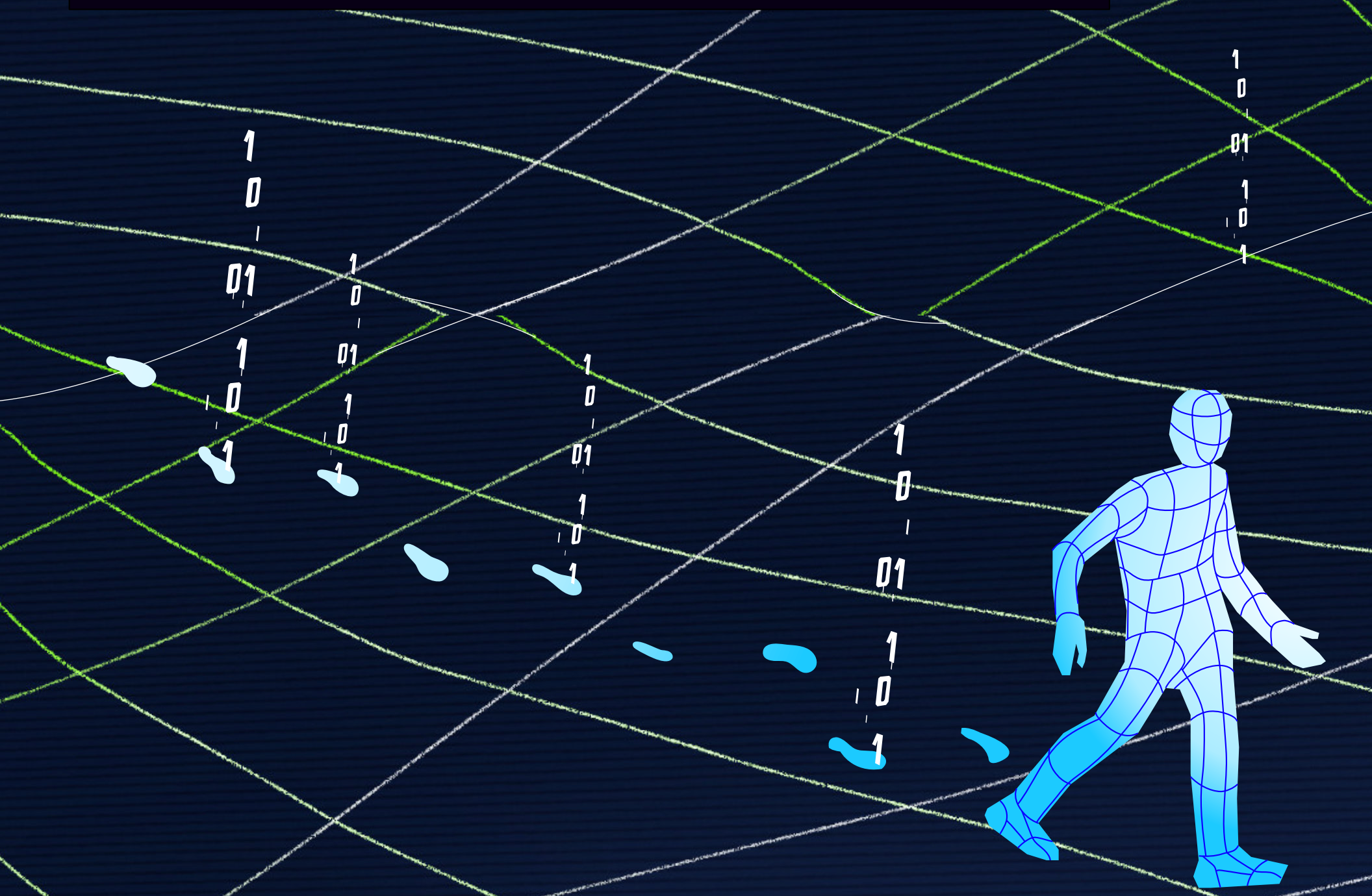
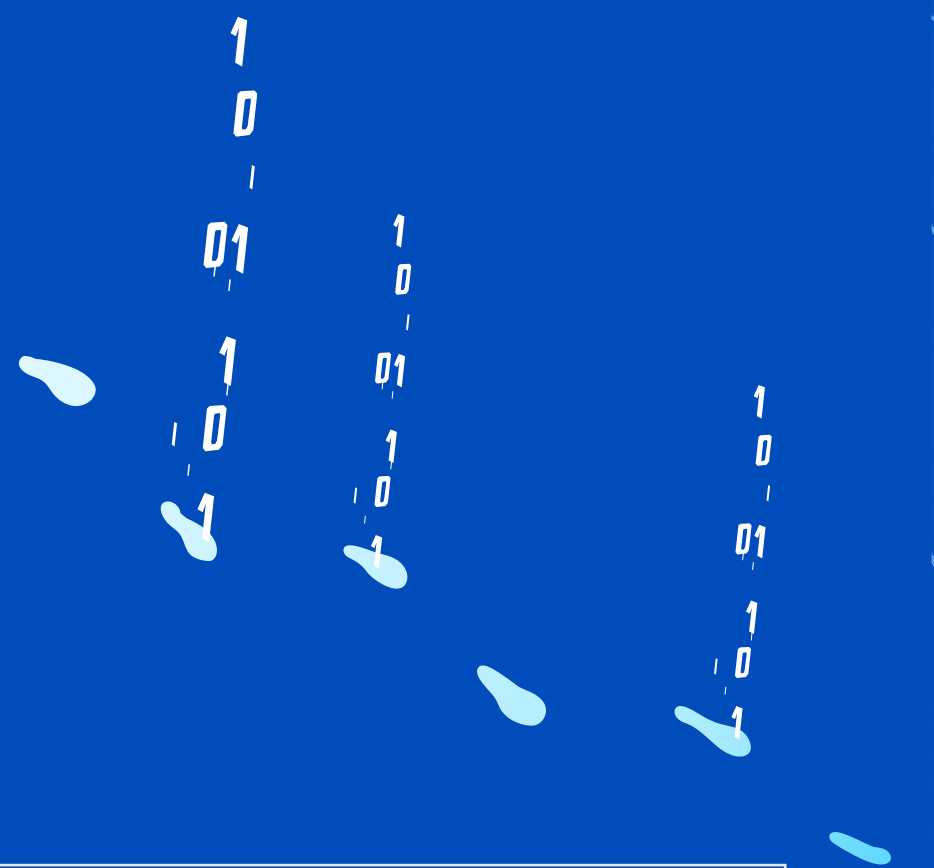
Rastros Digitales

¿Cuántos datos has dejado en la red?

