones se subsanan de manera sencilla con la implementación del sistema electoral más probado y usado en todo el mundo, la boleta única en papel.

Por supuesto, el sistema político podría darse debates sobre la representación proporcional, las listas sábanas, la realización de internas abiertas obligatorias, la ley de lemas o muchos otros aspectos que exceden la misión de Vía Libre y los tópicos a los que dedicamos nuestro trabajo. Sin embargo, ninguno de estos temas tiene directa relación con el instrumento electoral ni se soluciona con falsas promesas de modernidad electrónica.

Lamentablemente, la crítica al sistema de votación electrónica se usa hoy como un instrumento más para socavar y deslegitimar procesos electorales cuyo resultado es difícil de aceptar para diversos sectores, especialmente de la Administración Trump. Pero esta coyuntura no puede ocultar el hecho de que esta estrategia es posible porque efectivamente el sistema electoral mediado por estas tecnologías deja mucho que desear.

En la región, Paraguay se apresta a utilizar sistemas electrónicos en las próximas elecciones en 2021. Entendemos que nuestro país hermano del Mercosur está a tiempo de cambiar de rumbo e implementar un sistema que habilite el control público, promueva la transparencia electoral y respete la integridad y el secreto del sufragio.

En Argentina, algunas provincias que fueron pioneras en la materia están avanzando en el sentido contrario, tal como parece ser el caso de la provincia de Salta, que tras muchos años de experimento de votación electrónica está considerando volver a votar con sistemas tradicionales de voto impreso en papel. Si esto se confirma, habremos de celebrar un logro importante de colegas de Salta que vienen dando esta discusión desde hace años en esa provincia que se caracterizó por muchos años por ser más un agente de marketing de una empresa proveedora de sistemas de votación electrónica que una garantía para la ciudadanía y su derecho a votar.

Nuestro país tiene elecciones de medio término en 2021. Sabemos que algunos legisladores insisten con proyectos insólitos de votación electrónica, pero confiamos en la madurez del sistema político argentino que hasta el momento ha mantenidos las razonables dudas como para no avanzar en un sistema inviable a la hora de votar. Esperamos además que la Ciudad Autónoma de Buenos Aires tampoco vuelva a la experiencia de votación electrónica, ya que lamentablemente la legislatura de la Ciudad, con la aprobación del código electoral le ha dado lugar a tamaña irresponsabilidad.

Vía Libre cumple 20 años

VER EL NEWSLETTER COMPLETO

"Compartiendo la riqueza intelectual" fue la primera frase que identificó nuestra organización allá por el año 2000 cuando la Inspección de Personas Jurídicas de Córdoba aprobó la conformación de la "Fundación para la Difusión del Conocimiento y el Desarrollo Sustentable Vía Libre" tras la iniciativa de dos cordobeses: Daniel Polzella Cano y Federico Heinz, fundadores de la organización.

Cuentan los viejos que el nombre original iba a ser Fundación Bruno Diaz, que hasta se había reservado un dominio acorde y todo. Pero primó algo de cordura y finalmente la organización se terminó llamando todo eso que figura en el estatuto. Fundación Vía Libre para los amigos (amigas y amigues hoy). Con un logo que parecía más un aviso de una maternidad y rudimentos de comunicación humana, en un mundo integrado por geeks que propalaban chistes nerds de dudosa calidad, la Fundación inició su periplo hasta nuestros días.

Pensada como una organización emergente de la comunidad de Software Libre de Córdoba, pero con vínculos en todos los grupos de usuarios del país, Vía Libre se dedicó de lleno a la difusión, promoción y desarrollo de Software Libre, incluyendo la idea peregrina de tratar de contribuir al desarrollo de políticas públicas de uso de Software Libre en el Estado. Esta fue, quizás, la meta más ambiciosa de aquellos primeros años en los cuales el software libre no era tan popular y fácil de usar como es hoy.

Desde las viejas oficinas que supimos (y no supimos) mantener en Córdoba se hicieron infinidad de cosas: desde cursos de software libre, encuentros de Grulic, se montó un telecentro con acceso a todo el mundo, se hicieron proyectos locales, nacionales y hasta una buena cantidad de intervenciones a nivel internacional. La hermandad y cooperación con organizaciones internacionales siempre fue una fortaleza que pudimos profundizar con el correr de los años. Estuvimos en cuanto encuentro de Software Libre se hizo en los últimos 20 años, y compartimos infinidad de anécdotas y desafíos con esa comunidad de la que somos y seremos siempre parte.

