

TELECOMUNICACIONES DE AMÉRICA LATINA

..... Magazine Septiembre 2019 www.asiet.lat

Entrevista

Andrés Michelena, Ministro ecuatoriano de Telecomunicaciones
y de la Sociedad de la Información

“Nuestra meta es alcanzar un Ecuador Digital”

Opinión

**Crear conciencia para promover hábitos
saludables en la vida digital**

Maryleana Méndez, Secretaria
General a.i. de ASIET



2019
20&21
NOVEMBER
BUENOS AIRES





Realizado por



NUEVO MARCO REGULATORIO PARA LA CONVERGENCIA

Septiembre 2019

**DESCARGA AQUÍ EL NUEVO INFORME DEL CENTRO DE ESTUDIOS
DE TELECOMUNICACIONES DE AMÉRICA LATINA**



Ministro Andrés Michelena

“Nuestra meta es alcanzar un Ecuador Digital”

Desde marzo de este año usted ocupa la cartera del sector en Ecuador, lo que ha significado un impulso para colocar los temas de nuestra industria en primer plano, con la prioridad que entendemos necesita, ¿cuáles señalaría como sus principales retos o metas a cumplir en el actual periodo de gobierno? ¿Cómo puede contribuir la política pública en el avance del sector, dadas las transformaciones que ha tenido el Ecosistema Digital?

El trabajo que se viene desarrollando desde el Ministerio de Telecomunicaciones y de la Sociedad de la Información (MINTEL) está en el cumplimiento de las promesas de valor de Ecuador Digital, que es alcanzar un Ecuador conectado, con el 98% de cobertura de servicios de telecomunicaciones; un Ecuador eficiente y ciberseguro, con el 80% de trámites en línea y la estrategia nacional de ciberseguridad; así como un Ecuador innovador y competitivo, impulsando al sector productivo del país hacia la industria 4.0.

Tenemos grandes retos en los que, desde la política pública, venimos trabajando como la asignación del espectro radioeléctrico para servicios móviles, con la que pretendemos pasar del 28% al 60% de asignación, conforme a las recomendaciones de la Unión Internacional de Telecomunicaciones (UIT), generando, al menos, 27 mil empleos

entre los años 2020 y 2022; y, en cerca de 157 MM USD de inversión sectorial anual, solo por despliegue de infraestructura.

Esto permitirá sentar las bases para el desarrollo de nuevas tecnologías como el Internet de las cosas (IoT) y 5G. Además, de beneficios a la ciudadanía como la conectividad a escuelas y dotación de equipamiento tecnológico, despliegue, mantenimiento y operación de Infocentros Comunitarios; así también la instalación de puntos WiFi gratuitos.

“Pretendemos pasar del 28% al 60% de asignación de espectro radioeléctrico, conforme a las recomendaciones de la UIT”

Ustedes están impulsando la llamada estrategia ‘Ecuador Digital’, en cuanto a la inclusión digital y la universalización del acceso, elementos claves para el desarrollo, ¿qué medidas debe tomar Ecuador para cerrar la Brecha Digital? Qué debe hacer el país para lograr resolver las desigualdades de acceso entre hombres y mujeres, entre

“Impulsamos medidas regulatorias que permitirán fomentar la competencia en el mercado y generar un entorno favorable para las inversiones, por ejemplo, el uso diferenciado del espectro radioeléctrico en zonas de baja penetración de servicios”

personas mayores y jóvenes, o entre quienes viven en ámbitos rurales y urbanos?

En general, en la región existen grandes brechas de desigualdad en el ámbito digital, al menos un 50% de la población en Latinoamérica aún se encuentra desconectada. Es por eso, que estamos impulsando medidas regulatorias que permitirán fomentar la competencia en el mercado y generar un entorno favorable para las inversiones, por ejemplo, el uso diferenciado del espectro radioeléctrico en zonas de baja penetración de servicios, que permitirá el despliegue de redes comunitarias, las cuales son organizaciones sin fines de lucro que democratizar el acceso a internet a aquellas poblaciones más vulnerables, dándole autosustentabilidad a los proyectos de conectividad.

El despliegue de puntos WiFi y la utilización de los Infocentros facilitan el acceso a las Tecnologías de Información y Comunicación (TIC), contenidos educativos digitales y plataformas de educación - enfocadas a la productividad para mejorar las habilidades digitales- y la capacitación en las zonas rurales, para aquellas personas de escasos recursos. El MINTEL cuenta actualmente con 884 Infocentros a escala nacional.

En el aspecto regulatorio, ¿qué tipos de decisiones han tomado y deberían tomarse para lograr unaggiornamento de la regulación al sector telecomunicaciones? ¿Qué beneficios cree traerían estos cambios?

Estamos promoviendo la reforma a la Ley Orgánica de Telecomunicaciones y reglamentos que rigen al sector como son: los reglamentos de Prestación de Servicios de Telecomunicaciones y de audio y video por suscripción; así como el de otorgamiento de Títulos Habilitantes y el de Tarifas por Derechos de Concesión y uso de Frecuencias. Estos están siendo tratados desde una perspectiva de fomento a la inversión y desarrollo del sector, alejándonos de esa visión recaudatoria que se venía dando, sino que nos hemos enfocado hacia el desarrollo, impulsando el despliegue a las redes de telecomunicaciones, al servicio de la población.

Los cambios favorecerán la reducción de los precios para los usuarios y abonados, por el fomento a la competencia; así como acceder a servicios de calidad y con mejores prestaciones sin pagar más. Se ha demostrado que un 10% de aumento de la penetración de la banda ancha genera 0,52% de crecimiento en el PIB; además que creará nuevos empleos y beneficios por recaudación directa e indirecta al Estado, dinamizando la economía y mejorando la calidad de vida de los ciudadanos.

Para asegurar la asequibilidad de los dispositivos también, en conjunto con el Ministerio de Producción, Comercio Exterior, Inversiones y Pesca, estamos trabajando en la eliminación de aranceles a smartphones, computadoras, tablets y otros terminales para que la población; además de tener el acceso a los servicios, también pueda contar con dispositivos a mejores precios. El aumento de un 10% en la tenencia de dispositivos smartphones, por ejemplo, incrementa un 20% la productividad, por el acceso a mejores herramientas.

“Estamos promoviendo la reforma a la Ley Orgánica de Telecomunicaciones y reglamentos que rigen al sector como los reglamentos de Prestación de Servicios de Telecomunicaciones y de audio y video por suscripción, y el de otorgamiento de Títulos Habilitantes y el de Tarifas por Derechos de Concesión y uso de Frecuencias”

Desde el sector privado se señala como prioridad la actualización normativa del sector para maximizar las inversiones en la industria. ¿Cuál es la disposición del sector público en este sentido? ¿Es un tema que se ha abordado o se está teniendo en consideración desde la agenda del Ministerio de Telecomunicaciones y de la Sociedad de la Información?

La normativa se encuentra en proceso y se está priorizando en la agenda regulatoria que venimos cumpliendo, en el país. Al momento, tanto la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) como el MINTEL trabajamos, de la mano con la industria, la academia y organismos externos como el Banco Interamericano de Desarrollo, en estos nuevos instrumentos que estarán listos para el cuarto trimestre del presente año y que permitirán sentar las bases de este nuevo Ecuador Digital.

¿Qué decisiones cree que deberían acompañar al proceso de digitalización de la economía en materia de políticas de ciberseguridad y protección de usuarios y privacidad? ¿Y respecto a la piratería?

Conscientes que la economía digital necesita generar un



ambiente de confianza para masificar su uso, la política Ecuador Digital cuenta con acciones con relación a estos temas. Para diciembre de 2019, el país contará con la primera Estrategia Nacional de Ciberseguridad. Asimismo, el pasado 19 de septiembre entregamos a la Asamblea Nacional del Ecuador el proyecto de Ley de Protección de Datos Personales para su análisis y aprobación. Este cuerpo normativo garantizará los derechos digitales de los ciudadanos.

Respecto a los temas de piratería en Ecuador ya se cuenta con el Servicio Nacional de Derechos Intelectuales, institución que se encarga de estas temáticas.

¿Cuál es la importancia de contar con una Ley de Datos Personales en Ecuador?

Con una Ley de Protección de Datos Personales se garantiza al ciudadano el ejercicio de su derecho a la protección de datos personales, establecido en el artículo 66, numeral 19, de la Constitución de la República del Ecuador. El derecho a la Protección de Datos Personales se basa en la autodeterminación informativa, es decir, que el ciudadano tenga la decisión de controlar el manejo de sus datos, autorizar su uso y finalidad; de esta manera, impedir la circulación ilícita y perniciosa de los mismos.

Además, tiene muchos beneficios para el país. No solo necesitamos tener derecho a la seguridad, sino también derecho de acceso, de rectificación, de supresión, de oposición, de portabilidad y de educación digital. Asimismo, garantiza la democracia, dinamiza la economía, genera competitividad en las empresas, fortalece la innovación tecnológica porque construye un ecosistema digital confiable y transparente, en el que el Estado y las empresas, responsables de los datos personales, mantienen una relación directa con el ciudadano y el usuario para mejorar su interacción y darle bienes y servicios de calidad, al mismo tiempo que respeta sus derechos. Desde el 2018, como Gobierno realizamos mesas de trabajo para la construcción participativa del Proyecto de Ley de Pro-

“Para diciembre de 2019, el país contará con la primera Estrategia Nacional de Ciberseguridad. Asimismo, el pasado 19 de septiembre entregamos a la Asamblea Nacional el proyecto de Ley de Protección de Datos Personales para su análisis y aprobación”

tección de Datos Personales, lo que permitió difundir los conceptos básicos de la protección de datos; así como los principios y derechos que la rigen.

Los principales puntos del proyecto son:

1. Contempla principios para el tratamiento de datos personales como legalidad, lealtad, legitimidad, finalidad etc.
2. Reconocimiento y articulación de derechos a favor del titular de los datos derecho a la transparencia, derecho al acceso, derecho a la réplica etc.
3. Establece un régimen especial de tratamiento de datos sensibles de niños y adolescentes.
4. Establece un régimen de seguridad y protección de datos personales.
5. Regula la transferencia internacional de datos lo que permite establecer estándares de calidad en el tratamiento de los datos.
6. No solo contempla derechos sino también obligaciones a los responsables del tratamiento de datos personales.
7. Régimen de protección sancionatoria cuando no se manejan los datos con tratamientos mínimos de los datos como utilización de información o datos para fines distintos a los autorizados o declarados, sanciona la falta de implementación de políticas de protección de datos personales en las empresas.

Voces

Cómo *construimos* la seguridad cibernética

Contenido colaboración de **Huawei**

La seguridad está en el ADN de Huawei y los requisitos de seguridad están integrados en la forma en que diseñamos, construimos y entregamos todos nuestros productos. Desde que se fundó Huawei en 1987, no ha habido un solo incidente importante de seguridad cibernética.

Seguridad o nada

Si la industria global de las TIC no puede resolver o enfrentar las amenazas de seguridad cibernética, el mundo digital inevitablemente colapsará. Servir a los clientes es la única razón por la que existe Huawei. Asegurar una operación segura y estable de las redes de clientes es nuestra responsabilidad principal. Independientemente de los terremotos, tsunamis, guerras o ataques de piratas informáticos, hacemos todo lo posible para mantener en colaboración una operación de red estable, confiable y segura con nuestros clientes y proteger la privacidad del usuario.

Somos una empresa privada propiedad de empleados y cumplimos con las leyes y regulaciones aplicables. Si nos vemos obligados a violar maliciosamente la confianza de nuestros clientes, preferimos cerrar la empresa. Estamos comprometidos a desarrollar la tecnología más innovadora y segura, para llevar lo digital a cada persona, hogar y organización para un mundo inteligente y totalmente conectado. Haremos todos los sacrificios, a cualquier costo, para defender la seguridad sin dañar a ningún país, organización o individuo. Esta es nuestro objetivo mas importante.

US \$ 2 mil millones para mejorar la seguridad cibernética

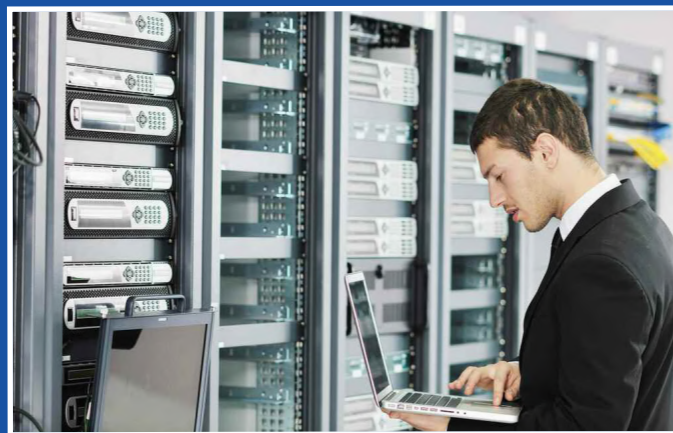
Estamos comprometidos con la seguridad cibernética y la protección de la privacidad. Estamos comprometidos a generar confianza y alta calidad en cada producto y solución de infraestructura de TIC que desarrollemos. Huawei gastará US \$ 2 mil millones en los próximos cinco años para aumentar los estándares de seguridad de nuestros equipos y mejorar nuestras capacidades y prácticas de ingeniería de software.

Áreas de enfoque de seguridad cibernética de Huawei:

Seguridad: para fortalecer las capacidades defensivas de nuestros productos, incluida su capacidad para proteger la confidencialidad, integridad y disponibilidad de servicios y datos

Resiliencia: para garantizar que el sistema pueda continuar en un estado conocido mientras está bajo ataque, incluso si está en un estado degradado, y recuperarse rápidamente después de un ataque.

Privacidad: proteger la privacidad es un requisito reglamentario y uno de los valores clave de Huawei. Los usuarios deben poder controlar adecuadamente cómo se utilizan sus datos y cuándo, y si desean recibir información en función de sus pro-



pias necesidades individuales. Las políticas de uso de datos deben ser transparentes, y debemos garantizar el conjunto correcto de capacidades y mecanismos para proteger completamente los datos privados.

Fiabilidad y disponibilidad: para garantizar operaciones sin fallas a largo plazo durante todo el ciclo de vida de nuestros productos. Deben poder recuperarse rápidamente y autogestionarse, y proporcionar un servicio predecible y consistente.

Certificado independiente de terceros

Las normas y certificaciones unificadas son una parte importante del sistema de garantía de seguridad cibernética de Huawei. Huawei defiende y cumple las normas y certificaciones de seguridad cibernética aceptadas a nivel mundial.

Desde 2004, el sistema de gestión de seguridad de Huawei ha pasado la certificación BS7799-2 / ISO 27001, y los productos de Huawei han pasado más de 200 certificaciones de seguridad, incluidas CC, FIPS, PCI DSS, CSA STAR y O-TTPS.

Huawei permanece abierto y transparente, y colabora activamente con gobiernos, clientes e instituciones de prueba de terceros que prueban y evalúan de forma independiente la seguridad de los productos y soluciones de Huawei. Hemos estado trabajando con el gobierno del Reino Unido desde 2010. Establecimos un Centro de Evaluación de Seguridad Cibernética independiente en el Reino Unido, que evalúa la seguridad de los productos que Huawei vende en el mercado de telecomunicaciones del Reino Unido. También hemos establecido un sistema similar en Canadá.