Condiciones de la privacidad e información personal de los usuarios en internet



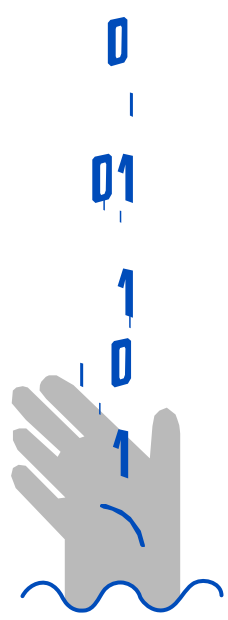
Instituto Prensa y Sociedad Venezuela



"La información personal es cualquier dato relacionado a ti, ya sea que se refiera a tu vida privada o pública. En el entorno en línea, donde una vasta cantidad de información es compartida y transferida alrededor del mundo de forma inmediata, se hace cada vez más difícil para las personas mantener un control sobre su información personal".

Access Now,
organización internacional dedicada a los derechos humanos, la política pública y el activismo por la defensa del Internet abierto y libre.

Rastros digitales: ¿Cuántos datos has dejado en la red?
Condiciones de la privacidad e información personal de los usuarios en internet



¿SOMOS DUEÑOS DE NUESTROS DATOS?

En su libro Leviatán, el filósofo Tomas Hobbes afirma que “quien tiene la información, tiene el poder” y aunque esta frase puede sonar desgastada y hasta cliché, esconde algo de verdad. Incluso en ámbitos como Internet que era prácticamente imposible considerar en la época en que fue escrita dicha obra.

Actualmente, la información se puede transformar en poder económico o incluso político, las grandes empresas de tecnología como Meta (anteriormente Facebook), Alphabet (anteriormente Google) y Amazon generan miles de millones de dólares a través de la recolección, el almacenamiento y el procesamiento de datos de sus usuarios, los cuales son utilizados para ofrecer servicios como publicidad a otras compañías.

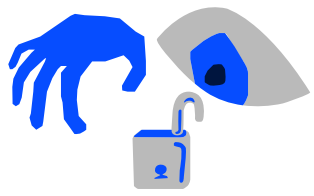
Pero no solo las empresas se benefician de la recolección de datos, ya que la información que se genera a partir de estos también puede permitir a los Estados aumentar el control sobre la población. El peligro es aún mayor en contextos autoritarios y donde no existen contrapesos que puedan hacer frente a los abusos de poder para defender los derechos de los ciudadanos.

La llegada de la pandemia causada por la COVID-19 puso el pie en el acelerador de la transformación digital en el mundo. Esta situación ha estado caracterizada por la migración de las actividades cotidianas a Internet y el aumento en la cantidad de usuarios que utilizan teléfonos inteligentes. El tema salud, por otro lado, también empezó a competir con el de la seguridad nacional al momento de pensar en soluciones tecnológicas para recolectar datos por parte de los Estados.

En contextos como el venezolano, el gobierno además ha utilizado la seguridad nacional y la lucha contra el terrorismo como argumentos para justificar la cibervigilancia, la censura y los agravios hacia las libertades de las personas en Internet. Este campo difuso en el que se encuentran la prevención de la violencia y el derecho a la privacidad ha dado paso a que los usuarios cuestionen qué vale más entre su seguridad y su libertad en la

red, y también ha fomentado la creación de instrumentos legales como la normativa Contra el Odio y la llamada Ley del Ciberespacio, que constituyen herramientas de control y acoso que debilitan aún más la situación de la libertad de expresión en el país.

Ante esta situación, es necesario preguntarse ¿cómo y por qué se llegó a este punto? Así como también si los beneficios derivados de la recolección masiva de datos justifican los potenciales peligros que su explotación indebida puede conllevar. Y, en ese mismo sentido, ¿está desprotegida la sociedad civil o existen acciones concretas que se pueden llevar a cabo tanto en el presente como en el futuro próximo para defender la privacidad?



EN VENEZUELA HAY SED DE INFORMACIÓN PERSONAL

El gobierno venezolano ha entendido la importancia de la información y de su almacenamiento. En este punto hay dos ideas ampliamente vinculadas: la sed insaciable de datos y el intento por configurar un Estado vigilante con expresión en el ámbito web. A este último postulado la literatura sobre la materia lo ha llamado Autoritarismo-totalitarismo digital o el Estado digital totalitario, cuyo ejemplo más ilustrativo viene a ser China.

Pero, ¿qué busca un Estado digital totalitario? Básicamente busca ejercer un control de la ciudadanía en la red a través del manejo de datos y de la vigilancia. Para la abogada y activista venezolana de derechos digitales, Marianne Díaz, un gobierno como el venezolano tiene especial interés en dos categorías de datos. “Por un lado, está todo lo que se refiere a comunicaciones privadas de activistas, políticos, investigadores de derechos humanos y periodistas. Eso está relacionado con el filtrado de comunicaciones. Por otro lado, hay un tema de Big Data qué es lo que se ha desarrollado con el Sistema Patria y es mi mayor preocupación con Venezuela”, asegura.

Desde hace años, Venezuela tiene convenios con diversas empresas cuyo foco es el manejo de datos. En 2003, se concretaron proyectos con Cuba para la Misión Identidad y la creación de una cédula de identidad electrónica. Luego, en 2005, se acordó el desarrollo del Servicio Administrativo de Identificación, Migración y Extranjería (SAIME). La empresa detrás era Albet Ingeniería y Sistemas, una figura comercial de la Universidad de Ciencias Informáticas de La Habana (UCI).