Pero con el correr de los años, el Software Libre fue indispensable más no suficiente. Abrimos numerosos frentes de trabajo, siempre bajo la idea de promover tecnologías más justas, apropiadas socialmente, con una mirada de autonomía y fundamentalmente con respeto a los Derechos Humanos.

Cuando Ushuaia probó por primera vez un sistema de voto electrónico, allá en el 2003, nos alineamos a los amigos de Tierra del Fuego para dar esa pelea, tras lo cual abrimos un eje permanente de trabajo sobre tecnologías electorales. Quizás este sea el eje que más nos ha desafiado pero el que reivindicamos como aquel en el que hemos tenido más éxito. Tuvimos que aprender sobre derecho electoral, rodearnos de organizaciones vinculadas a la política, dialogar con partidos y juristas, todo un campo nuevo para nuestra organización. Hoy, sentimos que nuestro trabajo ha sido una fuente clave en la construcción del consenso amplio de #NoAlVotoElectrónico en Argentina y en la región.

También aprendimos que la Convergencia con otros movimientos sociales era esencial para la discusión sobre propiedad intelectual de la que tanto hemos participado. Sin entender los demás aspectos de un tema global que involucra al comercio internacional y muchas otras áreas de la vida como la salud y la soberanía alimentaria no hubiéramos podido construir el trabajo de más de 15 años en seguimiento de la agenda de copyright y patentes. Desde ahí, nos forjamos una trayectoria en el seguimiento de las negociaciones de Comercio Internacional, un campo que superó con creces nuestro primer abordaje de la tecnología.

Sumamos también el área de la defensa del derecho humano a la intimidad, a la protección de datos personales y a la autodeterminación informativa como elementos centrales para la defensa de los derechos individuales, las libertades públicas y la autonomía de las personas. En este eje aprendimos además, junto a

organizaciones amigas y colegas, que la defensa de derechos humanos en ámbitos mediados por tecnologías necesita profundizar en esos entornos más allá de las tecnologías. Así, terminamos metidos en debates sobre reformas procesales, servicios de inteligencia, investigación criminal, derecho penal, escuchas e interceptaciones de comunicaciones, legislación sobre temas de criminalidad compleja, acuerdos internacionales y muchos otros temas de los que hemos aprendido de la mano de organizaciones colegas con las que trabajamos intensamente en los últimos años. No podemos olvidar también la incorporación de numerosos debates sobre regulaciones de internet, telecomunicaciones, medios de comunicación, que nos han desafiado a pensar más allá de lo obvio para buscar formas de promover, ante todo, los derechos de la ciudadanía. Y asi, con esos derechos como eje central de nuestra agenda, abordamos otros temas desafiantes de nuestro tiempo, como los nuevos temas vinculados al impacto de la Inteligencia Artificial, las decisiones mediadas por algoritmos, las nuevas relaciones laborales, las características propias del capitalismo post-industrial y muchos otros temas que convocan hoy nuestra agenda cotidiana.

Nada de esto sería posible sin la permanente ayuda y apoyo de un gran numero de amigos y amigas que forman parte del círculo cercano de Vía libre, que comparten visión, agendas y con quienes muchas veces debatimos para construir posiciones más sólidas. Nada de esto sería posible sin los organismos internacionales que confían y apoyan nuestro trabajo de forma sistemática y nos han permitido llegar a este extraño y dramático 2020 con una agenda llena de proyectos. Y así, nos disponemos a iniciar nuestros próximos 20 años con una cantidad de iniciativas y proyectos que nos llenan de satisfacción.

Hace muchos años, un directivo de una ONG de larguísima trayectoria en el tema ambiental me decía que una organización madura y se consolida recién cuando logra sostenerse por 20 años. Acá estamos. No se si maduramos. Pero trabajar, seguro que lo hacemos y mucho.