Huawei ha construido dos entornos de prueba de seguridad en Bruselas y en la ciudad de Dongguan, China. Estos entornos proporcionan las herramientas de prueba, el equipo, los recursos y el soporte técnico necesarios para los clientes o sus instituciones de terceros designadas. Esto les ayuda a verificar de forma independiente la seguridad de los productos de Huawei. Al día de hoy, ya son muchos clientes que han completado la verificación con el soporte de Huawei.

ENTREVISTA

“Es necesaria la **revisión y actualización** de la **Ley de Telecomunicaciones**, que data del año 1995, con algunas modificaciones”

Juan Carlos Duarte Duré. Presidente del Ente regulador de las telecomunicaciones de Paraguay (CONATEL)

Recientemente asumió como nuevo presidente de CONATEL, ¿Cómo afronta este reto de cara a la próxima semana de intensa actividad internacional del sector en Paraguay?

Como Presidente de la Comisión Nacional de Telecomunicaciones, ente regulador de las telecomunicaciones del Paraguay, asumo grandes compromisos tanto a nivel nacional como internacional. La CONATEL es miembro de la Unión Internacional de Telecomunicaciones (UIT), así también de la Comisión Interamericana de Telecomunicaciones (CITEL), entidad de la Organización de los Estados Americanos (OEA) y del MERCOSUR. Como tal, en la semana del 30 de setiembre al 4 de octubre, Paraguay es sede de eventos como el **Foro Regional de Desarrollo**

para las Américas (FRD-AMS) de la UIT, que ofrecerá una oportunidad de diálogo de algo nivel entre el Sector de Desarrollo de la UIT, los Gobiernos y los Organismos Reguladores de los Estados Miembros y Miembros del Sector de Desarrollo de la UIT, de forma a debatir planes de implementación, anunciar compromisos e intercambiar experiencias y mejores prácticas; y la **Reunión de MERCOSUR sobre la eliminación del cobro de cargos de Roaming Internacional**. A raíz del Acuerdo suscrito por los Presidentes de Argentina, Brasil, Paraguay y Uruguay, para la eliminación del cobro de cargos por roaming internacional a los usuarios finales del MERCOSUR, resulta necesario que nuestros países vayan analizando y debatiendo las estrategias para la adecuada aplicación de este Acuerdo, con la participación de los organismos reguladores de telecomunicaciones, así como los operadores de telefonía de los 4 países.

Además, tendrá lugar la **35 Reunión del Comité Consultivo Permanente I (CCP.I) de la CITEL**. Se desarrollarán las sesiones de los Grupos de Trabajo “Políticas y Regulación”, “Despliegue de Tecnologías y Servicios” y “Preparatorio de Conferencias”; y los Grupos Ad Hoc “para la coordinación de Iniciativas Estratégicas de la OEA relacionadas con Telecomunicaciones/TIC” y “sobre Resoluciones, Decisiones y Recomendaciones del CCP.I”. En dicha reunión de 4 días se tratarán temas tales como la protección de los derechos de los usuarios de los servicios de telecomunicaciones, la calidad del servicio de telecomunicaciones, aspectos económicos de telecomunicaciones/TIC, banda Ancha, universalización del acceso, inclusión digital y equidad de género, conformidad, control de fraudes y dispositivos móviles ilegales o irregulares, prevención, respuesta y mitigación de catástrofes, TIC y cambio climático, protección del medio ambiente, interoperabilidad, infraestructura, conectividad, numeración, servicios y aplicaciones, incluyendo Internet y la conectividad internacional, ciberseguridad, privacidad y protección de datos, evaluación de la vulnerabilidad, y construcción de



JUAN CARLOS DUARTE DURÉ

Presidente CONATEL

“El regulador debe acompañar la vertiginosa evolución de todo lo relacionado a tecnologías y telecomunicaciones”

confianza, o innovación tecnológica, Economía Digital, Internet de las Cosas, Comunidades y Ciudades Inteligentes.

Cabe resaltar que muchas de las acciones de regulación de los servicios de telecomunicaciones que ha implementado la CONATEL se han basado en políticas regionales armonizadas que se discuten en este ámbito.

También acogeremos el **Diálogo “Cerrando la Brecha: Paridad de género en los nuevos escenarios tecnológicos en las Américas”**. El objetivo es contribuir a que los diferentes actores del sector público, gubernamental, privado, academia y sociedad civil, tengan una mayor comprensión sobre la paridad de género para alcanzar la igualdad y los derechos de las mujeres con el fin de cerrar la brecha digital de género y seguir avanzando en la implementación de políticas y principios de empoderamiento en los nuevos mercados y escenarios tecnológicos en el ámbito de las telecomunicaciones y las TIC en las Américas.

Y finalmente, la **Reunión entre Autoridades de la UIT con Autoridades Universitarias**. En el marco de la vinculación de la Unión Internacional de Telecomunicaciones con la Academia, el Director del Sector de Normalización de la UIT, Señor Chaesub Lee, se reunirá con Autoridades universitarias para tratar temas como la participación de la Academia paraguaya en la UIT, ventajas de ser miembros, participación en el desarrollo de estándares, etc; y la **Conferencia del Director del Sector de Normalización de la UIT sobre “IoT, 5G e Inteligencia Artificial”**, abierto tanto para docentes como para estudiantes.

Recibiremos a dos altas autoridades de la UIT como la Directora del Sector de Desarrollo, Sra. Doreen Bogdan-Martin, y el Director del Sector de Normalización, Sr. Chaesub Lee. Así también, el Secretario Ejecutivo de la CITEL, Sr. Óscar León. Estarán presentes Autoridades nacionales, alrededor de 100 delegados de los estados miembros de la CITEL, estados asociados, representantes del MERCOSUR (tanto de los organismos reguladores como de los operadores de telefonía) y de la CONATEL.

¿Cuáles señalaría como sus principales retos o metas a cumplir desde su nueva función como presidente de CONATEL? ¿Cómo puede contribuir el regulador al avance del sector, dadas las transformaciones que ha tenido el Ecosistema Digital, para impulsar la digitalización de la economía?

Un reto importante es el apagón analógico. Al respecto, la CONATEL ha aprobado el Plan de transición de la Televisión Analógica a la Televisión Digital Terrestre (TDT), ade-

más de la modificación de algunos artículos del Reglamento del Servicio de Televisión. De forma a permitir que la ciudadanía en general esté mejor informada respecto a la Televisión Digital y al Apagón Analógico, se ha establecido por una parte prorrogar el apagón analógico y por otra, definir un Plan por zonas geográficas para el Encendido Digital y el Apagado Analógico. Para las zonas de Asunción, departamento Central y parte de los departamentos de Cordillera, Ñeembucú, Paraguari y Pdte. Hayes, se estableció el 31.12.19 como fecha límite para el encendido digital y el 31.12.21 para el apagado analógico. De la misma manera, se definieron distintas zonas con sus respectivos plazos para el resto del país, culminando el apagado analógico a finales del año 2024.

Es decir, el encendido digital se refiere a que los operadores o licenciarios del servicio de televisión deberán iniciar las transmisiones en el Sistema de TDT adoptado en el Paraguay y en casi toda Sudamérica, cual es el ISDB-TB. Y el apagado analógico implica que se deberá dejar de transmitir en el sistema analógico (PAL-N). Durante este período de 2 años se realizará la transmisión simultánea de los sistemas analógico y digital, denominado simulcasting, para que el usuario final pueda ir adaptándose al nuevo sistema. Este período se denomina de “transición a la TDT”.

El televidente podrá disfrutar de las ventajas y beneficios de la TDT, como ser imagen de alta definición, mejor calidad de sonido, datos adicionales, etc., ya sea a través de los televisores que cuenten con el sintonizador digital o en caso de decidir continuar utilizando los televisores analógicos, a través de un decodificador que permitirá convertir la señal digital en analógica.

“Para que la ciudadanía esté mejor informada respecto a la Televisión Digital y al Apagón Analógico, se ha establecido prorrogar el apagón analógico y definir un Plan por zonas geográficas para el Encendido Digital y el Apagado Analógico”

...

Sobre promoción de Telecentros y notebooks, quisiera destacar que como parte de la Licitación Pública N° 1/2017 “Banda Ancha Móvil”, para el otorgamiento de Li-

cencia para la prestación de los servicios de telefonía móvil celular y de acceso a internet y de transmisión de datos en la banda de frecuencias de 700 MHz mediante subasta simultánea ascendente, y las obligaciones para su operación y explotación, se establecieron compromisos sociales, que en resumen son los siguientes: Provisión de 96 (noventa y seis) Telecentros por parte de los licenciarios AMX PARAGUAY S.A. (20 telecentros), TELECEL S.A.E. (25 telecentros) y NÚCLEO S.A. (51 telecentros). Cada Telecentro incluye 7 terminales para capacitación y 1 terminal para gestión del Instructor, con todo el mobiliario adecuado, que servirán para capacitar a los usuarios en la adopción y uso del internet y herramientas ofimáticas. Incluye el servicio de capacitación y de contenidos que cubran las necesidades de aprendizaje de manera equilibrada entre niños y niñas, así como también el acceso a WiFi que cubra un radio de al menos 50 metros. Todos los servicios que presten estos Telecentros son gratuitos al público durante el período de 36 meses en los que deben estar operativos, con un funcionamiento mínimo de 8 horas diarias.

Además de la provisión de 12.672 notebooks, que serán distribuidas a estudiantes de Universidades Nacionales, la cuales incluyen acceso a internet.

“Muchas de las acciones de regulación de los servicios de telecomunicaciones que ha implementado la CONATEL se han basado en políticas regionales armonizadas que se discuten en este ámbito.”

...

Por otra parte, recientemente, la CONATEL llevó a cabo la recepción y apertura de sobres de ofertas en el marco de la licitación pública del subsidio a través de los Fondos de Servicios Universales (FSU 1/2019) para la implementación de la expansión de infraestructuras de las redes de telefonía móvil, acceso a Internet y transmisión de datos, en zonas del Chaco y parte del departamento de Concepción.

Se tiene previsto beneficiar a 23 comunidades mediante la instalación de 13 radio bases, para lo cual el ente regulador subsidiará la suma de 24.968 millones 500 mil guaraníes. En la ocasión se recibió una única oferta hecha por el consorcio VOX INGENIERÍA, formado por las empresas Hola Paraguay S.A., y la empresa Lexa Ingeniería S.R.L., por el monto mencionado anteriormente, el cual se encuentra dentro del tope de \$ 25 mil millones fijado por la CONATEL para el subsidio.

Es importante mencionar que los Fondos de Servicios Universales, tienen su origen en las recaudaciones de la CONATEL a través de los pagos realizados por los licenciarios, los cuales se destinan a obras de infraestructuras para conectar a zonas remotas de nuestro país, así también para apoyar a la Policía Nacional a través de la donación de equipos que posibilitan la ampliación del Sistema 911.

Adicionalmente, como tareas permanentes, el ente regulador realiza el monitoreo del espectro radioeléctrico de modo a poder detectar interferencias a operadores de los servicios de radiodifusión sonora en FM y AM, televisión, telefonía móvil celular y de acceso a internet y de transmisión de datos en las distintas bandas de operación, servicios de interés privado y prioritariamente las bandas de frecuencias utilizadas para la comunicación entre el piloto de las aeronaves con las torres de control de los aeropuertos.

La CONATEL cuenta con equipamiento de última tecnología con Estaciones Fijas de Monitoreo en más de 10 localidades, 7 Estaciones Móviles de Monitoreo y 3 Estaciones Transportables. Además de utilizarse para la detección de interferencias, permite ubicar estaciones no autorizadas, equipos de transmisión no autorizados, control de emisión de los parámetros técnicos de cada servicio, etc. En cuanto a los equipamientos de Calidad de Servicio de Telefonía Móvil y Acceso a Internet Móvil, se cuenta con 3 móviles (vehículos) y 3 equipos portátiles (tipo mochilas) para la medición de parámetros.

¿Desde el sector privado se señala como prioridad la actualización normativa del sector para maximizar las inversiones en la industria, cree que en Paraguay son necesarias decisiones importantes en este sentido? ¿Cuál es la postura del regulador frente al hecho de que existe una necesidad de fuertes inversiones para lograr que el país se convierta en un actor relevante en la cuarta transformación industrial?

Es necesaria la revisión y actualización periódica de las normas, reglamentos y de la propia Ley de Telecomunicaciones, que data del año 1995 con algunas modificaciones. En cuanto a las normas técnicas y los reglamentos de los diversos servicios, la CONATEL viene actualizándolos conforme a las necesidades.

El regulador debe acompañar la vertiginosa evolución de todo lo relacionado a tecnologías y telecomunicaciones: Internet de las Cosas (IoT), big data, inteligencia artificial, fábricas inteligentes, ciudades inteligentes, ciberseguridad, OTT, etc., tanto en lo referente a normas como regulación.

Para el efecto, debe contar con personal técnico calificado y capacitado permanentemente, de modo a poder cumplir su rol de regulador de las telecomunicaciones del país.

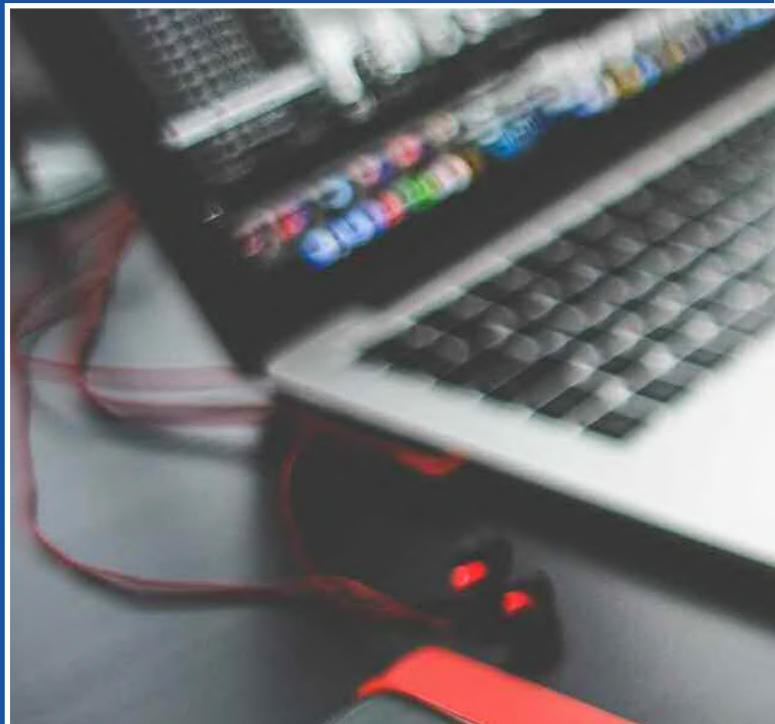
OPINIÓN



MARYLEANA
MÉNDEZ

Secretaria General
de ASIET

Crear conciencia para promover *hábitos* *saludables* en la vida digital



La ciberseguridad se refiere, en sus capas básicas, a la protección física y lógica de los activos digitales, es decir, invertir en servicios, dispositivos y software, que protejan a las organizaciones y a los usuarios de los posibles ingresos no autorizados a las plataformas. Según Gartner, a nivel mundial en el año 2018 se invirtieron \$58.9 billones de dólares en servicios de ciberseguridad, 14.1 billones en protección de infraestructura y 12.4 billones en equipos de seguridad de redes, lo que representa un 81% del gasto total en seguridad relacionada con las tec-

La mayor cantidad de ataques en línea lo sufren los usuarios domésticos, con especial mención de las infecciones en los dispositivos móviles. La piratería de software o de contenidos también son una fuente muy importante de contagio.

nologías de la información y la comunicación. Esta cifra viene en aumento, con un crecimiento interanual promedio de 9%. Así, también aumenta la cantidad de ciberataques y su costo directo. En 2018, de acuerdo con el World Economic Forum, los ciberataques tuvieron un costo total de 600 billones de dólares, lo que representa un 0.8% del PIB global. La naturaleza transnacional de las redes, la so-

fisticación de los ataques y el aumento en la exposición digital de los usuarios, son sin duda algunas de las razones para que el crecimiento de los incidentes se esté acelerando.