Con la Corporación Nacional de Importación y Exportación de productos electrónicos de China (CEIEC, por sus siglas en inglés), el gobierno venezolano negoció en 2005 y en 2014 proyectos para adquisición de equipos como radares y puestos de mando. Previamente, en 2013 Venezuela también desembolsó dinero a la compañía asiática para el desarrollo de un sistema de seguridad pública. En 2016, el Ejecutivo venezolano realizó otra negociación con CEIEC y adquirió un sistema de vigilancia para el servicio penitenciario. A finales de 2021 fue difundido un video en Twitter en el que

un supuesto efectivo de la Dirección General de Contrainteligencia Militar (DGCIM) aseguró que hacían uso del Dispositivo de Extracción Forense Universal (UFED, por sus siglas en inglés) para sustraer información de dispositivos. Este equipo es desarrollado por Cellebrite, una empresa de Israel. Pero esto no es todo lo que se conoce.

El Proyecto Fake Antenna Detection (FADe) detectó 33 potenciales antenas falsas (IMSI Catchers) en la ciudad de Caracas. Este estudio, que analizó 2.635 antenas y efectuó 898.070 mediciones entre marzo y mayo de 2019, arrojó que algunas de estas antenas estaban localizadas en lugares estratégicos de la capital venezolana como los principales puntos de acceso (entradas y salidas terrestres): el eje Plaza Venezuela - Sabana Grande - Zona Rental, la Autopista Caracas - La Guaira, la Carretera Panamericana a la altura del Distribuidor Los Salías y el Aeropuerto Internacional Simón Bolívar de Maiquetía, entre otros.

Así mismo, un artículo periodístico titulado "El espionaje no es un cuento chino", publicado en el Diario Las Américas en 2021, detalló que CEIEC transformó y adaptó el edificio sede de CANTV, la empresa estatal venezolana dedicada a las telecomunicaciones, en un centro de ciberespionaje desde el cual se han realizado ciberataques a plataformas web impulsadas por la administración de Juan Guaidó como Héroes de la Salud y VoluntariosXVenezuela, así como también a la Fuerza Aérea, la Agencia Espacial de Colombia y los dominios digitales de portales informativos críticos e independientes.

Entramado gubernamental para la recopilación y uso de datos personales

1991	Conatel	Institución que ejerce la regulación, supervisión y control sobre las telecomunicaciones en Venezuela.
2003	Misión identidad	Plan nacional de cedulación.
2004	Lista Tascón	Publicación en internet del listado de firmas recolectadas para la destitución del entonces presidente Hugo Chávez.
2005	Acuerdos sobre el Saime	Institución que regula la identificación ciudadana en el país.
2005 -2014	CEIEC	Radares y puestos de mando / Sistema de seguridad pública.
2016	CEIEC	Sistema vigilancia servicio penitenciario.
2017	Carnet de la Patria	Documento de identidad, que incluye un código QR personalizado, creado para que las personas accedan a servicios del Estado.
2018	Proyecto Ley del Ciberespacio	Normativa que impone la creación de un sistema nacional de ciberdefensa

2019 — IMSI Catchers

Revelan existencia de antenas falsas en Caracas

2019 — CEIEC

Una investigación revela que edificio de la CANTV funciona como Centro de Espionaje.

SISTEMA PATRIA: CENTRALIZACIÓN Y CONTROL SOCIAL

Las autoridades gubernamentales en Venezuela han ido más allá de la mera recolección de datos. En 2015, negociaron con la empresa ZTE, de origen chino, para el desarrollo del Carnet de la Patria y todo el Sistema Patria. Previamente, este proyecto había estado en manos de la corporación Soltein con sede en México. Fue precisamente la implementación del Carnet de la Patria -y más aún, del Sistema Patria- lo que marcó un hito en la recolección y el almacenamiento de grandes volúmenes de información de ciudadanos venezolanos por parte del Estado.

El Sistema Patria reúne datos personales como nombres y apellidos, números de teléfono, lugar de residencia, dirección de correos electrónicos, información del núcleo familiar, información bancaria, datos laborales, grupo sanguíneo y redes sociales. Tras la pandemia de COVID-19, se sumó una pestaña relacionada con el ámbito de la salud y en la plataforma se han generado encuestas para recabar datos sobre los síntomas de la enfermedad, los antecedentes médicos, los medicamentos, los registros de vacunación, la epidemiología y los doctores. La adquisición de combustible para vehículos a precio preferencial también está centralizada en esta plataforma, con lo que permite saber quién posee carro propio y quién no y detalles como marca del automóvil, año de fabricación, número de placa y uso. Si la persona tiene un vehículo asignado por otra persona o por

cuestiones de trabajo, debe añadir el nombre del propietario y -en caso de ser el propietario- debe suministrar el nombre de la persona a la que fue asignado el carro. Además, el Sistema Patria da opciones de pagos de servicios de telefonía y de Internet, servicios de televisión por suscripción, agua, electricidad y gas doméstico, que ameritan que el usuario proporcione más información. El llenado de sondeos como la Encuesta CLAP, la Encuesta Mercado o la Encuesta Emprendimiento Productivo, entre otras, van en esta misma línea de recabación desproporcionada de datos.

Lo anterior ha llevado a una erradicación de las barreras en datos: el Sistema Patria cada vez quiere saber más de los usuarios y con cada ítem de llenado de información que la plataforma anexa aumenta el control de datos de los ciudadanos. Se trata de la construcción de un entramado de información en redes que interconecta a una persona con otra, que está en manos del Estado y sin usos completamente claros y transparentes. Esta plataforma ha hecho que los rastros digitales de los ciudadanos se hayan maximizado, siendo una especie de marcaje web que cada vez recopila mayores volúmenes de datos.

Los peligros del manejo de información por parte del gobierno de Venezuela ya se han advertido. En 2004 fue difundida la “Lista Tascón”, una base de datos publicada por el entonces diputado Luis Tascón, que agrupó la información de quienes habían firmado en contra de Hugo Chávez en un Referendo Revocatorio. El listado y su difusión desató una serie de despidos en los entes públicos del país y fue usado como un arma de persecución política. El asunto llegó a la Corte Interamericana de Derechos Humanos tras una demanda introducida por tres ex trabajadoras del Consejo Nacional de Fronteras, una dependencia del Ministerio de Relaciones Exteriores de Venezuela, quienes fueron despedidas tras aparecer en la lista. En 2018, la Corte determinó que el Estado venezolano incurrió en la violación de una serie de derechos.