¡¡No hay mucho que decir más que Muchas Gracias a quienes pasaron, aportaron, discutieron, rieron, imaginaron y construyeron!! Y especialmente, a quienes nos han marcado el camino. Por eso, queremos dedicarle estos 20 años a la memoria de nuestro querido amigo Marcelo Baldi.

Por Vía Libre, 20 años y muchos más!!

¡Muchas gracias!

Diciembre

10 de diciembre. Día Internacional de los Derechos Humanos

VER EL NEWSLETTER COMPLETO

Cada 10 de diciembre es especial para la República Argentina. El mismo día de la recuperación de la Democracia allá por el año 1983 coincide con la que, a nuestro modo de ver, debería ser la celebración más importante que une a los diversos países del mundo: El Día Internacional de los Derechos Humanos.

Ese día se cumple un nuevo aniversario de la consagración de esa carta de principios que define de forma concreta y clara los consensos más profundos alcanzados por la humanidad hasta la fecha. Un 10 de diciembre de 1948, tras dos masacres en las cuales la humanidad testificó la crueldad y la violencia de un modo nunca antes visto, los países acordaron una visión para que esa barbarie no se vuelva a repetir.

En pleno siglo XXI, esa **Declaración Universal de los Derechos Humanos** que consagra la libertad, la justicia y la paz en el mundo, basadas en el reconocimiento de la dignidad intrínseca y la igualdad de derechos inalienables para todas las personas que componen la gran familia humana deben ser puestos sobre la mesa y estar más vigentes que nunca.

A lo largo de los años hemos presenciado catástrofes que afectaron los Derechos Humanos en diversos países del mundo, incluyendo las cruentas dictaduras en nuestra región latinoamericana. Es el derecho de toda la ciudadanía y el deber ineludible de los Estados hacer cumplir esas pautas y garantizar el respeto de la dignidad de las personas en todas sus prácticas humanas.

Aún falta mucho trabajo para el pleno respeto y cumplimiento progresivo de estos derechos que fueron incorporados a la Constitución Nacional Argentina en la reforma de 1994. Incluidos en el artículo 75, inciso 22, los Derechos Humanos son la matriz sobre la cual debemos trabajar día a día y cumplir los compromisos asumidos no sólo con los organismos internacionales, sino y muy especialmente con la ciudadanía.

En épocas complejas como la que nos toca transitar, la vara de nuestras acciones siempre debe estar en línea con los Derechos Humanos. Son tiempos de creciente conflictividad, con una polarización creciente en las sociedades, con medidas de excepción en un año totalmente atípico para la humanidad, sólo el marco jurídico de los Derechos Humanos nos permitirá superar las complejidades de nuestro tiempo.

En este mes de diciembre de este atípico 2020 y habiendo cumplido nuestros primeros 20 años de vida como institución, desde Fundación Vía Libre queremos celebrar el día internacional de los Derechos Humanos con el compromiso de seguir trabajando por los derechos de la ciudadanía y la dignidad de las personas en el campo que nos toca.

Nuestro compromiso para la comunidad de la que somos parte: seguir promoviendo debates, defendiendo libertades y derechos, a favor del avance progresivo de los Derechos Humanos como consenso fundamental para construir sociedades justas, equitativas, libres en las cuales promover y defender la dignidad de las personas. En esta semana de los Derechos Humanos, este es nuestro compromiso.

¿Y si Google dejara de funcionar?

VER EL NEWSLETTER COMPLETO

Esta mañana del 14 de diciembre Google y Gmail aparecieron como tendencia en las principales redes sociales. Una caída masiva de servicios había dejado fuera de línea los principales productos de la gran empresa tecnológica de la que depende casi todo el mundo (no todos, obviamente). Imposibilidad de acceder a correos, documentos, archivos, planillas, empresas enteras cuyo funcionamiento depende de los servicios en la nube de la gran empresa tecnológica global. Años atrás, la pesadilla de la quiebra o la pérdida de información tenía otro nombre: Microsoft. Hoy, el gigante del que depende todo el mundo es Google.

Se trata de fenómenos paralelos que demuestran que una de las más grandes preocupaciones en el campo informático sigue tan vigente como nunca: la enorme concentración de un mercado del que dependen no sólo las comunicaciones personales, sino los servicios sobre los que trabajan infinidad de empresas pequeñas, medianas y grandes. La productividad de buena parte del mundo occidental depende hoy de que funcione una sola empresa.