Los países de América Latina no escapan a esta realidad. A nivel macro, de acuerdo con el estudio de nivel de madurez en ciberseguridad de la OEA y el BID, en una muestra de 18 países de la región, el 55% de los estados están en etapas avanzadas en cuanto a los marcos jurídicos de la seguridad de las tecnologías de información y comunicación, pero el 89% tan solo alcanzan etapas iniciales respecto a la conciencia de ciberseguridad.

El desarrollo incipiente se refleja en las cifras. Según Kaspersky Lab, Brasil en el año 2017 fue uno de los 20 países con mayor cantidad de ataques de phishing en el mundo, en este grupo también se encuentran Argentina, Venezuela, Guatemala, Perú y Chile. Asimismo, Brasil, alojó el 50% de los sitios maliciosos en la región, desde los cuales se originaron ataques al resto del mundo. Es importante mencionar que, de acuerdo con las estadísticas producidas por esta firma, la mayor cantidad de ataques en línea lo sufren los usuarios domésticos, con especial mención de las infecciones en los dispositivos móviles. Las empresas se ven más afectadas por correos electrónicos o contaminaciones fuera de línea como llaves USB. La piratería de software o de contenidos también son una fuente muy importante de contagio.

En particular, el crecimiento del phishing es muy alto (solo en el 2018 Kaspersky Lab detuvo 40 millones de ataques



en América Latina). La mimetización de los ataques en correos electrónicos de firmas conocidas, SMS, llamadas telefónicas y redes sociales, hacen que en ocasiones los usuarios se confíen y entreguen su información bancaria o de tarjetas de crédito sin reparo. Incluso a nivel de empresas, de acuerdo con el estudio realizado por ESI ThoughtLab, a nivel global el 87% de los ejecutivos consideran a los empleados sin entrenamiento apropiado como la principal amenaza de ciberseguridad.

Estas cifras evidencian un problema de fondo, el eslabón más débil de la cadena de ciberseguridad es la de los usuarios finales. El desarrollo de habilidades en esta capa usuaria es esencial para que una estrategia de ciberseguridad nacional o empresarial sea efectiva. Los usuarios no solo tienen en ocasiones actitudes de exceso de confianza, sino que también se producen descuidos respecto a la actualización de las versiones del software de sus dispositivos, la renovación de las contraseñas, en la lectura detallada de los términos y condiciones cuando acceden a cierta información o aplicaciones, e incluso es de señalar la indiferencia en ciertos casos al acceder a aplicaciones o contenidos de origen dudoso que despiertan fácilmente la curiosidad.

Se ha reiterado que la generación de capacidades en el desarrollo la economía digital es muy importante, sin embargo, respecto a la ciberseguridad esto es un imperativo. Las habilidades únicamente de uso ya no son suficientes, se necesita desarrollar habilidades generales de configuración. Todos los usuarios de tecnologías digitales deberán tener la capacidad de configurar sus dispositivos para que al menos sean aprovechados los mecanismos de actuali-

Se ha reiterado que la generación de capacidades en el desarrollo la economía digital es muy importante, sin embargo, respecto a la ciberseguridad esto es un imperativo. Las habilidades únicamente de uso ya no son suficientes, se necesita desarrollar habilidades generales de configuración

zación automática, así como las herramientas de software para prevenir los contagios. El último nivel de especialización lo completarán los profesionales en ciberseguridad, especialidad de alta demanda, pues según el WEF para el 2021 habrá 3.5 millones de posiciones de esta naturaleza sin llenar

La mejora de la ciberseguridad es un reto de enormes dimensiones para todo el ecosistema. Los múltiples factores que influyen en esta tarea, y la necesidad primaria de generar cultura y cambio de hábitos, deberá acometerse entre todas las partes interesadas, tanto el sector público como el sector privado y la academia requieren reconocerse como parte de la solución y complementar sus acciones de tal forma que la promoción de la seguridad cibernética se convierta en una prioridad regional para el bienestar de los ciudadanos.

OPINIÓN



**PABLO
DE CARVAJAL**

Secretario General y del
Consejo - Dtor. global de
Regulación **Telefónica S.A**

¿Por qué necesitamos un *Nuevo Pacto Digital*?



Los responsables políticos y empresariales necesitan unirse para promover una digitalización centrada en las personas

Mire a su alrededor, casi todo es digital. Claramente, la transformación digital está cambiando nuestra forma de trabajar, de vivir y de disfrutar de nuestro tiempo de ocio. No estamos viviendo una época de cambios, sino un cambio de época. La humanidad nunca había disfrutado de tanta tecnología como lo hace ahora. La combinación de conectividad, supercomputación, big data e inteligencia artificial (IA) está ayudando a resolver algunos de los desafíos más importantes de la actualidad: curación de enfermedades, combatir epidemias o proporcionar educación de calidad a todos.

Pero también un gran número de personas está mostrando una actitud precavida frente a la digitalización y desconfían de ella como el proceso que puede aumentar la calidad de vida y hacer más competitiva la economía. Uno de los motivos es que los marcos políticos y legislativos actuales no se han creado para la era digital. Los rápidos cambios propiciados por la digitalización han dejado muchas normas y políticas obsoletas e incapaces de lidiar con problemas apremiantes. Esto tiene que cambiar. Es el momento de acordar cómo queremos que sea la sociedad digital del futuro y de aplicar principios éticos y valores comunes de un mundo digital. En Telefónica creemos que ha llegado el momento de crear un Nuevo Pacto Digital entre actores públicos y privados para administrar los profundos

cambios que nuestras sociedades experimentarán en los próximos años. Por eso, hemos publicado un [Manifiesto Digital](#) que se centra en tres objetivos fundamentales:

“Es el momento de acordar cómo queremos que sea la sociedad digital del futuro y de aplicar principios éticos y valores comunes de un mundo digital”

1: La digitalización debe ser inclusiva

La conectividad es esencial para la digitalización y requiere la implementación de las mejores redes. Según el Banco de Desarrollo de América Latina (CAF) alrededor de la mitad de la población tiene acceso a Internet en la región. En el caso de Latinoamérica y Caribe, aún no pueden conectarse a la red 288 millones de personas y solo 4 de cada 10 hogares cuenta con conexión de banda ancha fija, a pesar de los grandes avances registrados en los últimos años.

La conectividad no es solo un factor esencial para mitigar la brecha digital, sino que también representa un pilar estratégico para el crecimiento económico. Numerosos estudios demuestran que la relación entre tasa de



digitalización y productividad es proporcional, de tal forma que un índice elevado del primer factor incide positivamente sobre el segundo. A este respecto, Latinoamérica presenta un índice de digitalización de la producción un 24% más bajo que la de la media los países de la OCDE, lo que está lastrando su desarrollo económico.

Para conseguir que la región mejore estas cifras, se precisa fijar unas condiciones propicias para el despliegue de infraestructura, para la innovación y la experimentación, así como la unión de esfuerzos público-privados. Del mismo modo, se necesita un paradigma regulatorio favorable a la inversión y al desarrollo de infraestructuras destinadas a conseguir una inclusión digital plena.

Más allá de la conectividad, la perspectiva de una nueva brecha digital se divisa en el horizonte. La inteligencia artificial, la Internet de las cosas y la automatización son tecnologías que representan un desafío para nuestro mercado de trabajo. La OCDE indica que un 65 % de los niños de hoy en día crecerán y tendrán trabajos que aún no existen. El McKinsey Global Institute predice que casi la mitad del trabajo que hacemos en la actualidad estará automatizado para el año 2025. Las máquinas y las personas coexistirán de formas nuevas en el lugar de trabajo y los sistemas sociales, la educación y los derechos fundamentales tendrán que adaptarse al nuevo entorno. La industrialización, la última gran transformación econó-

“Telefónica cree que es el momento de crear un Nuevo Pacto Digital para conseguir una digitalización centrada en las personas y para proteger nuestros valores y derechos fundamentales, sin dejar atrás a nadie”

mica, creó políticas como la educación pública obligatoria, planes de bienestar y derechos laborales. Es probable que necesitemos desarrollar un nuevo conjunto de políticas sociales adaptadas a las sociedades digitales. Algunas personas pueden necesitar más tiempo y ayuda para adaptarse. Con el fin de evitar nuevas formas de desigualdad, las políticas públicas deben centrarse en ayudar a integrar a los segmentos más vulnerables de la sociedad y garantizar que no se quedan fuera de las ventajas de la digitalización.

2: Las empresas necesitan un nuevo enfoque sobre la responsabilidad empresarial

Las personas esperan poder disfrutar de servicios digitales justos, competitivos y no discriminatorios. La mejor forma de hacerlo sería que las empresas usaran de forma ética tecnologías como la inteligencia artificial y algoritmos y que permitieran que las personas controlen sus datos. La

transparencia es un elemento clave para que las personas se sientan cómodas con el uso de sus datos, pero es incluso más importante darles opciones. Un modelo centrado en las personas debe permitir que todos podamos decidir cómo y cuándo se utilizan nuestros datos.

De hecho, la nueva ética de datos puede que necesite ir más allá del cumplimiento de la regulación sobre la protección de datos. Esto es especialmente relevante para el uso de la inteligencia artificial y de algoritmos que deben guiarse por criterios éticos y deben ser responsables cuando tienen un impacto sobre los derechos de las personas.

3: Debemos modernizar nuestras políticas e instituciones para adaptarlas a la era digital

La supervisión de los mercados no le sigue el ritmo al cambio tecnológico. La aplicación desigual y el cumplimiento de las normas existentes están situando a las empresas tradicionales y locales en una situación de desventaja competitiva frente a nuevos modelos de negocios digitales. La regulación debe promover la innovación, el espíritu empresarial y debe dejar espacio para la experimentación, mientras se supervisa estrechamente y se investiga la evolución del mercado para poder intervenir con rapidez y con una mayor pericia para proteger la competencia justa, si fuera necesario.

“Debemos modernizar nuestras políticas e instituciones para adaptarlas a la era digital. La supervisión de los mercados no le sigue el ritmo al cambio tecnológico”

La Asociación Interamericana de Empresas de Telecomunicaciones (ASIET) revela que la industria de las telecomunicaciones soporta la presión fiscal más alta de la región, con una carga que supera en un 51% al resto de sectores de las economías latinoamericanas y caribeñas. Esta situación repercute negativamente en la inversión en nuevos modelos de despliegue de infraestructura que contribuyan a cerrar la brecha digital existente que separa a los países de la región de los de otras economías.

Por tanto, se requiere un tratamiento fiscal justo y equitativo para los servicios digitales (level playing field) que garantice una contribución adecuada de las empresas a las sociedades en las que operan y que aseguren la sostenibilidad de los servicios públicos. El debate debe centrarse

“Las autoridades deben intensificar también sus esfuerzos para encontrar soluciones globales o regionales en áreas como las transferencias de datos internacionales, la ciberseguridad y los impuestos, ya sea a través de acuerdos bilaterales o multinacionales”

entonces en la regulación de actividades (“el qué”), en lugar de la regulación de entidades (“el quién”).

Además, las políticas fiscales deben ir acompañadas de políticas sociales que guíen y preparen a la ciudadanía para alcanzar una sociedad digital sostenible. Con el fin de evitar nuevas formas de desigualdad, las políticas públicas deben centrarse en ayudar a integrar a los segmentos más vulnerables de la sociedad y garantizar que pueden disfrutar de las ventajas de la digitalización.

Obviamente, la información está estrechamente relacionada con la privacidad y la protección de datos, pero también se ha convertido en un gran activo competitivo con valor monetario. A menudo, las autoridades de competencia no tienen en cuenta lo suficiente estas dinámicas de mercado. Las autoridades deben intensificar también sus esfuerzos para encontrar soluciones globales o regionales en áreas como las transferencias de datos internacionales, la ciberseguridad y los impuestos, ya sea a través de acuerdos bilaterales o multinacionales.

Todo esto implica establecer una Carta de Derechos Digitales para adaptar los derechos fundamentales a las nuevas dimensiones propiciadas por la innovación tecnológica y garantizar su aplicación. Los valores importantes como la equidad y la no discriminación, la responsabilidad, la inclusividad, la transparencia y la posibilidad de elección necesitan estar protegidos y aplicarse de la misma forma en línea y sin conexión.

Las empresas también tendrán que cumplir su papel mediante la adopción de un enfoque ético para el uso de nuevas tecnologías, como la inteligencia artificial o los algoritmos y asumir la responsabilidad de su impacto en nuestras vidas, especialmente en un momento de cambios que requerirá una mayor adaptación de las personas. Telefónica cree que ha llegado la hora de construir un Nuevo Pacto Digital para conseguir una digitalización centrada en las personas y proteger nuestros valores y derechos fundamentales sin dejar a nadie atrás.

Voces

Alianza de Cisco y la OEA
para *democratizar* e
impulsar la *ciberseguridad*
en Latinoamérica

Por **Mario de la Cruz Sarabia**, MBA.
Senior Director Government Affairs Latinoamérica. **Cisco**

El pasado 15 de agosto, la Organización de los Estados Americanos (OEA) y Cisco formalizaron una alianza estratégica para democratizar e impulsar la ciberseguridad en América Latina. Además de ser el primer organismo multilateral que se creó a nivel mundial, la OEA ha tenido grandes contribuciones a la consolidación de la democracia en el hemisferio, la promoción y protección de los derechos humanos de los habitantes de la región y a desarrollar un enfoque integral en la seguridad multidimensional del continente, destacando especialmente un exitoso programa de ciberseguridad.

A través de esta iniciativa la OEA ha impulsado el desarrollo de doce estrategias nacionales de ciberseguridad, sin contar las 2 que están en desarrollo, el apoyo a 6 equipos de respuesta a incidentes, así como miles de servidores públicos, estudiantes y ciudadanos que recibieron capacitación y entrenamiento en ciberseguridad.

A través de esta iniciativa la OEA ha impulsado el desarrollo de doce estrategias nacionales de ciberseguridad, sin contar las 2 que están en desarrollo, el apoyo a 6 equipos de respuesta a incidentes, así como miles de servidores públicos, estudiantes y ciudadanos que recibieron capacitación y entrenamiento en ciberseguridad

Por su parte, Cisco se ha convertido en la empresa de seguridad más grande del mundo con ventas anualizadas de 2 mil 600 millones de dólares, con crecimientos de doble dígito en este segmento año con año.