El Sistema Patria no está exento de riesgos, sobre todo porque los datos allí almacenados han ido pasando al dominio público. Algunos de los receptores de la información alojada en la plataforma son jefes comunitarios, líderes de Consejos Comunales, personas afines al modelo gubernamental pero que no son funcionarios del Estado. “Se trata de gente que no tiene ninguna formación ni tiene ningún límite para el manejo de esos datos, pero tiene acceso a ellos”, manifiesta Díaz Hernández, quien añade que es un terreno abonado por la desprotección legal o la invención de legislaciones que no apuntan enteramente hacia el tema de la protección.

Aunque desde el oficialismo se ha impulsado la Ley del Ciberespacio y reformas a la Ley de Responsabilidad Social en Radio, Televisión y Medios

Electrónicos, de acuerdo con Díaz Hernández “ese tipo de leyes tratan fundamentalmente de ampliar los poderes de organismos preexistentes”. La especialista en derechos digitales asegura que “lo que se busca es la justificación para poder controlar la información” y acota que “el gobierno venezolano tiene como herramienta crear leyes que son en su lenguaje ambiguas para que puedan ser interpretadas de muchas maneras”.

Con respecto a la creación de una autoridad nacional que regule la protección de datos en el país y que es uno de los parámetros internacionales que se recomiendan en la materia, Díaz Hernández considera que “esto es perfectamente viable en un país con separación de poderes”. El rol de la Comisión Nacional de Telecomunicaciones (Conatel) surge como referencia al momento de hablar de una instancia que en lugar de ser autónoma y facilitar y coordinar los procedimientos en la materia que regula, más bien aplica sanciones y ordena cierres sobre medios de comunicación siguiendo las órdenes del Poder Ejecutivo venezolano. Con este marco, crear -por ejemplo- un “Comité Nacional de Protección de Datos Personales” o una “Oficina Venezolana de Protección de Datos Personales” que funcione con plena autonomía resulta una quimera.

El uso político de los datos personales en Venezuela

Datos Sistema Patria:

- Nombres y apellidos
- Números de teléfono
- Lugar de residencia
- Dirección de correos electrónicos
- Información del núcleo familiar
- Información bancaria
- Datos laborales
- Grupo sanguíneo
- Redes sociales
- Vehículo particular
- Antecedentes médicos
- Vacunación Covid

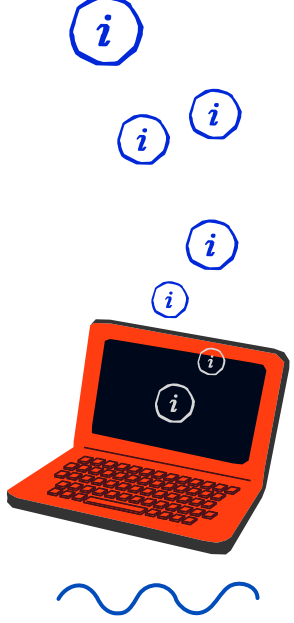
INTERNET, UNA EXPERIENCIA PERSONALIZADA

Internet es considerada actualmente como una herramienta fundamental para que gran parte de la población a nivel global pueda trabajar, estudiar, informarse, entretenerse y estar en contacto con personas de todas partes del mundo. Pero esto no siempre fue así, hace algunas décadas la navegación en Internet se limitaba a actividades específicas, con muy poca interacción y que se caracterizaban por ofrecer una experiencia bastante genérica. Hoy en día los resultados de las búsquedas, los anuncios y el contenido mostrado en los sitios web está profundamente personalizado con base en los intereses y gustos de cada usuario.

Este cambio ha significado un aumento casi exponencial del tiempo que las personas están conectadas y ha sido posible en parte gracias a la información que recolectan las plataformas, aplicaciones y sitios web sobre el uso que se le da a las mismas. En pocas palabras, se podría decir que son los propios usuarios quienes se encargan de educar a losalgoritmos para personalizar su experiencia y que estos muestren más contenido que les pueda interesar.

Uno de los motivos que explica el surgimiento de este fenómeno es el auge de lo que se conoce como “Web 2.0”, cuyo objetivo era empoderar a los usuarios para que tomaran un rol más activo, motivándolos a interactuar con otros usuarios y producir contenido que pueda ser compartido a través de Internet. Esto a su vez ocasionó que la cantidad de información disponible creciera rápidamente, a tal punto que hoy en plataformas como YouTube se pueden encontrar desde contenidos de humor hasta tutoriales de cómo reemplazar componentes de una computadora. La abundancia de información además dio origen a la competencia para captar la atención del usuario, donde la personalización de la experiencia es un factor clave, ya que si bien el tiempo de uso de estas plataformas por usuario ha aumentado, continúa siendo un recurso limitado y nuevos competidores se siguen incorporando constantemente.

*La personalización excesiva también puede conducir a los usuarios a lo que se conoce como **“cámaras de eco”**, que son espacios en los que se expone al usuario de forma recurrente solo a aquellos mensajes que reafirman su visión sobre distintos temas y no a otras opiniones, lo que puede fomentar la polarización ideológica en temas sensibles como política, religión y más.*



RECOLECCIÓN DE DATOS MASIVA, UN PELIGRO LATENTE

Las “cámaras de eco” no son el único peligro de la recolección de datos masiva, en 2018 Facebook se vio envuelta en un escándalo internacional cuando se reveló que la empresa Cambridge Analytica recopiló datos de aproximadamente 87 millones de usuarios de la plataforma sin su consentimiento. Estos datos fueron utilizados para inferir perfiles psicológicos precisos y determinar el contenido, tema y tono de mensajes políticos que se mostraban de forma individual con el objetivo de modificar el comportamiento de la audiencia.

Entre las fuentes usadas por la compañía para obtener datos de los usuarios se encontraba una aplicación de test de personalidad desarrollada en 2013 que no solo daba acceso a la información de los usuarios que completaron el test, sino también a la de su red de amigos en Facebook. De esta forma, en el caso de las elecciones presidenciales de 2016 en Estados Unidos, Cambridge Analytica fue capaz de acceder a los estados, interacciones y hasta mensajes privados de casi el 20% de la población del país, elementos que utilizó para dirigir mensajes micro-segmentados de la campaña del entonces candidato presidencial y posterior ganador de la contienda electoral, Donald Trump.

Esto permite hacerse una idea del potencial que tienen los datos para influir no solo en la actividad en Internet y el contenido que se encuentra al navegar, sino también del impacto que puede tener el mal uso de esta información en el mundo físico. Sin embargo, no toda información es igual de sensible y tampoco cualquier tipo de dato puede ser considerado un dato personal.