Desde el movimiento de Software Libre venimos alertando desde hace años sobre el impacto que supone la falta de diversidad en materia de servicios informáticos, sobre la dependencia de un puñado de empresas de tecnología y sobre la necesidad de crear capacidades y autonomía para el uso de la informática.

Lo cierto es que, a partir de las crecientes preocupaciones por la privacidad de los datos y el auge del concepto de soberanía tecnológica, no son pocos los que han empezado a plantear los problemas inherentes a la utilización masiva de servicios como los que provee Google. Sin embargo, estas dos cuestiones no son más que significantes vacíos si no se acompañan de políticas y estrategias concretas de acción.

La comunidad de Software Libre viene advirtiendo que el software como servicio supone una amenaza a la libertad de las personas y la autonomía de las organizaciones. **El propio Richard Stallman lo sintetizó hace muchos años al expresar que 'nunca podremos tener control sobre los servicios que un tercero provee'.**

El marketing de estos servicios lo presenta habitualmente como servicios en la nube, básicamente, un eufemismo para definir servicios montados sobre la computadora de otros, tal como claramente expresó Evgeny Morozov. Es bastante impresionante ver cómo estos servicios se han ido concentrando cada vez más en muy pocas manos y cómo las personas que usamos computadoras para comunicarnos y trabajar dependemos cada vez más de servicios que de otra forma hubiéramos bien podido administrar por nuestra cuenta. No se trata de no usar absolutamente nada de ellos, sino tener la capacidad de generar autonomía frente a ellos y seleccionar lo que hacemos o dejamos de hacer.

En buena medida, el sistema económico actual de internet que Shoshana Zuboff denominó capitalismo de vigilancia se basa especialmente en que dependamos cada vez más de este tipo de servicios que sirven fundamentalmente para cosechar datos. Sin embargo, desde empresas tecnológicas hasta ONGs, pasando también por oficinas estatales depositan sus datos y servicios en manos de muy pocas empresas de las que hoy depende buena parte de lo que hacemos en línea.

Es claro que empresas como Google o Amazon tienen la capacidad instalada de solucionar problemas rápidamente y ofrecen una estabilidad y seguridad de servicios envidiable. Sin embargo, esto no debe hacernos perder de vista que un colapso en sus sistemas puede implicar la paralización de múltiples sectores cuya infraestructura depende de un puñado de empresas.

De nada sirve llenarse la boca con el discurso de la soberanía tecnológica tan de moda actualmente si no se desarrollan dos procesos que son anteriores a ese logro: la creación de capacidades y la construcción de autonomías. Sin capacidades instaladas, ya sea para el Estado como para los múltiples sectores productivos de una sociedad, difícilmente se logre la autonomía fundamental que se requiere para independizarse de esos servicios.

No se trata tampoco de un planteo contracara del actual: que el Estado se hiciera cargo de la nube, como se sugiere muchas veces como solución al problema de la concentración de la industria tecnológica, o de la obligación de hospedar los datos en centros de datos que maneje el propio estado. Se trata de diversificar y crear capacidades para lo cual el Estado tiene un rol central, que no necesariamente implica reemplazar al monopolio empresarial de turno por un monopolio estatal.

El software libre viene planteando esta cuestión desde hace más de 35 años ya y siempre se ha topado con las mismas dicotomías engañosas. Son múltiples los actores que tenemos que trabajar para construir un ecosistema informático más justo, equitativo, viable económicamente saliendo de la dicotomía de depender completamente de una empresa o depender del Estado. La creación de capacidades supone necesariamente la educación en software libre pero a su vez también la creación de una demanda de servicios para que funcione una multiplicidad de servicios ofrecidos por empresas pequeñas, medianas, cooperativas e iniciativas de todo tipo que puedan brindar soporte, mantener servicios y proveer la infraestructura para generar autonomías.

Es claro que no podemos reemplazar todos los servicios que nos brindan las grandes compañías tecnológicas, pero es necesario comenzar en algún punto a generar políticas de fomento y un mercado de acceso a servicios que permitan avanzar en ese sentido. A su vez, adoptar servicios de otros proveedores de búsqueda, de documentos compartidos, montar servidores propios en cooperación, contratar soporte local. En definitiva, invertir en aquellos que pueden proveernos servicios que nos habiliten a manejar nuestra propia infraestructura.