Así mismo, Cisco cuenta con la telemetría de mayor alcance a nivel global a través de su grupo de inteligencia de amenazas cibernéticas, Talos, el cual bloquea más de 20 mil millones de amenazas diariamente. Para dar contexto a la magnitud de

este volumen, en Google se realizan 5 mil 600 búsquedas cada día, lo que nos da una idea del tamaño del flujo de amenazas que Cisco bloquea cada día. Sin duda estas capacidades y el liderazgo en la materia, hacen de Cisco el socio ideal para la OEA para juntos incrementar la concientización de este enorme reto y mejorar la ciberseguridad en el hemisferio occidental.

Este esfuerzo conjunto se traducirá en el corto plazo en la creación de Consejos de Innovación de Ciberseguridad en México, Brasil, Colombia y Chile. Los consejos, son espacios de diálogo y colaboración entre expertos del sector público, la academia, organizaciones civiles y los gobiernos para encontrar soluciones específicas a los retos y riesgos en materia digital que viven en materia de ciberseguridad cada uno de estos países.

La transformación digital está sucediendo ahora mismo, y la ciberseguridad está al frente de ella, de como la gestionemos, dependerá el éxito de la economía digital. Debemos trabajar unidos y los consejos de innovación de ciberseguridad marcarán la pauta y mostrarán como los gobiernos, las empresas y la sociedad civil de Latinoamérica tomarán plena ventaja de esta nueva era digital.

Para apoyar la labor de los consejos, utilizaremos la gran capacidad instalada con la que hoy cuenta el programa Cisco Networking Academy en la región a través del cual y en conjunto con la Organización de Estados Americanos ofreceremos cursos de entrenamiento y educación para reducir la brecha en materia de ciberseguridad.

En Cisco, estamos muy honrados y agradecidos por la confianza depositada en nosotros por el Secretario General de la OEA, Luis Almagro y todo su equipo, para impulsar esta importante iniciativa que estamos seguros se traducirá en mayor seguridad digital y crecimiento para América Latina.



Michael Tmmeny SVP Chief Government Strategy Officer de Cisco Systems junto al Secretario General de la OEA, Luis Almagro.



INCLUSIÓN DIGITAL EN PARAGUAY

“La tecnología permite derribar muros, romper paradigmas y hacer el mundo más pleno, permitiendo una verdadera evolución social y educativa”

Ha pasado un año desde que la Compañía Paraguaya de Comunicaciones - COPACO S.A., experimentó un cambio de mando en su Directorio y, en este corto tiempo, ha llevado adelante un ambicioso plan de instalación de fibra óptica de última milla, con el cual logró dar acceso a internet a 586.000 jóvenes de 35 localidades del país, a través del programa ‘Escuelas Conectadas’.

El acceso a Internet se ha constituido como un facilitador por excelencia para mayores oportunidades por su potencial contribución para reducir la pobreza, crear nuevos puestos de trabajo, así como impulsar el acceso a, por ejemplo, las finanzas o a la educación. Se nos hace imposible ignorar el hecho de que se trata de un aliado imprescindible para el cumplimiento de los Objetivos de Desarrollo Sostenible, al ofrecer un abanico de posibilidades para acelerar su cumplimiento y reducir los costos de implementación. En esta línea, se realizó un acuerdo

de Cooperación Interinstitucional entre COPACO y el Ministerio de Educación y Cultura de Paraguay, ‘Escuelas Conectadas’, para la provisión de Servicios de Comunicación de Datos a instituciones de enseñanza de varios puntos del país. Así es que mediante este programa, se han beneficiado 966 escuelas e Institutos de Formación Docente (IFD), llegando a 1.000 establecimientos conectados de distintas localidades.

“Muchas de las escuelas conectadas se encuentran en sitios alejados de las ciudades, de difícil acceso por los caminos, a lo que si le sumamos que durante el desarrollo del proyecto fueron meses de intensas lluvias, con niveles superiores a los últimos 10 años, podemos decir y sentirnos orgullosos de haber podido realizar este trabajo en tiempo record” aseguró Sante Vallese, presidente desde hace un año de COPACO, la compañía responsable de un despliegue de más de 1200 km de Fibra Óptica, llegando, de este modo, a más de 35 nuevas localidades del país.

De esta manera, la incorporación de las TIC tanto en el sistema educativo como en el desarrollo del país, se hace realidad, acortando así la brecha digital e impulsando la inclusión de niños y jóvenes a la era digital. “Los alumnos de estas escuelas tienen la posibilidad de acceder a los mismos contenidos que los chicos de los colegios más renombrados de la capital, rompiéndose la barrera de conectividad existente a nivel país y hacia el mundo. La tecnología permite derribar muros, romper paradigmas y hacer el mundo más pleno, permitiendo una verdadera evolución social y educativa.” señaló Vallese.

Pero este es tan solo un mojón en el ambicioso plan que se ha trazado a nivel país a través del Ministerio de Tecnologías de la Información y la Comunicación, ya que el desafío no solo abarca conectar escuelas sino también centros de salud e instituciones del Estado para lo cual se utilizará la ‘Red Nacional de Banda Ancha’. Vallese declaró que “Desde COPACO, como integrantes de la Red Nacional de Banda Ancha, estamos preparados como brazo estratégico del Gobierno Nacional, para el despliegue de la infraestructura y brindar conectividad a más escuelas y centros de salud” concluyó.

El Programa Escuelas Conectadas de COPACO ha beneficiado 966 escuelas e Institutos de Formación Docente (IFD), llegando a 1.000 establecimientos conectados de distintas localidades.



Por su parte, Juan Carlos Duarte Duré, recientemente nombrado Presidente del regulador paraguayo, CONATEL, señaló que valora el Proyecto de la COPACO como un emprendimiento auspicioso, que “permitirá acceder a muchas comunidades y en especial a las escuelas, a las TIC que es de suma importancia para la educación de los niños y jóvenes, y en el presente debe formar parte de la enseñanza básica el acceso a tecnologías y a la información”.

ENTREVISTA

“En un contexto donde se busca incentivar la *creatividad, innovación* y economías basadas en el conocimiento, **combatir la piratería** resulta una obligación”

Facundo Recondo, Vicepresidente de Relaciones Internacionales y Política Pública para América Latina de **Warner Media**

¿Cuál es el contexto regional en materia de piratería?

El contexto regional en materia de piratería en América Latina es realmente alarmante. Es un problema serio que no solo afecta a consumidores e industria audiovisual en su conjunto, sino también a la totalidad de la economía de la región.

La totalidad de los participantes de la industria audiovisual se encuentra amenazada por la piratería. Estudios de cine, plataformas de internet, operadores de televisión, programadores de señales, productores de contenido, artistas, etc. La piratería afecta a todos por igual y es una preocupación que todos compartimos.



FACUNDO RECONDO

Es realmente importante tomar conciencia respecto a la gravedad de la situación y todo el daño que la piratería genera. Muchas veces se omite señalar el perjuicio que la piratería genera en la economía de los países. Debe tenerse presente que la piratería genera inmensas pérdidas en impuestos no recaudados. Me refiero a millones que podrían ser percibidos por las autoridades impositivas si el consumo fuere legal. También debe destacarse los empleos que dejan de generarse por culpa de la piratería. Estos temas son súper importantes y deben ser tenidos en cuenta.

Estamos en un momento donde la creatividad, innovación y economías basadas en el conocimiento, buscan ser incentivadas en toda la región. Es una obligación combatir la piratería. Así también, es una obligación educar y proteger a los consumidores acerca de los riesgos que consumir piratería trae aparejado. La posible pérdida de privacidad, el robo de datos o contagio de virus son algunos de los peligros directamente relacionados con la piratería y deben ser atendidos.

¿Qué tan grave es en relación al resto de las regiones?

Si bien existen diversas formas a través de las cuales los piratas realizan la distribución no autorizada de contenido audiovisual, el crecimiento de internet ha convertido al streaming no autorizado en el formato dominante de piratería en América Latina.

Respecto a otras regiones, también estamos en los primeros puestos. El consumo de contenido no autorizado en Brasil, por ejemplo, es uno de los más altos del mundo, después de India^[1]. El resto de los países de la región, tales como Argentina, Colombia, México o Perú -por citar algunos- también presentan graves problemas.

Viendo el gran impacto que supone a día de hoy la piratería en el sector, de no tomarse medidas a corto plazo ¿A qué se puede enfrentar la industria?

Como señalaba anteriormente, la piratería debe verse como un flagelo de la economía en general y no solo del sector o industria audiovisual. Empleos que no se generan, impuestos que no se pagan, violación de privacidad, robo de datos, etc. son consecuencia reales y directamente relacionadas a la piratería.

Respecto a la industria audiovisual en particular, la piratería se está convirtiendo en nuestro principal competidor, poniendo en riesgo empleos, inversiones en creatividad, innovación, desarrollo de cultura local o generación de contenido de calidad.

¿Qué medidas se deben adoptar a corto plazo para cortar este flagelo y para hacer del sector una industria viable?

Si bien no existe una sola medida para combatir la piratería, entiendo que lo mas relevante es continuar recibiendo la mayor colaboración posible de fiscales, jueces y policías para poder identificar y detener a los administradores de plataformas que distribuyen contenido no autorizado.

“La piratería debe verse como un flagelo de la economía en general y no solo del sector o industria audiovisual. Empleos que no se generan, impuestos que no se pagan, violación de privacidad, robo de datos”

El número de plataformas que realiza distribución no autorizada de contenidos en América Latina es muy alto[2] y, a fin de tener un impacto real combatiendo la piratería, necesitamos poder detener a los administradores de estas plataformas. En muchos casos se trata incluso de organizaciones criminales que utilizan las ganancias obtenidas en la piratería para otros fines.

Es importante que aquellos administradores de plataformas que realizan la distribución no autorizada sepan que la violación de la propiedad intelectual tiene consecuencias graves. Asimismo, es importante contar con la colaboración de las plataformas intermediarias que proveen acceso a contenido, a fin de evitar que las mismas faciliten la distribución no autorizada.

¿Existe una coordinación efectiva a nivel nacional o regional de lucha contra la piratería? ¿Es necesario mejorar la coordinación regional?

Efectivamente existe una coordinación tanto a nivel re-

“La piratería se está convirtiendo en nuestro principal competidor, poniendo en riesgo empleos, inversiones en creatividad, innovación, desarrollo de cultura local o generación de contenido de calidad”

gional como a nivel local en la mayoría de los países. Son muchos los esfuerzos y caminos que se recorren en la lucha contra la piratería y muchas las entidades involucradas, tanto gubernamentales como privadas. ASIET es una de ellas, y su rol es vital como socio estratégico en este tema. El apoyo de ASIET y otras asociaciones similares es fundamental para tener éxito.

Si bien existen aspectos por mejorar, creo que la coordinación funciona. No obstante, es de vital importancia que los gobiernos den mas y mas prioridad a este tema, entendiendo sus alcances y perjuicios. La piratería es un problema grave y su lucha debe ser prioridad.

La piratería en la mayoría de las ocasiones no es percibida como un problema importante para la ciudadanía. ¿Qué importancia juega la concientización ciudadana? ¿Qué experiencias modelo existen en la región?

Es realmente muy importante que todos tomemos conciencia del problema al que nos enfrentamos. La concientización es un trabajo que realizamos día a día.

Debo destacar que gobiernos e industria han realizado (y continuamente realizan) diversas campañas destinadas a los ciudadanos. Estas campañas se realizan con mensajes pensados y ajustados a las circunstancias de cada país y de acuerdo con la cultura del mismo. Como parte de las mismas no solo se informan los riesgos de la piratería y los daños que genera, sino también las alternativas legítimas a las que los ciudadanos pueden acceder cuando buscan contenido.

Si bien entendemos que estas campañas nos ayudan a evitar el crecimiento de la piratería, aún no podemos decir que hemos logrado bajar el consumo, como si lo hemos visto en otras regiones.

[1] Conforme datos de www.texcipio.com

[2] Conforme datos de www.alexas.com

OPINIÓN



ÓSCAR LEÓN

Secretario Ejecutivo
de la CITEL

¿Eres un pirata digital *sin saberlo*, o sin considerarlo?



La piratería digital existe, pero **cientos de millones de usuarios consideran normal acceder a contenidos digitales de forma gratuita o a muy bajo costo**. Lo que es peor, muchos usuarios desconocen la ilegalidad que reside en el consumo y compartición de productos pirateados.

Paralelamente, el común denominador es que las personas no tienen realmente en cuenta los costos de producción o derechos de autor, que solo por mencionar algunos implica el pago a artistas, extras, camarógrafos, editores, efectos especiales, etc. En este esquema, sin saberlo, terminan perjudicando a toda la cadena de producción de contenidos, situación que en general en Latinoamérica afecta directamente a la industria local: transmisión de deportes, películas, cortometrajes. Lo cual implica efectos negativos sobre: las empresas, sus ganancias, los gobiernos, la recaudación impositiva, y sobre las fuentes de trabajo, pero también especialmente a la identidad cultural.

Cuando el consumidor accede a un sitio web pirata percibe que está adquiriendo contenidos a muy bajo precio o quizá en forma “gratuita”. En muchos casos los consumidores asumen que el pagar un bajo precio, atiende a buenos acuerdos comerciales y a que lo restante se cubre con los anuncios publicitarios que aparecen en esas plataformas ilegales. Lo cierto es que, los piratas involucran a los suscriptores con ofertas convincentes que parecen legítimas, monetizando de manera sistemática el contenido pirateado. Pero también monetizan por actividades en contra de los propios consumidores.

Utilizando productos de hardware y software comerciales, los piratas interceptan canales en cualquier parte del mundo y los hacen disponibles a través de Internet, en cualquier pantalla. Desde el fútbol europeo hasta el drama local y las películas de gran éxito, así, los consumidores pueden tener acceso al mejor contenido a una fracción del precio.

Es claro que se necesita concientizar a las personas de la gravedad del problema. En realidad, estos sitios piratas además de recaudar por anuncios publicitarios o micro pagos, están preparados para rastrear y obtener toda la información posible del cliente a través del navegador web: datos personales, datos financieros, etc. Todo ello con el fin de vender esa información, en el mejor de los casos.

Más aún, aquellos que exigen la instalación de algún software, ya sea en la computadora, el celular o en un Smart TV, representan un mayor peligro potencial para el consumidor dado que dicho software podría convertir al dispositivo en parte de una botnet con fines de mailing masivo, minería de cryptomonedas, ataques DDOS, o simplemente contener código del tipo ransomware, por ejemplo.

En América Latina, solo en cuanto a TV, representa aproximadamente el 28% del mercado, 7%. en el caso de Estados Unidos, lo que quiere decir que termina siendo el “operador” más importante de la región. Por su parte, estudios de Alianza Contra la Piratería muestran que en pro-



En américa latina, solo en cuanto a TV, la piratería representa aproximadamente el 28% del mercado, 7%. en el caso de Estados Unidos (...) estudios de Alianza Contra la Piratería muestran que en promedio el 50% de los latinoamericanos accede a algún contenido pirata en línea.

medio el 50% de los latinoamericanos accede a algún contenido pirata en línea. Sin embargo, Estados Unidos lidera la lista de países con visitas a sitios pirata: 27,9 billones de visitas y 52 % de las mismas fueron a través de celulares.