En este sentido, Paul Aguilar, experto en seguridad digital de Social TIC —una organización sin fines de lucro dedicada a la investigación, formación, acompañamiento y promoción de la tecnología digital e información para fines sociales en América Latina— explica que un dato personal es aquel que permite identificar a una persona específica, por ejemplo, un documento de identidad, número de teléfono o correo electrónico; información que de ser utilizada de forma incorrecta podría generar consecuencias desde el ámbito legal.

La preocupación por la exposición de datos personales sin autorización ha crecido al ritmo en que mejora el desarrollo de software. Es decir, mientras más fácil es el acceso a las tecnologías, muchas más personas pueden utilizarlas. Aguilar señala que la sociedad “está frente a una tecnología diseñada para que no puedas salir de ese espacio. Un ejemplo es el scroll infinito, que tú estés deslizando en una aplicación y no tiene fin, eso está creado intencionalmente para captar tu atención y que permanezcas ahí”.

Este incremento en la accesibilidad de las personas a estos espacios ha ocasionado que se normalice aún más compartir información personal, lo que ha servido de llave maestra para que dichas empresas, proveedores y demás actores que las administran accedan con más facilidad a datos de los usuarios que incluso pueden considerarse sensibles pues se vinculan con aspectos más íntimos como la orientación sexual, condiciones de salud, origen racial, convicciones ideológicas o religiosas, que los titulares no necesariamente quieren compartir y que podrían utilizarse para causar algún daño o perjuicio.

Desde este punto es pertinente hablar del derecho a la privacidad, que se basa en proteger a las personas de la intromisión de la parte de su vida privada que se desarrolla en un espacio reservado. Para ello deben cumplirse dos factores sustanciales: que la persona pueda apartarse por completo si así lo desea, pero también que tenga el poder de determinar a cuánta información de sí misma pueden acceder los demás.

Es por eso que los mecanismos como las cámaras de reconocimiento facial invaden esa esfera de privacidad que permite a las personas poder decidir qué hacer con sus vidas, a ir a un lado u otro, o a moverse y comportarse de cierta manera. “De ahí que a la privacidad se le conozca como este derecho de dejar a uno ser” expresa Verónica Arroyo, quien es analista y líder de políticas de identificación digital de América Latina en la organización internacional Access Now —dedicada a los derechos humanos, la política pública y el activismo por la defensa del Internet abierto y libre— y a esta reflexión añade que, por otro lado, el derecho a la protección de los datos personales tiene más bien un arraigo en el derecho a la autodeterminación informativa.

Esta noción corresponde al derecho que justamente habilita a cada persona a decidir, de forma autónoma, sobre su información, es decir, aquella que tiene una relación intrínseca con ellos mismos. Arroyo indica que la autodeterminación informativa ha evolucionado y se encuentra en varias legislaciones de América Latina. “Hoy en día hablamos de una protección de datos personales que no es la defensa o amparo de los datos en sí sino de la persona que está detrás”, precisa citando a Isabel Davara Fernández de Marcos.

Por último, también existe el llamado derecho al olvido. En la opinión de Access Now, dice Verónica Arroyo, se considera que el derecho al olvido está mal interpretado principalmente en América Latina y en Europa y explica que la aplicación de este derecho se basa en la desindexación de la información personal en manos de terceros, no en el borrado. Eso significa que el contenido persiste en Internet, pero no es mostrado por los motores de búsqueda. Entonces, cuando se habla del derecho al olvido, no es que se quiera que la información se borre y no exista más. Aún así, dicha interpretación se utiliza más bien para justificar la remoción de contenidos, como ocurre mayormente con los datos de personas como funcionarios públicos que tienen escándalos.

¿LA PRIVACIDAD ES UN DERECHO, UN PRIVILEGIO O UN NEGOCIO?

En la cosmovisión de las grandes compañías de tecnología, la privacidad de los datos no genera muchos réditos debido a que su modelo de negocio está impulsado precisamente en el manejo de la información de las personas. En términos comerciales, el dato es visto como un "manjar" que es más provechoso cuando viaja sin restricción ni cerco alguno de aplicación en aplicación, de plataforma en plataforma y sin el consentimiento de los usuarios. Después de todo, "los datos son una mina de oro", enfatiza Verónica Arroyo, quien defiende la idea de que "las bases de datos que se comercializan ilegalmente y que son adquiridas para mercadeo son un punto relevante para la conversación".

Pero cambiar esto y crear o afinar políticas de privacidad, no es una prioridad para las plataformas, pues para garantizar su rentabilidad y por lo tanto su supervivencia deben aprovechar la información que obtienen de los internautas para ofrecer servicios a otras empresas. Al respecto, Paúl Aguilar explica que "todo ese seguimiento de información deriva en anuncios" y que eso constituye un mercado atado a las grandes plataformas como Google y Meta, cuyos ingresos por este concepto superan el 70%. La publicidad en línea se erige entonces como el ideal empresarial que está apuntalado en la recolección de datos. Ciertamente, Alphabet (empresa matriz de Google) y Meta son piezas claves en el desarrollo de este ecosistema publicitario que enarbola la bandera de la intermediación web porque acercan ávidos oferentes a potenciales consumidores. Su ecuación comercial es la siguiente: se presentan productos y servicios a los usuarios a partir de la construcción de perfiles de acuerdo a necesidades, gustos e intereses y en donde lo privado no tiene cabida.

Cualquier intento de ir en contra del modelo es nocivo para los intereses de las empresas. En febrero de 2022, Meta experimentó la caída en bolsa más grande de toda su historia, la cual se presume que podría estar relacionada, en parte, a una función implementada en los dispositivos de Apple que obliga a las aplicaciones a solicitar permiso explícito del usuario para realizar seguimiento de su actividad a través de otros servicios y sitios web. Asimismo, por primera vez en su historia la compañía registró un estancamiento en la cantidad de usuarios activos en el último trimestre de 2021, lo que se traduce en un golpe para sus ingresos ya que, a menor número de usuarios, menor cantidad de datos a partir de los cuales anunciar y vender.