Porque como bien decimos desde el software libre, la libertad nunca ha sido gratis. Tampoco es gratis ceder todo el control a un puñado de empresas que dominan el mercado más concentrado del que tengamos memoria. Para solucionar esto no sólo hacen falta Estados capaces de hacer cumplir las regulaciones antimonopolios, también hacen falta ciudadanos capaces y con la voluntad de recuperar el control.

Requisitos mínimos para una política de seguridad de la información en la Administración Pública Nacional

VER EL NEWSLETTER COMPLETO

La semana pasada, el Director Nacional de Ciberseguridad Gustavo Sain anunció el desarrollo de los 'Requisitos mínimos para las políticas de seguridad de la información de los organismos de la APN' que fueron elevados a las autoridades competentes para su pronta aprobación. Desde Fundación Vía Libre contribuimos a la tarea de formular estos requisitos porque entendemos que es urgente una política apropiada de protección y custodia de los activos digitales en poder del estado, en particular, cuando se trata de infraestructuras críticas y de datos personales de la ciudadanía.

En numerosas ocasiones en este mismo espacio y en otros ámbitos donde participamos activamente, hemos criticado con énfasis la negligencia del Estado a la hora de custodiar datos personales de la ciudadanía. Recordamos en forma permanente que los datos de todos los habitantes de la Nación que el Estado administra no le pertenecen y que es su obligación y responsabilidad la protección de los mismos.

Hace años venimos dando vueltas con el tema. Sin ir más lejos, siendo Jefe de Gabinete de Ministros, quien hoy es Presidente de la Nación, el Dr. Alberto Fernández, estampó su firma a la **Resolución 669/2004 'Política de Seguridad de la Información'** que establecía que el Sector Público Nacional debería dictar o adecuar sus políticas de seguridad, conformár comités de seguridad de la información y generar políticas claras en la materia, incluyendo metodologías y procesos relativos a la seguridad, evaluaciones y asegurar la continuidad de esas políticas.

Mucha agua ha corrido bajo este puente en el Estado Argentino, pero lo cierto es que a pesar de algunas

declaraciones rimbombantes a lo largo de los años, la infraestructura de seguridad de la información en la Administración Pública está lejos de cumplir con estándares mínimos apropiados.

Hemos hablado varias veces ya sobre la necesidad de tener una política, protocolos de acción, equipos sólidos desde lo técnico pero también desde lo político que permitan dar cuenta de la importancia que tiene la seguridad de la información en poder del estado. Dotar al área de Ciberseguridad de recursos apropiados y muy especialmente de respaldo político que le permita fijar una línea de acción que sea adoptada, respetada y promovida como política de Estado en toda la administración pública.

Basado en la Decisión Administrativa 669/04, se elevó a las autoridades el proyecto de requisitos mínimos de una política de seguridad de la información para los organismos públicos. El objetivo es establecer lineamientos generales, mínimos y de cumplimiento obligatorio para los organismos del sector a fin de proteger los activos de información frente a los riesgos que pudieran comprometer la seguridad de los mismos, proteger la confidencialidad, integridad y disponibilidad de los datos.

En este sentido, es indispensable proteger los derechos de los titulares de los datos personales que administra y trata el sector público, la información y los datos del conjunto de organismos del estado y promover una política responsable y rigurosa en materia de seguridad de la información.

Parece una obviedad, pero está lejos de serlo en un Estado en el que las áreas que se ocupan de esta tarea carecen del presupuesto suficiente y la entidad administrativa necesaria para cubrir un área fundamental de los estados modernos. No es nuestra voluntad compararnos aquí con las áreas equivalentes en países como Francia, Alemania o Nueva Zelanda. Antes de romper en llanto, es menester reconocer las limitaciones vigentes y activar de forma urgente los mecanismos posibles para la construcción, adopción e implementación de una política real en la materia. Una política real no se queda en declaraciones, sino que invierte en formación, establece presupuestos apropiados, ejerce autoridad sobre el campo y fija lineamientos de riguroso cumplimiento.