En vista de todo lo anterior, afortunadamente son varias las diferentes medidas que los Estados Miembros de la comisión Interamericana de Telecomunicaciones – CITEL, han adoptado para combatir el fraude. Si bien en general todas tienden prohibir la importación, la venta o la pro-

paganda de aparatos que permiten la piratería de la señal de tv paga, desde julio de 2019 Estados Unidos posee una regulación específica contra la piratería de contenidos, Ley DMCA. Todo ello implica 13 nuevas regulaciones en la materia, dos Recomendaciones de CITEL contra la piratería y un manual antipiratería. Aun así, es claro que debe haber una armonización sobre la regulación en la materia y, al mismo tiempo, uno de los puntos a enfocarse, tanto desde la regulación como desde el modelo de negocios, sería justamente en la fragmentación y exclusividad de contenidos.

Óscar León continuará 4 años más al frente de CITEL

El Comité Directivo Permanente de la CITEL (COM/CITEL) recomendó en la Res. 303 (XXXV-18) la renovación del cargo al Ingeniero León por un periodo de cuatro años, iniciando el 21 de septiembre de 2019. El Ingeniero León se ha destacado en la CITEL por realizar alianzas estratégicas con gremios TIC y proveedores de servicios de telecomunicaciones, con proyectos orientados a desarrollar redes para la atención de emergencias, en conectar a los habitantes de las Américas en las zonas más apartadas, reducir la desigualdad impulsando el desarrollo de capacidades a través de la educación digital e innovando para lograr la meta de tener todas las escuelas públicas de las Américas conectadas al Internet con contenidos relevantes.

Voces

Un aporte de **regulación democrática** capaz de entender a Internet

Andrés Piazza, Director de Desarrollo Digital

Casi de manera invariable, quienes hemos participado o asistido a los debates sobre Políticas relacionadas con la Sociedad de la Información o la Economía Digital durante las 2 últimas décadas hemos necesitado desarrollar, como un reflejo, una dosis de escepticismo regulatorio en lo que a Internet respecta.

Personalmente, es uno de los asuntos que más me interpela, considerando que desde los inicios de los debates de "Gobernanza de Internet" pude advertir iniciativas regulatorias nacionales o propuestas dentro de foros internacionales que adolecían de información sobre el funcionamiento de Internet en sus diferentes capas, o que poseían rasgos autoritarios.

A su vez, si bien los diálogos sobre Gobernanza han alcanzado un punto de madurez luego de 15 años de evolución con transparencia, apertura, amplio reconocimiento internacional, los proyectos de ley y los fallos judiciales no se han servido, en su mayoría, de esa calidad de debate ni de los canales de representaciones de múltiples partes.

Los individuos y organizaciones de la sociedad civil, así como del sector privado y la academia que estamos comprometidos con la vigencia de los Derechos Humanos nos hemos encontrado en incontables ocasiones colaborando para impedir la sanción de leyes torpes, propuestas autoritarias en tratados o fallos judiciales inaplicables.

En los últimos años, el crecimiento de las llamadas "Grandes Plataformas" y, en especial, la creciente intervención de estos intermediarios en los contenidos mediante los de términos de servicio hizo aumentar las voces de alerta en el mundo sobre las formas de regulación privada de espacios públicos y torno impostergable el debate sobre regulación que tenía a la Comunidad Global en una suerte de "zona de confort".

En este contexto, [en conjunto con un grupo de organizaciones](#), presentamos [durante el pasado LACIGF](#) un documento que intenta aprovechar una de las pocas ventajas que posee la región para aportar a la agenda global, como lo es el elevado estándar normativo interamericanos sobre derechos humanos. Esta [perspectiva regional](#) busca enriquecer el debate y mejorar los procesos de moderación de contenidos.

El documento, [que se encuentra abierto a Consulta hasta el 15 de Octubre](#), busca ser compatible con los referidos estándares internacionales de derechos humanos y tomar en cuenta las asimetrías existentes, alcanzando a las grandes plataformas de Internet sin ser un freno u obstáculo para la innovación, la competencia o el desarrollo de start-up, pe-



queñas empresas o iniciativas comunitarias, educativas o sin fines de lucro.

La propuesta postula una regulación democrática y equilibrada que también se oriente a proteger a las plataformas de las presiones ilegítimas que puedan sufrir de gobiernos y otros actores para ejercer moderación de discurso. Para focalizar el debate sobre fenómenos específicos, planteamos una regulación "progresiva y asimétrica" que alcanza a "plataformas de contenidos", es decir, redes sociales, motores de búsqueda y plataformas de intercambio de contenidos de terceros). En cambio, no incluye a servicios de mensajería.

En base a los estándares de derechos humanos, la propuesta de las organizaciones sociales para regular plataformas retoma el criterio de proporcionalidad. El estándar de proporcionalidad aplica no sólo a las sanciones que pudieran aplicar sino también a los procedimientos y debido proceso para ajustarse a los derechos humanos en línea.

En materia de transparencia y rendición de cuentas y derecho de apelación, intentamos evitar "reinventar la rueda" y nos limitamos a recoger las propuestas de organismos multilaterales y organizaciones sociales tales como Principios de Santa Clara o Principios de Manila o los Relatores, pero las transforma en obligaciones y no en sólo en recomendaciones que las plataformas pueden adoptar si quieren.

La participación de actores del sector privado, ya sea en la consulta o en los debates que se deriven será invaluable y bienvenida, con plena conciencia de las limitaciones que encontrarán estos avances, por fructíferos que fueran, en la precariedad institucional que posee la región.

Si bien no existe un organismo latinoamericano que pueda diseñar e implementar regulaciones a escala, contar con "acuerdos específicos" de alta calidad puede contribuir a informar la regulación de cada uno de nuestros países en el futuro cercano.

Jornadas Internacionales de TV

En la lucha contra la piratería es esencial que haya más actores de la economía creativa involucrados y más conciencia social sobre sus impactos negativos

Así lo expuso el actual Presidente del Directorio de ASIET, Ángel Melguizo, en el marco de la 29ª edición de las Jornadas Internacionales que organizan en Buenos Aires la Asociación Argentina de Televisión por Cable (ATVC) y la Cámara Argentina de Productores y Programadores Audiovisuales (CAPPSPA).



El encuentro realizado entre el 25 y 26 de septiembre reunió a destacados protagonistas de las industrias de la TV por suscripción y las tecnologías de la información y la comunicación (TIC), en mesas de debates y talleres en torno a temas como los desafíos de la industria en la era digital, las nuevas formas y recursos en la lucha contra la piratería, la democratización del acceso a Internet, y los nuevos retos del sector digital.

Personalidades como Manuel Abelleira (Presidente de DirecTV Latin America) y Carlos Moltini (CEO de Telecom Argentina) conversaron acerca de los desafíos de la industria en la era digital, destacando la necesidad de fomentar el desarrollo de la infraestructura de las telecomunicaciones e impulsar la productividad en América Latina, donde el reto es lograr marcos regulatorios previsibles y estables en un contexto de constante revolución digital. Abelleira también hizo referencia a la necesidad de unir esfuerzos contra la piratería, “un problema para toda la industria, no sólo para los distribuidores”.

Por su parte, Ángel Melguizo, Vicepresidente para Asuntos

La lucha contra la distribución ilegal de contenidos es clave de cara a maximizar las oportunidades que representa la economía creativa para impulsar la productividad y la inclusión en la Región

Externos y Regulatorios de AT&T DIRECTV Latin America y actual Presidente de ASIET, formó parte de la mesa redonda sobre “nuevas formas y recursos de la Piratería y cómo combatirla”, donde destacó que la lucha contra la distribución ilegal de contenidos es clave de cara a maximizar las oportunidades que representa la economía creativa para impulsar la productividad y la inclusión en la Región. En esta línea, aseguró que hay que innovar en la protección de la propiedad intelectual 4.0, “tenemos la convicción de que más conciencia social, y más actores de la economía creativa involucrados, es esencial”, y agregó que ASIET cobrará un rol activo en concienciar sobre los beneficios socioeconómicos de reducir la piratería.

Cullen International

El GDPR y su relación con Latinoamérica

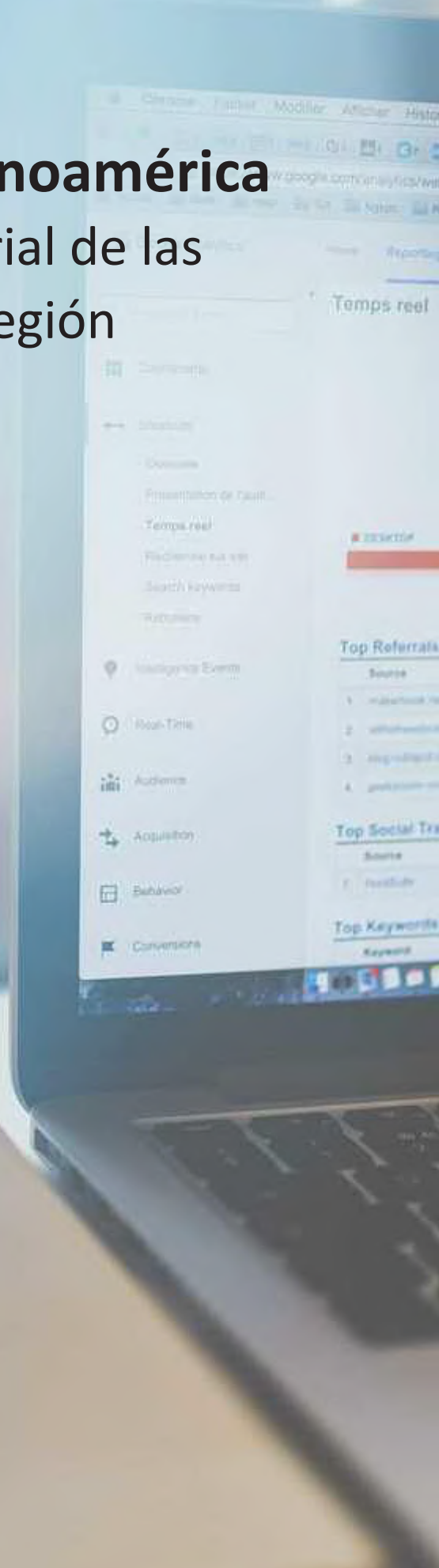
El debate sobre el alcance territorial de las regulaciones en la materia en la región

Por **Carlos Castellanos**, Analyst Americas
Telecoms | Media | Digital Economy, **CULLEN**

Es muy probable que desde comienzos del 2018 en Latinoamérica se hubieran recibido y, quizás, también leído, varios correos electrónicos que se han transmitido con noticias, solicitudes de autorización de tratamientos de datos personales y declaraciones tales como: "Nos preocupamos por su privacidad". Es posible que, asimismo, en la región se hubieran recibido decenas de emails con "avisos importantes", "revisión de políticas" o "actualizaciones de privacidad". ¿Qué tienen en común todos estos mensajes? Que todos se relacionan con el Reglamento General de Protección de Datos (GDPR, por sus siglas en inglés) vigente en la Unión Europea (UE) desde el 25 de mayo de 2018 y, principalmente, con el alcance extraterritorial de su aplicación.

En los países de América Latina, a diferencia de lo que sucede en Europa, no existe un conjunto armonizado de regulaciones sobre datos personales. Sin embargo, el GDPR constituye el gran cambio en el mundo de la protección de datos personales. Su ámbito territorial está determinado por el artículo 3 del Reglamento y representa una evolución significativa de la ley de protección de datos de la Unión Europea (UE) en comparación con el anterior marco definido por la Directiva 95/46 / CE^[1].

Tal alcance extraterritorial del GDPR abre el debate sobre cual es el alcance territorial de la regulación sobre protección de datos personales en los países de América Latina. Lo anterior, al considerar que resulta inevitable reconocer que los flujos de datos personales alrededor del mundo son bastante relevantes para delinear el criterio que determine el alcance territorial de las regulaciones sobre datos personales en la región. Cuestión que resulta ser de notable importancia para que los responsables y encargados del tratamiento de tales datos entiendan lo que deben hacer para cumplir con las reglas nacionales e internacionales en la materia.



Al abrir tal debate, el GDPR proporciona dos criterios, uno de "establishment o establecimiento" y otro de "targeting o de focalización" para determinar cuándo se aplicarán las disposiciones relevantes del GDPR al tratamiento de datos personales por parte de los responsables o encargados de los mismos. De acuerdo con los lineamientos sobre el alcance territorial del GDPR^[2], se observa que:

o el primer criterio hace que el GDPR aplique tanto a los responsables como encargados del tratamiento de datos personales establecidos en la UE (sin importar el lugar real donde se efectúe el procesamiento);

o mientras que el segundo extiende el alcance de aplicación del GDPR a situaciones en el que los responsables y encargados del tratamiento no se encuentran establecidos en la UE, pero sus actividades de tratamiento de datos personales se relacionan con el ofrecimiento de productos o servicios a titulares de datos personales localizados en la UE, o al monitoreo de datos comportamentales de tales titulares dentro de la UE.

Por lo tanto, el artículo 3 del GDPR refleja la intención del legislador europeo de garantizar una protección integral de los derechos de los interesados de la UE y establecer, en términos de requisitos de protección de datos, un campo de juego nivelado para las empresas activas en los mercados de la UE, en un contexto de constante movimiento alrededor del mundo de datos personales; los cuales se insertan en un mercado digital en el cual los datos se convierten en su principal driver –como lo decía la portada de The Economist de mayo del 2016: “El recurso más valioso del mundo ya no es el petróleo, sino los datos”.

En los países de América Latina, a diferencia de lo que sucede en Europa, no existe un conjunto armonizado de regulaciones sobre datos personales. Sin embargo, el GDPR constituye el gran cambio en el mundo de la protección de datos personales.

Así las cosas, y teniendo en cuenta que el debate sobre el alcance territorial de este tipo de regulaciones se intensifica ante el constante movimiento transfronterizo de datos personales, resulta preciso entender cual es el alcance territorial de las normas de protección de datos en cuatro países

Reesulta inevitable reconocer que los flujos de datos personales alrededor del mundo son bastante relevantes para delinear el criterio que determine el alcance territorial de las regulaciones sobre datos personales en la región.

de Latinoamérica, a saber, Argentina, Brasil, Chile y Colombia^[3]. Mas precisamente, entender si adoptan algún tipo de criterio similar al adoptado por la UE para efectos de imprimirle dinamismo a su protección dentro de las dinámicas comerciales de los mismos en un ecosistema digital. Veamos:

Argentina

Las principales leyes aplicables a nivel nacional en materia de protección de datos son la ley 25,326 del 2000^[4] y el decreto 1558 del 2001^[5]. En cuanto al alcance territorial de su protección y aplicación, la ley dispone que aplica a cualquier persona natural o jurídica que tenga su domicilio legal u oficinas en el país (i.e. criterio de establecimiento).