SEGURIDAD VS FUNCIONALIDAD: EL DILEMA DE LOS USUARIOS

Los expertos consultados para este reporte concuerdan en que los usuarios tienen un papel importante en la protección de su información. Verónica Arroyo comenta que “es un trabajo de nosotros el revisar qué permisos concedemos a las aplicaciones y cerrarlos porque esto es posible”, principalmente cuando se está frente a herramientas que pueden almacenar datos de una forma excesiva, desproporcionada e inconsulta.

Por su parte, Paúl Aguilar resume los límites que se le deben imponer a las aplicaciones en estos aspectos clave: a) Coherencia / Congruencia, b) Especificidad y c) No control / No manipulación. Del primero manifiesta que debe haber congruencia entre el permiso que solicita la aplicación y su función. El segundo se refiere a que la información adicional que se solicita en temas de rastreo y modelado de comportamiento por parte de la plataforma sea explícita, y el tercer punto es que la información recabada por la aplicación no vaya a ser usada para algún tipo de control o manipulación por parte de una autoridad o entidad.

Sin embargo, los usuarios se enfrentan a un dilema que trasciende del hecho de otorgar o no permisos, ya que muchas veces limitar los permisos concedidos a una aplicación puede quitar alguna funcionalidad y las personas son conscientes de ello, quedando en una encrucijada.

Por ello, es necesario poner en una balanza y reflexionar en la idea de si el uso de determinada aplicación o herramienta vale la información que se está entregando. Aguilar sostiene que una pregunta reveladora aparece en este punto: “¿quiero proteger la información o quiero mantener la

funcionalidad?”. Para usar una aplicación de transporte, por ejemplo, es casi obligatorio conceder el permiso de ubicación. Ahí la persona tendría que sopesar entre movilizarse o entregar su localización. Existen casos más triviales, pero igual de significativos: “Si la aplicación es un juego y te pide acceso a los contactos, tal vez no es la aplicación adecuada para jugar”, puntualiza el experto de Social TIC. Una vía adicional como reacción a este acertijo es pensar sobre si los principios individuales van en consonancia con lo que promueve la plataforma que se quiere utilizar.

HACIA LEYES DE PROTECCIÓN DE DATOS SÓLIDAS

Existen algunos esfuerzos por parte de los gobiernos para establecer controles sobre la información de los ciudadanos. El principal ejemplo es el Reglamento General de Protección de Datos de la Unión Europea (RGPD o GDPR por sus siglas en inglés), que entró en vigor en 2018 y es el estándar en cuanto a las normativas que regulan la protección de los datos y la privacidad de los ciudadanos.

A pesar de esto, Verónica Arroyo afirma que “no existe una Ley de Protección de Datos que sea ejemplar” por dos principales razones: la primera es que no se pueden importar estas normas, o ningún tipo de ley en general, sin conocer cuál es la realidad particular de cada país. La segunda es que tradicionalmente al proponer estas regulaciones se ponía el énfasis en el banco de datos, en lugar de colocar en el centro a la persona, como sí se está haciendo en las legislaciones que se están aprobando ahora. Por su parte, Paul Aguilar considera que “este tipo de reglamentos son el ejemplo de buenas ideas, pero ejecuciones que tienen muchos vacíos e inconvenientes”.

En el pasado, la protección de datos se contemplaba en lo que se llamaba habeas data, que todavía persiste en muchas constituciones. Sobre la capa del Estado, dice Verónica Arroyo, además está el Convenio 108, que fue el primer instrumento jurídico internacional relacionado con el ámbito de la protección de datos personales y la privacidad. Así los Estados pueden no tener leyes de protección de datos personales, pero sí firmar este tratado internacional que se debe ver reflejado a nivel nacional.

Conforme a los criterios que deben incluir las normativas para asegurar el cumplimiento de una buena gestión y protección de información personal, los expertos entrevistados para la elaboración de este reporte coinciden en una idea base: solamente se debe procesar y recolectar información que sea necesaria para el objetivo que se tiene.

Verónica Arroyo señala que no existe una lista cerrada de principios, pero es fundamental que estas leyes los formulen, así como la asignación de una autoridad libre e independiente que esté centrada en el usuario, y que reconozca una lista de derechos derivados del derechos a la protección de datos personales. A continuación se presentan los principios que son esenciales para que los marcos legales especializados en esta materia puedan cuidar de forma efectiva los derechos de los usuarios:

PRINCIPIOS PARA LA BUENA GESTIÓN Y PROTECCIÓN DE INFORMACIÓN PERSONAL:

1.	**Principio de legalidad y transparencia:** porque el procesamiento, tratamiento y divulgación de los datos se debe hacer de acuerdo a la ley y cumpliendo con estas especificaciones.
2.	**Principio de minimización:** porque los datos deben ser adecuados, limitados y respectivos a los propósitos que legitiman su tratamiento.
3.	**Principio de calidad:** porque los datos deben ser precisos, verdaderos y deben mantenerse actualizados.
4.	**Principio de seguridad:** porque los datos deben ser guardados de forma segura, para evitar la pérdida o el uso indebido y no autorizado de los mismos.
5.	**Principio de limitación de finalidad:** porque el tratamiento de los datos personales debe adaptarse a fines específicos, declarados de forma explícita al momento de ser recolectados.
6.	**Principio de limitación de almacenamiento:** porque solo deben ser procesados durante el tiempo que sea necesario para los fines establecidos.
7.	**Principio de adecuación:** porque se debe ofrecer un mecanismo que habilite la libre circulación de datos entre países y garantice un nivel adecuado de protección para los usuarios en relación con sus datos personales.
8.	**Principio de responsabilidad:** porque quienes se encargan de procesar datos personales deben rendir cuentas sobre el cumplimiento de los principios antes señalados.

A pesar de las dificultades para gestionar la información personal que se almacena y comparte en las plataformas digitales, también hay mecanismos de rectificación o cancelación de datos que las personas pueden aplicar para controlarlos. Referente a esto, Marianne Díaz Hernández, menciona los llamados derechos ARCO, que son básicamente aquellos a través de los cuales una persona puede manejar sus datos personales.

Se trata de la posibilidad de los titulares de los datos para decidir sobre el acceso, rectificación, cancelación y oposición de sus datos, ya sea ante un Estado, una plataforma de redes sociales o cualquiera que pueda almacenar contenidos sobre las personas. “Hay un mínimo de datos que el Estado puede conservar sobre ti, pero en general casi cualquier otra cosa se puede pedir que se elimine. Esto varía en cada país. En Venezuela esto no aplica porque no existe una regulación”, aclara la abogada.