Desde Vía Libre entendemos que esta tarea es urgente, mucho más que ponerse a desarrollar una base de datos de salud centralizada o seguir atajando crisis como la generada por el ataque a la base de datos de Migraciones hace pocos meses.

La protección de los datos de la ciudadanía es una obligación del Estado y el avance en estas políticas es apenas el primer paso que celebramos con énfasis y esperamos pronto sea aprobado por las autoridades del área competente.

Otro tema abierto en las últimas horas es la urgente definición de quién asumirá el cargo de Director Nacional de Acceso a la Información Pública que el Dr. Eduardo Bertoni deja vacante a partir del 1 de enero del próximo año. Una vez más, repetimos que es necesario revisar la arquitectura institucional a cargo de la protección de datos personales para dotarla de las capacidades necesarias para el cumplimiento de la misión de proteger los datos de la ciudadanía, tanto frente al sector público como al privado.

Ambos temas requieren respuestas apropiadas en el corto plazo. Desde Fundación Vía Libre asumimos una vez más el compromiso de acompañar el debate y la construcción de políticas públicas para la defensa de los derechos y la protección de los datos de la ciudadanía en poder del Estado.

Anuario Vía Libre 2020

VER EL NEWSLETTER COMPLETO

En este atípico 2020, nuestra organización cumplió 20 años de existencia. Desde aquel Noviembre del año 2000 pasaron infinidad de cosas, proyectos, experiencias, aprendizajes, trabajos, colaboradores y amistades de todo tipo.

Arrancamos hace 20 años con la convicción de que el Software Libre y su filosofía eran un camino importante a seguir para asegurar la autonomía, la libertad y los derechos de las personas en el uso de computadoras.

Esa perspectiva que marcó nuestros primeros pasos creció hasta consolidar al día de hoy una misión que nos obliga a abordar temas más complejos y a trabajar intensamente en todas las áreas de intersección entre los Derechos Humanos y las Tecnologías de Información y Comunicación.

En este largo proceso de maduración de visiones y proyectos, este 2020 nos encontró con una agenda de temas que impactan de lleno en la ciudadanía: las regulaciones de Internet, los avances sobre la privacidad de las personas, la protección de datos y las políticas de vigilancia, las discusiones sobre propiedad intelectual y acceso a conocimiento, la necesidad de poner un ojo crítico en la incorporación de sistemas de inteligencia artificial en la vida social, la autodeterminación informativa, la libertad de expresión, los derechos electorales y muchos otros aspectos que convocaron nuestra atención.

Este 2020 fue un año complejo, que afectó la vida de millones de personas en todo el mundo, que expuso como nunca antes las desigualdades y las injusticias, que nos obligó a ser más responsables que nunca, que nos puso frente a procesos de cambio y adaptación brutales y nos llevó a hacer más trabajo que nunca en nuestros temas de agenda. Este año nos obligó a adaptarnos a una coyuntura que no nos había tocado vivir nunca antes y a seguir construyendo un mundo basado en el respeto y promoción de los Derechos Humanos.

En el cierre de este año, en este contexto que promete no cambiar demasiado a partir del 2021, construimos este anuario que sintetiza lo hecho en estos últimos 12 meses en los que todo cambió pero seguimos trabajando.

Este anuario que compartimos hoy con ustedes es una muestra de esfuerzo, resiliencia, adaptación y nos ayuda a visualizar la enorme cantidad de actividades realizadas en este año atípico. Nada de lo hecho sería posible sin un equipo dedicado y riguroso y sin el apoyo de quienes nos acompañan día a día para cumplir nuestra misión. A ellos, infinito agradecimiento.

Recibimos el fin de año con la triste noticia del fallecimiento de nuestra ex tesorera, pero por sobre todo querida amiga, María Elena Casañas, en cuya memoria seguiremos trabajando siempre con la tenacidad y la alegría que nos supo transmitir en **cada momento que pasó junto a nosotros en Vía Libre**.

En este 2020, este es el trabajo que hicimos y queremos compartir con ustedes junto a los mejores deseos para el 2021. Desde Fundación Vía Libre les deseamos un muy feliz año nuevo.

Fundación
Vía Libre

info@vialibre.org.ar

twitter.com/FViaLibre

youtube.com/FundacionViaLibreOficial

vialibre.org.ar