De igual manera prevé que los registros, archivos de datos, bases de datos o bancos de datos que se encuentren interconectados a través de redes a un nivel internacional también se cobijan bajo la aplicación de la ley.

En septiembre del 2018, el Gobierno argentino presentó una modificación a la actual ley^[6], en la cual respecto a su ámbito de aplicación territorial propone que la ley aplique cuando:

o el responsable del tratamiento se encuentre establecido en la argentina, aún cuando el tratamiento de datos tenga lugar fuera del territorio nacional;

o el responsable del tratamiento no se encuentre establecido en el país, pero se encuentre establecido en un lugar en que se aplica la legislación argentina; y

o el tratamiento de datos de titulares que residen en el país sea realizado por un responsable del tratamiento que no se encuentre establecido en la argentina, y las actividades de dicho tratamiento se encuentren relacionadas con la oferta de bienes o servicios a dichos titulares en la argentina, excepto cuando exista ley mas favorable que aplique al titular de datos personales.



Brasil

En el 2018, el entonces presidente de Brasil sancionó la ley 13,709^[7] la cual dispone el marco general de protección de privacidad y datos personales, y que entrará en vigor en agosto del 2020. Esta ley:

- consolida las diferentes normas existentes en el país en la materia, adaptándolas a un entorno digital; e
- introduce obligaciones para los sectores públicos y privados, modificando el Marco Civil da Internet del 2014^[8] para requerir un nivel más exigente de consentimiento de los titulares de datos personales para ciertos usos de su información personal.

Al no existir un conjunto armonizado de regulaciones sobre reglas de datos personales, la cuestión a resolver es cómo darle un sentido de armonización y coherencia a las regulaciones en la materia en la región, para así evitar un rompecabezas de normas e interpretaciones.

Respecto a su alcance territorial, el marco general de protección de datos personales del país se extiende al aplicar a personas naturales o jurídicas de carácter público o privado

que realicen el tratamiento de datos personales, con independencia del medio (es decir, procesamiento físico o digital), del lugar de establecimiento o de la localización de los datos personales (i.e. criterio de establecimiento), siempre que^[9]:

o el tratamiento se realice en Brasil (excepto los datos que provienen de países extranjeros y que no se comunican con ningún agente en Brasil y provienen de un país con suficiente nivel de protección de datos -art. 4, IV-, en cuyo caso la ley no aplica);

o el tratamiento tiene como objetivo ofrecer productos o servicios a los interesados en Brasil (i.e. criterio de focalización); y

o el tratamiento utiliza datos que se han recopilado en Brasil (i.e. criterio de focalización).

Chile

En el año 1999 se promulgó la ley N° 19.628^[10], sobre protección de la vida privada, que establece las normas que actualmente regulan la protección y el uso de los datos de carácter personal de las personas naturales, tanto en sus aspectos sustantivos como procedimentales. Respecto a su ámbito de aplicación, la ley solamente dispone su ámbito material (i.e. las personas a las que se les aplica la ley) y su ámbito objetivo (i.e. el tratamiento de datos personales).

No obstante, y conscientes de la “insuficiencia de la normativa frente al acelerado desarrollo tecnológico”^[11], en el 2017 el gobierno presentó una propuesta de ley en donde el alcance de aplicación territorial de la protección de datos

personales fue uno de los temas que se diagnosticaron para actualizar el régimen de protección de datos del país. Al punto, la propuesta en discusión en el congreso chileno plantea que el ámbito de aplicación territorial de la ley abarque todo tratamiento de datos personales que realicen las personas naturales o jurídicas, incluidos los órganos públicos, que no se encuentren regulados por una ley especial.

Colombia

La Constitución del país[12] introdujo el derecho fundamental al habeas data, el cual es el derecho que toda persona tiene para auto determinar la recolección, uso, almacenamiento, tratamiento y transferencia de sus datos personales, lo cual les otorga una protección especial a tales datos. El marco de protección de estos se sustenta, principalmente, en la ley 1581 de 2012[13] y su decreto reglamentario No. 1377 del 2013[14].

Respecto a su ámbito de aplicación territorial, la ley aplica: o al tratamiento de datos que se haga en Colombia (i.e. criterio de establecimiento); y

o a las actividades de tratamiento que efectúen tanto los responsables como los encargados de este, y cuyos actos se relacionen con personas domiciliadas en el país (i.e. criterio de focalización).

Como puede observarse, entre los países estudiados actualmente Colombia es el único que adopta similares criterios de establecimiento y focalización adoptados por el GDPR; mientras que Brasil hasta agosto de 2020 podrá imprimirle similar efecto extraterritorial a su nueva ley, bajo los mismos criterios que el GDPR utiliza para extender su alcance territorial.

Por su parte, Argentina propone una reforma de su regulación en la materia para adoptar mismos criterios aplicados en el GDPR para extender el alcance territorial de su aplicación; y Chile actualmente no cuenta con un alcance extraterritorial de su regulación, aunque el debate que se lleva en Congreso sobre su reforma plantea una expansión territorial de su regulación.



Solamente Colombia y Brasil (a partir del 2020) cuentan con un alcance extra-territorial de su norma de protección de datos personales (Cullen International)

Para entender las implicaciones prácticas del anterior análisis, presentamos el siguiente ejercicio de eventuales casos que involucran a Brasil (desde agosto de 2020) y Colombia, dado su efecto extraterritorial de sus regulaciones, junto con el alcance extraterritorial del GDPR:

CASOS	¿Le aplicaría el GDPR?	¿Le aplicaría la regulación de Brasil? (A partir de agosto de 2020)	¿Le aplicaría la regulación de Colombia?	Nº de regulaciones a considerar
Una empresa de medios establecida en Colombia sin presencia en Europa, que dirige su servicio a individuos ubicados en la Unión Europea	Si	No	Si	2
Un distribuidor brasileiro de comercio electrónico con un sitio web en ingles, accesible para ciudadanos europeos y colombianos, pero sin ofrecer servicios en la UE	No	Si	Si	2
Un minorista chileno de comercio electrónico con un sitio web en ingles, accesible para ciudadanos europeos, brasileiros y colombianos, y permitiéndoles la compra electrónica de productos y servicios a los mismos.	Si	Si	Si	3

En suma, y posterior a la entrada en vigor del GDPR, el alcance extraterritorial de las regulaciones de protección de datos parece ser la tendencia a adoptar en las reformas a las regulaciones de protección de datos en la región. Situación que puede hacer que los responsables y encargados del tratamiento de datos personales en la región tengan que hacer lupa en cada una de las situaciones en las que normas extranjeras les pueden imponer obligaciones en el tratamiento de datos perso-

nales o de titulares de datos ubicados en el exterior. Por lo que, al no existir un conjunto armonizado de regulaciones sobre reglas de datos personales en Latinoamérica, la cuestión a resolver es cómo darle un sentido de armonización y coherencia a las regulaciones en la materia en la región, para así evitar un rompecabezas de normas e interpretaciones nacionales que hagan la protección comercialmente inviable o excesivamente complicada de cumplir.

[1] En cuanto al alcance geográfico, la anterior Directiva 95/46/EC sólo aplicaba a empresas con un establecimiento en la UE. Sin embargo, el GDPR también se aplica a las empresas no establecidas en la UE que ofrecen bienes o servicios a particulares en la UE; o monitorean su comportamiento. Las empresas no establecidas en la UE pero sujetas al GDPR deben designar un representante en la UE, a menos que procesen datos personales ocasionalmente y sin riesgo para las personas.

[2] Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), adopted on 16 November 2018. Fuente [enlace](#).

[3] Los países cubiertos en Latinoamérica en este artículo son los mismos que los servicios de Cullen International cubre para Digital Economy.

[4] Ley 25,326 del 4 de octubre de 2000. Fuente [enlace](#).

[5] Decreto 1558 de 29 de noviembre de 2001. Fuente [enlace](#).

[6] El Proyecto de ley se puede leer accediendo a través del siguiente link [enlace](#).

[7] Ley No. 13.709 del 14 de agosto de 2018. Fuente [enlace](#).

[8] Ley 12.965 del 23 de abril del 2014. Fuent [enlace](#).

[9] Artículo 3 de la Ley No. 13.709 del 14 de agosto de 2018.

[10] Ley 16628 del 18 de Agosto de 1999, sobre protección de la vida privada. Fuente [enlace](#).

[11] Proyecto de Ley que regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de datos personales. Fuente [enlace](#).

[12] Artículo 15 de la Constitución política de Colombia.

[13] Ley 1581 del 17 de octubre de 2012. Fuente [enlace](#).

[14] Decrero 1377 del 27 de junio de 2013. Fuente [enlace](#).

Voces

Asumimos el *desafío* de estos tiempos

La demanda en la utilización del espectro se ha incrementado en los últimos años debido a la aparición de nuevos servicios, como los sistemas de comunicaciones móviles, las nuevas redes de difusión de la televisión digital terrestre, el acceso en movilidad a la banda ancha e Internet de las Cosas. Además, numerosas bandas de frecuencias están congestionadas, especialmente en centros urbanos densamente poblados.

El crecimiento del número de usuarios de los servicios de telecomunicaciones y el consecuente aumento de tráfico en las redes, así como la evolución de las tecnologías en uso y la diversidad de servicios y de aplicaciones ofrecidas por los prestadores, supone un desafío para el regulador, que debe adaptarse rápidamente a los cambios para no correr de atrás en materia de diseño de políticas que tiendan a proteger el derechos de los usuarios de servicios de telecomunicaciones y comunicación audiovisual ante el avance creciente de la digitalización de amplias esferas de la vida diaria.

A nivel audiovisual estamos viviendo un fuerte cambio de paradigma en el consumo de contenidos. El encendido de la televisión lineal por aire o cable convive con contenidos desprogramados que se consumen vía OTT's, YouTube o plataformas de streaming.

Tanto por el lado de la oferta como por el de la demanda, debemos ser capaces de acompañar el crecimiento del mercado, que tiende naturalmente a la convergencia de redes y servicios, pero sin poner en riesgo el derecho de la población al acceso a la información, las comunicaciones, la privacidad de los datos personales y la gobernanza, entre otros muchos desafíos que impone la digitalización de la sociedad. ¿Y cómo hacer todo estos desde una perspectiva humanista, plural y democrática?

Sin querer evadir la pregunta del párrafo anterior, quiero aprovechar este espacio para repasar brevemente lo que hemos hecho desde que asumimos la gestión.

En relación a las comunicaciones móviles, durante estos años hemos trabajado para proteger a los usuarios reforzando las facultades de fiscalización y control, simplificando los trámites y generando las modificaciones regulatorias necesarias para



Una colaboración de **Silvana Giudici**, Presidenta de **Enacom Argentina**

alentar la inversión privada en infraestructura de red. Gracias a ello, en solo tres años pasamos a encabezar el ranking de países con más acceso al 4G después de Uruguay y Chile.

En términos de banda ancha fija, hemos potenciado el despliegue de internet en todo el país gracias a programas financiados con Fondos del Servicios Universal. Cooperativas y Pymes acceden a créditos subsidiados y a aportes no reembolsables para despliegue de infraestructura.

Estas políticas tienden a reducir la brecha digital, que a su vez tiene impacto en la brecha social y de género, igualan oportunidades y revierten el fenómeno del despoblamiento en zonas rurales haciendo frente al reto demográfico.

A nivel audiovisual estamos viviendo un fuerte cambio de paradigma en el consumo de contenidos. El encendido de la televisión lineal por aire o cable convive con contenidos desprogramados que se consumen vía OTT's, YouTube o plataformas de streaming. Sin embargo, la radio y la TV "tradicional" sigue cumpliendo un rol fundamental como vehículos culturales e identitarios.

Por eso, encaramos un ambicioso programa de regularización de radios que operaban con Permisos Precarios y Provisorios (PPP), abrimos un concursos simplificados para licencias de FM en zonas con espectro disponible, establecimos una cuota mínima de pantalla de 30% de producción local independiente que debe ser de estreno, regularizamos los pagos adeudados del FOMECA y abrimos nuevas líneas, al mismo tiempo que estamos conduciendo la transición definitiva al encendido digital.

A partir de estos datos y estos ejemplos es que podemos decir que, si bien tenemos por delante muchos desafíos, es muy significativo lo que hemos avanzado desde la creación del ENACOM y que siempre lo hicimos con el horizonte de hacer realidad la pluralidad de voces, la libertad de expresión y la óptima comunicación de todos los argentinos.

ENTREVISTA

“Apesar de ser um desafio dos governos, o *consumidor* também tem um papel fundamental na luta contra a pirataria”

Carlos Baigorri, Superintendente de Controle de Obrigações da Anatel

Neste último período, a TV por assinatura no Brasil sofreu um declínio significativo. Essa diminuição, ocorreu devido à alteração deste serviço por alguma opção ilegal? O que você acha que é a diminuição do número de assinantes e que impacto isso pode ter na sustentabilidade do mercado? Quais são as perspectivas para esse mercado no Brasil no médio prazo?

De fato temos observado uma redução gradual e constante da base de usuários no mercado de TV por assinatura. Diversos são os fatores que podem ser associados a essa redução.

O primeiro fator que chama a atenção é a competição

com as aplicações de internet (over the top), como Netflix, Amazon Prime, etc. Ainda não temos estatísticas sobre a base de clientes desses novos fornecedores, mas é inegável o movimento de migração da plataforma tradicional de TV por assinatura em direção de soluções baseadas na Internet.

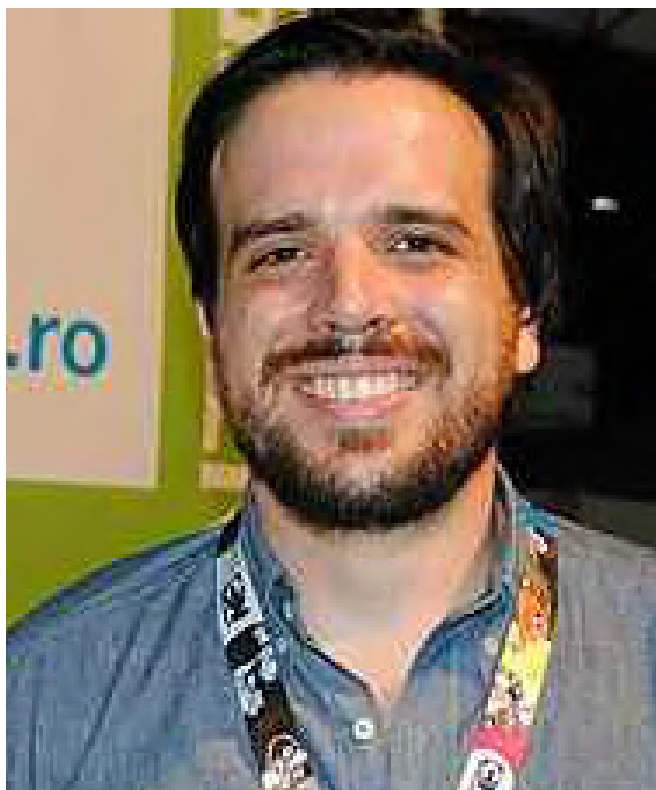
Essa migração é catalisada pela crise econômica que o Brasil está enfrentando nos últimos anos e que começa a arrefecer a partir das medidas de liberdade econômica introduzidas pelo Governo do presidente Jair Bolsonaro. No contexto dessa crise econômica é natural ver os usuários migrando para serviços mais baratos, como os OTT.