VENEZUELA, DEUDA LEGAL Y VULNERACIÓN

En Venezuela, aunque no existe un marco legal que regule la protección de datos personales, los derechos a la privacidad e intimidad sí están contemplados en la Constitución nacional, que en su artículo 60 establece que: “Toda persona tiene derecho a la protección de su honor, vida privada, intimidad, propia imagen, confidencialidad y reputación. La ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y ciudadanas y el pleno ejercicio de sus derechos”.

Así mismo, esta normativa también consigna el habeas data en su artículo 28, en el que señala el derecho de cada persona de acceder a la información y a los datos sobre sí misma o sobre sus bienes que consten en registros oficiales o privados “con las excepciones que establezca la ley, así como de conocer el uso que se haga de los mismos y su finalidad, y de solicitar ante el tribunal competente la actualización, la rectificación o la destrucción de aquellos, si fuesen erróneos o afectasen ilegítimamente sus derechos”. Una disposición similar se encuentra en el artículo 167 de la Sala Constitucional del Tribunal Supremo de Justicia (TSJ).

En enero de 2022, la organización no gubernamental venezolana Espacio Público hizo una aproximación a la legislación y prácticas vigentes en Venezuela. Este informe presenta una compilación de las normas y regulaciones nacionales sobre protección de la privacidad y de los datos personales, entre las que además describe otros instrumentos como la Ley de Infogobierno, la Ley de Delitos Informáticos, la Ley sobre Protección y Privacidad de las Comunicaciones, así como otras jurisprudencias y

decisiones como la sentencia José R.C.F del 2012 de la Sala Constitucional del TSJ, que reconoce el derecho a los datos personales y plantea una serie de principios que deben inspirar la legislación especial.

Pero la existencia de legislación no necesariamente garantiza la protección de los derechos o limita el campo de acción de las grandes empresas o los Estados. Y esto no solo ocurre en países con contextos no democráticos, ya que incluso en países que cuentan con separación de poderes e instituciones fuertes se permite la recolección masiva de datos bajo el argumento de la seguridad nacional o el orden público.

BIOMETRÍA: SISTEMAS QUE RECONOCEN Y PERFILAN

Frente al avance tecnológico, los sistemas de identificación se han actualizado y hay una necesidad hasta cierto punto desmedida por saber quién es quién. Aunque son más comunes bajo regímenes autoritarios, cada vez más naciones emplean mecanismos de cibervigilancia y avanzan con la complicidad de las plataformas digitales que recogen los datos personales sin autorización. Ya no es suficiente un documento de identidad físico —en papel o plástico—, sino que también se han puesto en práctica herramientas capaces de ir más allá en la identificación de la ciudadanía.

Ahora, el ideal parece ser la incorporación de más elementos que permitan construir un perfil de información lo más completo posible y que incluya, por ejemplo, la detección de las huellas dactilares o el reconocimiento de los rasgos faciales.

La implementación de estas tecnologías no solo se circunscribe a escáneres o espacios cerrados. Al contrario, algunas incluyen la instalación de cámaras en sitios públicos como calles y semáforos y sistemas de autenticación en lugares como estaciones de metro o unidades de transporte colectivo, lo que permite tener un registro de las personas. Pero ello supone un reto a la hora de ejercer garantías como el derecho a la libre circulación, el derecho a la protesta o el derecho a la libertad de reunión y asociación. Difícilmente un ciudadano podrá transitar determinadas calles, asistir a manifestaciones pacíficas o a concentraciones públicas sin el temor de ser identificado por estos dispositivos. Sin contar que muchas veces las personas no tienen conocimiento de que están siendo monitoreados por medio de estas tecnologías.

La investigación “Reconocimiento facial en América Latina: tendencias en la implementación de una tecnología perversa”, elaborada por el Consorcio Al Sur en 2021, mapeó 38 iniciativas de uso de reconocimiento facial repartidas en nueve países latinoamericanos (Argentina, Brasil, Chile, Colombia, Costa Rica, México, Panamá, Paraguay y Perú) que —en su mayoría— habían sido desarrolladas entre 2018 y 2021. De acuerdo con el estudio, “los usos que se le dan a estos mecanismos en el hemisferio están relacionados con áreas como la seguridad pública, la vigilancia de espacios públicos, el transporte, la asistencia social y la migración”.

Así mismo, el proyecto evidenció que “en más del 60% de los casos no existía una base legal específica que avalase la implementación de la biometría en estos países”. Concluyó que estos mecanismos biométricos “fueron implementados sin ningún tipo de consulta o participación pública” y señaló que “no hubo estudios de impacto en privacidad o derechos humanos”. En relación con las empresas involucradas, la investigación indicó que “se trata de una diversidad de corporaciones como Dahua y Hikvision (China), IDEMIA (Francia) y FaceWatch (Reino Unido), las cuales en determinados casos han sido cuestionadas por supuestas vulneraciones a los derechos humanos”.

Hoy es una realidad que en América Latina todos estos sistemas han tomado auge: la creación de pasaportes y cédulas biométricas, la utilización de máquinas captahuellas o el escaneo de iris. Algo que plantea también como condicionante la conversión de los rasgos corporales en información y en datos sin marcha atrás. Al momento que la persona entrega sus datos biométricos queda inmiscuida en un proceso que prácticamente es irreversible. Se entrega, además, el poder y la autonomía sobre el propio cuerpo que termina siendo digitalizado y almacenado en pequeñas dosis en una base de datos que puede ser administrada por compañías o por gobiernos.

Según Marianne Díaz, la identificación biométrica no debería existir en ningún caso y, además, impone problemas. “Si se utilizan deben contar con distintas opciones de implementación porque deben considerarse todas las personas que, por ejemplo, han perdido sus huellas dactilares; pensar en las personas transgénero cuya identidad física no se corresponde con su identidad legal o en las personas que han sufrido alguna desfiguración del rostro”. En los sistemas biométricos se debe cumplir con un arquetipo, con un patrón y si la persona no encaja por alguna diferencia -aunque sea mínima- esos sistemas arrojarán errores. De allí los inconvenientes de discriminación racial o de género que estos mecanismos suscitan.