O impacto dessa migração deve ser sentida nos resultados econômicos do setor de TV por assinatura, entretanto não vislumbro que isso poderá comprometer a sustentabilidade desse segmento. Por outro lado, essa nova realidade exigirá das empresas uma revisão dos seus modelos de negócio, bem como de suas estratégias comerciais frente a esses novos concorrentes.

Como é o diálogo com os prestadores de serviços? Existe alguma colaboração?

Sim, a Anatel mantém um diálogo amplo e transparente com todos os agentes que atuam no setor de telecomunicações. Esse diálogo envolve não somente os grandes grupos empresariais que atuam no Brasil, mas também os órgãos de defesa do consumidor, os pequenos provedores, a sociedade civil organizada, bem como órgãos de governo no nível federal, estadual e municipal.

Como o Regulador está enfrentando as mudanças no ecossistema de TV paga a partir da convergência? Que mecanismos existem hoje para lidar com a pirataria



CARLOS BAIGORRI

neste mercado? Você acha que o consumidor brasileiro conhece os danos causados à economia e os criadores por consumir conteúdo pirata? A Anatel já fez campanhas de conscientização a esse respeito?

O Plano de Ação de Combate à Pirataria (PACP) foi criado no início de 2018 com o objetivo de fortalecer a atuação da fiscalização da Agência no combate à comercialização e à utilização de equipamentos para telecomunicações sem homologação, com ações de fiscalização em todo o país.

O principal mecanismo que a Anatel dispõe para enfrentar a pirataria é a fiscalização, busca e apreensão de equipamentos não certificados. Nossas atividades de fiscalização são focadas em aeroportos, supermercados e grandes distribuidores.

Importante destacar que a luta contra a pirataria não é uma iniciativa apenas da Anatel, mas sim de todo o Governo Federal. Nesse sentido, a Anatel é membro do Conselho Nacional de Combate à Pirataria e aos Delitos contra a Propriedade Intelectual, criado pelo Decreto nº 9.875 de 2019.

“A Anatel é responsável por garantir o sigilo das comunicações (...) a Agência estabelece em toda sua regulamentação uma série de obrigações para que as prestadoras de serviços protejam as informações de seus clientes. Nesse contexto de sigilo telefônico não temos nenhum problema”

Apesar de ser um desafio dos governos, o consumidor também tem um papel fundamental na luta contra a pirataria. Infelizmente percebemos que a grande maioria dos cidadãos ainda não tem a consciência sobre os riscos envolvidos no uso de equipamentos piratas. Nesse sentido, Precisamos trabalhar junto ao consumidor, criando essa consciência, por meio de campanhas de educação para o consumo.

No Brasil, embora os ataques cibernéticos e phishing tenham diminuído substancialmente, ainda é um problema relevante. Quais causas explicam esse fenômeno? Você poderia nos contar como o Brasil se saiu para enfrentar esse problema?

A segurança cibernética tem ganhado destaque no mundo inteiro, inclusive no Brasil. À medida que nossa sociedade está cada vez mais conectada, à medida que

os principais serviços são prestados por meio da internet, e à medida que todos os dispositivos que utilizamos irão se conectar no mundo IoT, a questão da segurança cibernética será cada vez mais relevante nas políticas públicas.

O Estado brasileiro tem tomado uma série de medidas para mitigar os riscos no contexto cibernético. A primeira medida que destaco foi a aprovação da Lei nº 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). Essa Lei cria todo o arcabouço institucional e regulatório para a questão da proteção, sigilo, privacidade e transparência no uso e na comercialização de dados pessoais.

A segunda medida que destaco foi a aprovação do Decreto nº 9.573, de 2018, que aprova a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), e que prevê uma Estratégia Nacional e um Plano Nacional de Segurança de Infraestruturas Críticas.

Já no âmbito da Anatel, destaco as iniciativas previstos no nosso Planejamento Estratégico e na nossa Agenda Regulatória 2019-2020, especificamente o regulamento de certificação de equipamentos 5G, prevista para aprovação até o final do presente ano.

Ainda, destaco a elaboração do Regulamento de Segurança Cibernética, também com previsão para aprovação até o fim de 2019. Além disso, a Anatel tem participado do Exercício Guardião Cibernético 2.0, concebido e executado pelo Comando de Defesa Cibernética – ComdCiber. Esse exercício de riscos cibernéticos aconteceu durante o mês de julho de 2019 e contou com a participação de 39 organizações da academia, iniciativa privada e governos.

Quais são os principais eixos de ação do regulador em relação à privacidade e proteção de dados pessoais? Que projetos têm em conta para melhorar nesse sentido? Como o uso de dados por empresas privadas é legislado no Brasil, por exemplo, aqueles que prestam serviços pela Internet?

A Anatel é responsável por garantir o sigilo das comunicações. Essa garantia de sigilo está prevista como um direito fundamental na nossa Constituição. A partir desse comando constitucional a Agência estabelece em toda sua regulamentação uma série de obrigações para que as prestadoras de serviços protejam as informações de seus clientes. Nesse contexto de sigilo telefônico não temos nenhum problema.

No que diz respeito ao uso de dados pessoais por serviços prestados na Internet, foi aprovada a Lei nº 13.709 de 2018, conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD). De acordo com esta Lei, a regulação e fiscalização ficará por conta da Autoridade Nacional de Proteção de Dados (ANPD) que está ainda em fase de implementação.

CRC (COLOMBIA)

Ciberseguridad y protección de los datos: los retos de la 4° Revolución Industrial

Por Carlos Lugo Silva, Director Ejecutivo de la Comisión de Regulación de Comunicaciones (CRC)

Vivimos en una sociedad donde la información y la rapidez con la que se accede a ella está generando nuevas dinámicas en la productividad y competitividad. Antes, las empresas establecían relaciones comerciales con sus usuarios a través del teléfono o de sus tiendas físicas, sin embargo, con la evolución del comercio se establecieron nuevas preferencias para el intercambio de bienes y servicios, siendo Internet el nuevo protagonista como canal.

Este cambio de paradigma ha venido creciendo a un ritmo constante, en Latinoamérica, para el año 2018, el 67% [1] de la población estaba conectada a internet y se espera que para el 2021 cerca de 18.2 millones de usuarios estén suscritos a algún servicio de pago de OTT [2]. La evolución de la conectividad hacia el internet productivo ha tomado cerca de 15 años, en los que la mayoría de los procesos se aceleraron cuando los nativos digitales empezaron a categorizarse como consumidores digitales.

Las vulnerabilidades en la red no sólo están asociados con la privacidad de datos, de acuerdo con el Foro Económico Mundial en el 2019, cada segundo se crean cuatro nuevas muestras de software malicioso y , los sitios de phishing duran al aire en promedio 4 horas lo que hace difícil rastrearlos

Este cambio en la forma en que los consumidores de todas las edades adquirieren bienes y servicios a través de internet, ha evidenciado algunas problemáticas y riesgos como fallas de seguridad y violación de datos personales, que se convierten en los grandes retos a enfrentar para el desarrollo de la cuarta revolución industrial, tanto desde la perspectiva de la política pública, como la regulación, y aún más importante, para la sociedad en general y sus procesos de apropiación

En Colombia, el Internet se consolida como el principal medio de interacción, de acuerdo con la Encuesta TIC, de-



sarrollada por el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia, según la cual el 97% de los colombianos usa internet para comunicarse, el 78% para entretenerse, el 66% para informarse, 44% para acceder a educación, el 33% para trabajar y el 26% para hacer transacciones comerciales entre otros, sin embargo, aunque el acceso a internet es considerablemente alto, el estudio de Comercio Electrónico publicado por la CRC en 2017 concluyó que uno de cada cuatro colombianos hace uso del comercio electrónico y que dos de esos cuatro no acceden a estos servicios por desconfianza en la entrega de los datos, esto en parte, porque hay una transacción monetaria detrás del bien o servicio a adquirir. Aunque los colombianos como la mayoría de los consumidores digitales en el mundo, para acceder a servicios gratuitos en internet “pagan con sus datos” y no se oponen a entrégalos, como si lo hacen en el caso del comercio electrónico. Esto por supuesto trae inmerso unas causas relacionadas con el proceso de apropiación TIC y de educación digital que deberán ser abordados.

Las vulnerabilidades en la red no sólo están asociados con la privacidad de datos, de acuerdo con el Foro Económico Mundial en el 2019 [3], cada segundo se crean cuatro nuevas muestras de software malicioso, los sitios de phishing duran al aire en promedio 4 horas lo que hace difícil rastrearlos, los ataques de acceso remoto están dirigido en su mayoría a dispositivos IoT, el 80% de los fraudes en línea se hacen a través del celular, y finalmente la utilización de inteligencia artificial, hacen cada vez más difícil enfrentar las actividades ilícitas en internet.

Pero ¿a quién corresponde el cuidado en la ciberseguridad? La respuesta y el punto de vista de los actores del ecosis-



tema es contradictoria, por un lado, los ciudadanos piensan que las compañías son 100% responsables y que los gobiernos no cuentan con las herramientas para protegerlos, mientras que las empresas consideran que el gobierno es quien deben garantizar una regulación equitativa de cara a los nuevos actores que compiten en el mercado y no cuentan con las mismas cargas regulatorias, además estableciendo reglas que exijan el diseño responsable de las plataformas utilizadas para el intercambio de información durante el proceso de adquisición de bienes y servicios, también esperan que los consumidores entiendan, asimilen y acepten los términos y condiciones sin objeción. Por su parte, los gobiernos exponen que su función es la apropiación de las tecnologías y velar porque esos nuevos mercados no generen fallas ni abusos a los usuarios.

Se hace necesario entonces que los actores del ecosistema digital compartan responsabilidades, puesto que no todo se soluciona con modelos regulatorios, es indispensable conocer las dinámicas de los mercados antes de intervenir, no hay diseños sofisticados que cumplan con todos los controles de seguridad y privacidad antes de su lanzamiento, ni siquiera la responsabilidad debe recaer en su totalidad en los usuarios, que a menudo se muestran ansiosos por adquirir bienes y servicios digitales, sin pensar en las consecuencias de la huella digital y los riesgos de acceder a estos contenidos.

Desde nuestra experiencia estos retos pueden ser afrontados en conjunto, a través de un trabajo coordinado que disminuya los riesgos. Los Gobiernos deben concentrar sus esfuerzos en: i) Informar y asesorar a los usuarios y empresas sobre los riesgos en la ciberseguridad y la protección de

datos, esto a través de educación digital en todos los niveles, y procesos de apropiación integrales ii) Sensibilizar a los usuarios para que lean los términos y condiciones, usen conexiones seguras, y que aprendan a reconocer posibles ataques y iii) Identificar y analizar las quejas para introducir actualizaciones en la regulación.

Por su parte, las empresas pueden trabajar en: i) Informar y asesorar a los usuarios sobre cómo cumplir con las normas de protección de datos y ciberseguridad, ii) Crear conciencia y proporcionar capacitación a sus empleados que se tengan que involucrar en actividades de procesamiento de datos y iii) Manejar las quejas o solicitudes de las instituciones, el regulador, los interesados o introducir mejoras por iniciativa propia.

Finalmente, los usuarios deben esforzarse por informarse sobre sus derechos y obligaciones en la protección de datos y la ciberseguridad, entender el alcance de la información que entregan a cambio de acceder a bienes y servicios digitales e informar sobre la violación de sus datos privados, vulnerabilidades, ataques, etc. En conclusión, no podemos aislarnos por miedo a sufrir ataques en la red, pero tampoco podemos dejar que la ciber delincuencia gane, así que estas acciones son el principio para generar un ambiente adecuado que permita el impulso de la cuarta revolución industrial.

[1] Penetración de Internet en Latinoamérica 2018 fuente statista

[2] Estudio Dataxis

[3] Here are the biggest cybercrime trends of 2019-WEF

Contenido Mediapartner

Convergencia Latina

Industria 4.0: Las redes de tecnología operativa dejan de ser estáticas y se vuelven vulnerables a ataques cibernéticos

Una colaboración aportada por **Convergencia Research & Convergencialatina**

A través de un estudio realizado por la consultora AGON para el Centro de Estudios de La automatización de procesos industriales trae consigo riesgos que, anteriormente, no eran considerados como tales. La seguridad por capas y la autenticación multifactor son algunas de las herramientas diseñadas para proteger estos ámbitos.



ELa denominada Cuarta Revolución Industrial demanda cada vez más una alta conectividad entre los componentes de la industria, sin sacrificar los requerimientos básicos de continuidad del negocio y alta disponibilidad, lo que representa grandes riesgos y vulnerabilidad informática. Estas vulnerabilidades pueden afectar a las personas y a las empresas, como es el caso de un apagón masivo de energía eléctrica, aseguró Hernando Castiglioni, gerente de Ingeniería de Fortinet para el Cono Sur, durante una entrevista con Convergencialatina.

Tradicionalmente las redes OT (red de tecnología operativa) —compuestas por dispositivos y procesos de control— actuaban separadas de las redes IT (red de tecnología de la información), que abarca a las aplicaciones empresariales y de escritorio. En la era industrial que recién comienza, ambas redes convergen en pos de la automatización y la administración remotas. Así las cosas, la industria 4.0 trae consigo riesgos que, anteriormente, no eran considerados como tales, porque el mundo OT era muy estático. Históricamente, las redes industriales

La demanda de informatización de las plantas industriales se incrementará con el próximo despliegue de las redes 5G, debido a la mayor conectividad entre los distintos actuadores, sensores y máquinas. Y, cada punto que se conecta es una puerta de entrada para posibles ataques.

fueron aisladas del Internet y ahora están convergiendo de una forma u otra para facilitar la automatización de procesos.

De acuerdo con Luciano Meléndez, gerente de Desarrollo de Negocios del área de Seguridad de Logicalis, la demanda de informatización de las plantas industriales se

Una de las recomendaciones desde los especialistas consultados por Convergencialatina es aplicar herramientas de seguridad por capas, lo que permite segmentar la red – de acuerdo con el nivel de importancia- para protegerla por elementos específicos.

incrementará con el próximo despliegue de las redes 5G, debido a la mayor conectividad entre los distintos actores, sensores y máquinas. Y como advirtió el vocero, cada punto que se conecta es una puerta de entrada para posibles ataques.

En ese sentido, las medidas de protección que se apliquen en estas redes se vuelven clave, por las consecuencias que acarrearía un eventual ataque para la operación, logística, reputación e impacto financiero de las empresas. Una de las recomendaciones desde los especialistas consultados por Convergencialatina es aplicar herramientas de seguridad por capas, lo que permite segmentar la red – de acuerdo con el nivel de importancia- para protegerla por elementos específicos.

Leonardo Cesário, ingeniero de Ventas de la empresa norteamericana WatchGuard, comentó a este medio que una de las principales preocupaciones de los proveedores de soluciones de seguridad para el sector industrial es ofrecer protección a los usuarios finales de forma automática, sin necesidad de que los empleados tengan pleno conocimiento de las amenazas posibles. El ejecutivo mencionó como tendencia en el campo de la ciberseguridad la implementación de tokens para la validación, así como firewalls y reconocimiento biométrico.