Otra implicación es que las tecnologías biométricas están íntimamente relacionadas con la vigilancia masiva, con el escrutinio público. Un individuo cuyo rostro, huella o iris es escaneado queda a la merced de quien controla estos sistemas. Se convierte en un objetivo que constantemente es monitoreado. El informe "Tecnología de vigilancia en América Latina: hecha en el extranjero, utilizada en casa", realizado por Access Now en 2021, expuso cuáles eran algunas de las empresas detrás de la vigilancia masiva, los gobiernos que compran estas tecnologías, y las políticas y prácticas de despliegue que perjudican los derechos de las personas.

El estudio tomó como ejemplo los casos de Argentina, Brasil y Ecuador y mostró que un grupo de corporaciones internacionales como AnyVision y Cellebrite (Israel), Huawei y ZTE (China), IDEMIA (Francia), Verint (Estados Unidos) y NEC (Japón), entre otras, han desplegado sus sistemas de vigilancia en estos países de la región. Igualmente, el reporte reflejó que "estas compañías están pasando inadvertidas, vendiendo tecnología de vigilancia que se utiliza en toda América Latina sin la transparencia ni el escrutinio público suficientes". Indicó que "en algunos casos, las empresas proporcionan esta tecnología peligrosa de manera gratuita para probarla en la población, pasando por alto el impacto en los derechos fundamentales de las personas".

TECNOLOGÍAS QUE OBSERVAN Y ESCUCHAN

La ausencia de marcos regulatorios sólidos y la creciente relevancia que ha ganado manejar datos han generado el desarrollo de sistemas sofisticados para rastrear a las personas como las tecnologías de espionaje. En palabras de Paul Aguilar, estas tecnologías "lo que buscan es romper los mecanismos de seguridad y privacidad que existen como algún tipo de cifrado o algún tipo de contraseña". El experto cita casos de sistemas que se han creado a lo largo de los años como Galileo, DaVinci, Finfisher y, más recientemente, Pegasus. Estos mecanismos maliciosos pertenecientes a la categoría malware son usados generalmente contra personas objetivos.

Pegasus, por ejemplo, es catalogado como spyware, un software de

espionaje que una vez instalado en el dispositivo puede extraer una gran cantidad de información del equipo o, lo que es más relevante, de la persona que figura como su propietario. Uno de los principales hallazgos del Proyecto Pegasus (o Pegasus Project) fue que muchas de las personas consideradas como objetivos de este software de espionaje perteneciente a una empresa llamada NSO Group, de origen israelí, eran periodistas, activistas, defensores de derechos humanos e incluso políticos. Pero los spywares como Pegasus no son los únicos. Otras tecnologías de espionaje son el stalkerware, muy usado en ámbitos cerrados (familias, parejas) y las herramientas de intervención de comunicaciones como los IMSI Catchers.

Ahora bien, las tecnologías de espionaje configuran lo que Aguilar denomina una “tierra de nadie”, en donde básicamente impera “la ley de la jungla”. El especialista resalta que se han roto barreras como la posesión de estas tecnologías porque ya no solo están en manos de Estados o gobiernos, sino también de funcionarios públicos, empresarios, y hasta del crimen organizado, cuyos fines pueden ser desde personales hasta económicos. Lo anterior constituye una paradoja compleja debido a que, en teoría, los postulados de creación y los usos de estas herramientas deberían obedecer a ideales como la defensa de la seguridad nacional, la lucha contra el terrorismo o la erradicación de redes criminales. Sin embargo, nada de eso se cumple en la práctica. Más bien, el espionaje se ha puesto en marcha para monitorear, perseguir, vulnerar y cercar a personas, violando su intimidad y su privacidad.

MEDIDAS PARA MEJORAR EL MANEJO DE LOS DATOS PERSONALES

A partir de las consideraciones de los especialistas en derechos digitales entrevistados para este análisis, IPYS Venezuela plantea a continuación siete recomendaciones fundamentales que se deben implementar para mejorar las condiciones en el manejo de los datos personales de los usuarios:

1.	**Desarrollar un marco regulatorio** que incluya la entrada en vigencia de una Ley de Protección de Datos Personales que se centre en los usuarios, que se base en los principios de minimización, calidad, transparencia, entre otros, y que establezca la creación de una autoridad nacional independiente y autónoma.
2.	**Promover un mayor activismo** en derechos digitales a través de la creación de redes de defensa y protección de información que tengan incidencia desde lo local hacia lo global.
3.	**Poner en práctica soluciones para la protección de datos personales** como los mecanismos de cifrado en las comunicaciones con el fin de que el usuario pueda resguardar su información ante empresas y gobiernos.
4.	**Imponer límites** a las aplicaciones y plataformas basados en tres principios importantes: 🌐 Coherencia / Congruencia 🌐 Especificidad 🌐 No control / No manipulación
5.	**Impulsar el desarrollo** de mecanismos de transparencia y políticas de privacidad para las empresas vinculadas al sector tecnológico, y específicamente al manejo de información y de datos.
6.	**Exigir a gobiernos claridad y rendición de cuentas** en procesos de negociación para la adquisición y puesta en marcha de tecnología que pueda ser usada para vigilar, espiar o controlar a la ciudadanía y para vulnerar sus derechos.
7.	**Implementar medidas para garantizar una mayor alfabetización digital** con miras a reducir brechas notables en el ámbito tecnológico y la desventaja en la que se encuentran los usuarios de plataformas y aplicaciones.

CRÉDITOS

DIRECCIÓN EJECUTIVA
Marianela Balbi

COORDINACIÓN DE LIBERTADES INFORMATIVAS
Daniela Alvarado Mejias

ASESORÍA Y EDICIÓN
David Aragort

REDACCIÓN E INVESTIGACIÓN
David Aragort, Carlos Carreño Zabala
y Daniela Alvarado Mejias

ESTRATEGIA DE COMUNICACIÓN Y DIFUSIÓN
Claudia Machillada

COORDINACIÓN DE COMUNICACIONES
Aura García

DISEÑO Y VISUALIZACIÓN DE DATOS
Camila Agelvis

CAMPAÑAS Y REDES SOCIALES
Aura García, Carlos Carreño Zabala y
Kira Al Assad