En caso de que la industria trabaje con sistemas remotos,

es necesario implementar un sistema de Autenticación Multifactor (MFA, por sus siglas en inglés), que requiere más de una forma de autenticación para comprobar la legitimidad de una transacción. “Recomendamos mecanismos como la autenticación vía ‘push’”, pues permiten establecer un canal de doble vía y en tiempo real, para que el usuario responda inmediatamente si desea aprobar o declinar una acción”, agregó el vocero. Y destacó que, para las empresas, el mecanismo de ataques de mayor riesgo es el phishing.

Un caso de aplicación: Sinopec en Argentina

En el yacimiento petrolífero que Sinopec tiene en Argentina, Logicalis y Redline implementaron una red wireless de alta capacidad y baja latencia, para brindar servicios en sitios remotos fijos y temporales como oficinas en campo, plantas de separación y equipos de perforación y mantenimiento.

En el yacimiento petrolífero que Sinopec tiene en Argentina, Logicalis y Redline implementaron una red wireless de alta capacidad y baja latencia, para brindar servicios en sitios remotos fijos y temporales como oficinas en campo, plantas de separación y equipos de perforación y mantenimiento.

Para este desarrollo se usó un diseño de Logicalis, especializado en infraestructura crítica, que contempla una capa de ciberseguridad, mediante segmentación inteligente y automatización en el tratamiento de amenazas. A su vez, se incorporó la gestión de identidades y NAC (Network Access Control) para identificar y permitir acceso granular a usuarios basado en perfiles o roles, de manera que los dispositivos conectados a la red industrial tengan un control en el punto de acceso a la red.

CONVERGENCIA
RESEARCH

research@convergencia.com
+54 11 4342 3740

Inteligencia

para entender
la evolución del mercado y
las oportunidades de negocio

Expertos

en estudiar la convergencia,
su impacto social
y la economía digital

Voces

Estrategia Antipiratería
de ANDEBU en Uruguay

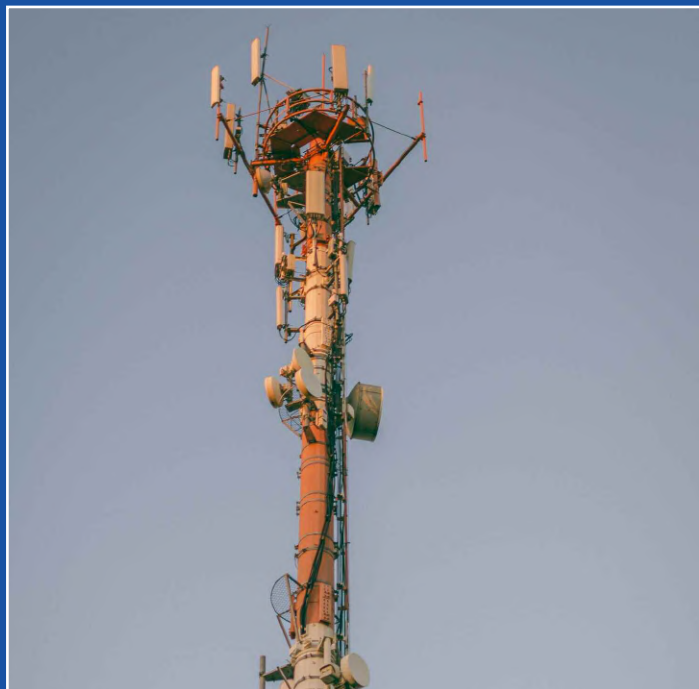
Una colaboración de la Asociación Nacional de Broadcasters Uruguayos, por Omar de León

La difusión ilegal de señales afecta seriamente a los operadores de TV de abonado. Una modalidad fácilmente perseguible, y por tanto casi en desuso en muchos países, pero no en todos, son las cajas especiales y antenas satelitales. En Uruguay se ha combatido eficazmente controlando la importación y el contrabando, y principalmente mediante el decomiso de los equipos a los usuarios a través de la vía judicial. Cuando se desarrolla la banda ancha en un país, la actividad ilegal es desarrollada en la Internet a través de cajas multipropósito (p.e. STB), computadoras, celulares, tabletas o Smart TV, a los que se les instala una aplicación o programa, lo que es solamente el vehículo para procesar el stream hasta la pantalla. La actividad ilegal reside en la venta o el abono mensual para tener acceso a la aplicación o a las listas de archivos de texto m3u que proveen el link final al contenido deseado empleando una EPG. Estas listas deben ser actualizadas periódicamente debido a los cambios permanentes de las IP del contenido. Esta modalidad tiene un perfil fuertemente elusivo de las medidas de control. En Uruguay este fenómeno ha adquirido mayor vigor debido a la alta calidad de los accesos a Internet.

Ante el impacto que provoca en el churn de los operadores de cable, ANDEBU ha adoptado una fuerte estrategia defensiva por múltiples caminos que está colaborando eficientemente a este combate.

Las principales líneas desarrolladas son:

- Constituir un pequeño grupo multidisciplinario con reuniones frecuentes y que gestione todas las actividades. Lo integran abogados, ingenieros, especialista en plataformas, así como las partes interesadas como los representantes de los operadores de cable y los propietarios de los derechos de las señales.
- Línea 1. Atacar las vías electrónicas de publicidad y venta. En este sentido hemos acordado procedimientos muy ágiles y en tiempos muy cortos, para el bloqueo de anuncios probadamente ilegales con Facebook y Mercado Libre. Ambas empresas han mostrado un fuerte compromiso con estas acciones. A la fecha se ha eliminado virtualmente toda la publicidad que en su momento fue la principal fuente para la venta. Igualmente se está desarrollando la preparación para acuerdos o para las acciones de denuncias con otras plataformas. En general las plataformas tienen una alta disposición y mecanismos para asegurar el respeto a los Derechos de Autor y ANDEBU agrupa además a los principales productores de contenido de Uruguay.
- Línea 2. Medios de Pago. Con ellos se ha logrado el bloqueo de cuentas dificultando la percepción de los ingresos de los piratas.
- Línea 3. Denuncias penales ante la justicia, las que se están llevando a cabo en múltiples ciudades con particular éxito. Las consecuencias han sido importantes en la medida en que se han logrado cerrar bocas de venta y clausurar los servicios, se ha obtenido información de clientes y proveedores, y han tomado estado público como noticia policial concientizando a la población y

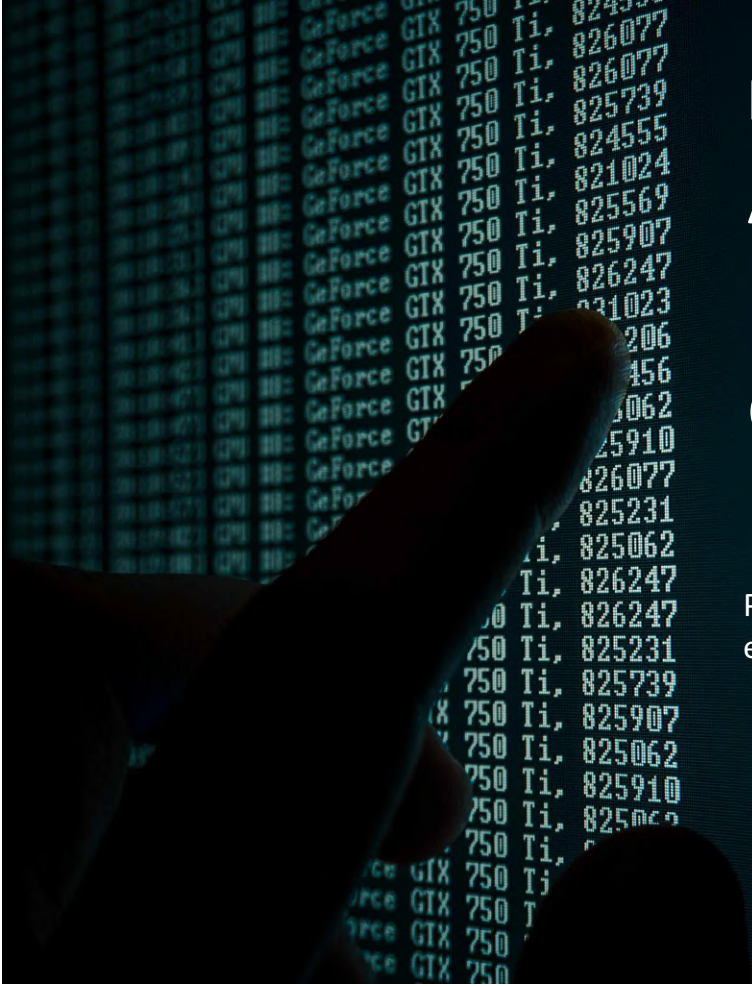


desanimando incurrir en este delito. En las ciudades donde se tomaron acciones se ha observado el retorno de clientes a los operadores. Esta acción debilita en general el interés por la piratería, máxime considerando que en Uruguay también quien compra es perseguible penalmente.

- Línea 4. Generación de spots de TV mostrando que quien compra contenido ilegal no solamente está cometiendo un delito, sino que además pone en riesgo su persona y bienes al entregar datos personales y de pago a delincuentes. Está línea está en proceso de implementación.
- Línea 5. Trabajo con las autoridades a los efectos de lograr acciones de bloqueo de las IP de publicación de las listas o de la ubicación del contenido final. Esta línea presenta algunas dificultades, en las que se está trabajando, ya que implica disponer de un marco legal sólido. Estas dificultades de implementación ya se han observado en otros países, entre ellos algunos europeos.
- Línea 6. Trabajo conjunto con otras instituciones importantes como ASIET y la Alianza contra la Piratería de la TV Paga. ASIET ha colaborado internacionalmente en nuestra lucha y además le ha dado visibilidad internacional. La Alianza acaba de reestructurarse creando una Junta Directiva para unificar esfuerzos de proveedores de señales, de servicio y de tecnología en América Latina, y volverla una herramienta eficaz a nivel continental. Consideramos a ambas como apoyo internacional en este emprendimiento.

ANDEBU entiende que la persecución y neutralización persistente de la piratería en varios frentes como los mencionados, y en algunos que estamos abriendo, son las calves para su debilitamiento y eventual eliminación.

Omar de León es Presidente de la Asociación Nacional de Broadcasters de Uruguay para el período 2017 - 2019. Es Director de Teleconsult y sus proyectos y estudios se extienden a más de treinta países de las Américas, Europa y África. Es consultor de la UIT, el CAF, ASIET, el Banco Mundial, la CEPAL, COMTELCA y LACNIC, entre otros organismos internacionales. Ha sido Profesor de la Facultad de Ingeniería durante 35 años y ha publicado diez libros de telecomunicaciones.



Protección de datos

Actualidad sobre la Protección de Datos de Carácter Personal en Panamá

Por la **Dra. Nadia A. Ortiz Q.**, miembro del
equipo de Ipandetec

Desde el año 2004 con la última reforma constitucional a nuestra Carta Magna, la República de Panamá reconoció la importancia del derecho a la autodeterminación informativa o libertad informática al otorgarle a este derecho rango constitucional e incluirlo en el Título III correspondiente a los Derechos Fundamentales, Capítulo I sobre Garantías Fundamentales. Quince años han transcurrido para que el ordenamiento jurídico panameño cuente con una normativa dedicada exclusivamente a la protección de datos de carácter personal. Esto es así toda vez que desde el pasado 26 de marzo de 2019, se promulgó la Ley No. 81 sobre Datos de Carácter Personal.

No obstante lo anterior, pese a esta reciente promulgación específica en protección de datos de carácter personal, el ordenamiento jurídico panameño contaba con una plétora de normas legales en diferentes áreas (salud, historial crediticio, telecomunicaciones, bancaria, entre otras), que regulaban de forma dispersa diversos aspectos de la protección de datos de carácter personal. Para la referencia del lector, a continuación le detallamos las diversas normativas que han regulado y continúan normando la protección de datos personales en Panamá. Hemos de señalar que dichas excertas legales no han perdido validez, puesto que pese a la promulgación de la Ley No. 81 de 2019, las mismas siguen siendo aplicadas.

15 años han transcurrido para que el ordenamiento jurídico panameño cuente con una normativa dedicada exclusivamente a la protección de datos de carácter personal

- Ley No. 26 de 17 de diciembre de 1992, por la cual se dictan medidas de profilaxis y control de la epidemia del Síndrome de Inmuno Deficiencia Adquirida (SIDA) y de propagación del Virus de Inmuno Deficiencia Humana.
- Ley No. 31 de 8 de febrero de 1996, regula las telecomunicaciones. Reglamentada por el Decreto Ejecutivo No. 73 de 9 de abril de 1997.
- Ley No. 11 de 22 de enero de 1998, sobre información almacenada en medios informáticos.
- Ley No. 6 de 22 de enero de 2002, sobre Transparencia en la Gestión Pública, establece el derecho del habeas data y dicta otras disposiciones.
- Ley No. 68 de 20 de noviembre de 2003, que reglamenta la Ley No. 68 de 20 de noviembre de 2003, que

regula los derechos y obligaciones de los pacientes, en materia de información y de decisión libre e Informada.

- Ley No. 4 de 18 de mayo de 2006, modifica y adiciona artículos a la Ley No. 24 de 22 de mayo de 2002, que regula el servicio de información sobre historial de crédito de los consumidores. Modificada por la Ley No. 135 de 31 de diciembre de 2013.
- Decreto Ejecutivo No. 263 que crea el Consejo de Seguridad y dicta otras disposiciones.
- Ley No. 83 de 9 de noviembre de 2012, regula el uso de los medios electrónicos para los trámites gubernamentales y modifica la Ley No. 65 de 2009, que crea la Autoridad Nacional de Innovación Gubernamental (AIG).
- Ley No. 33 de 25 de abril de 2013, crea la Autoridad Nacional de Transparencia y Acceso a la Información.
- Decreto Ejecutivo No. 511 de 24 de noviembre de 2017, que adopta la política pública de transparencia de Datos Abiertos de Gobierno.

El ordenamiento jurídico panameño cuenta con normas que protegen los datos bancarios y crediticios de los, datos médicos o de salud, y delega en la Autoridad Nacional de Transparencia y Acceso a la Información el respeto y vigilancia de los derechos ARCO de la población panameña.

Cada una de las normativas citadas se centra en regular la protección de datos personales en su área de acción, es decir, la Ley No. 26 de 17 de diciembre de 1992, regula la protección de datos personales médicos de pacientes con el Síndrome de Inmuno Deficiencia Adquirida (SIDA) y establece un deber de confidencialidad del personal médico que atiende a dichos pacientes. Por otro lado, la Ley No. 68 de 20 de noviembre de 2003, que reglamenta la Ley No. 68 de 20 de noviembre de 2003, que regula los derechos y obligaciones de los pacientes, en materia de información y de decisión libre e informada es a su vez, aplicable al ámbito de la protección de datos en materia de salud.

En consecuencia, el ordenamiento jurídico panameño cuenta con normas que protegen de forma puntual los datos bancarios y crediticios de los panameños, sus datos médicos o de salud, e igualmente, delega en un ente gubernamental como lo es la ANTAI (Autoridad Nacional de Transparencia y Acceso a la Información), el respeto y vigilancia de los derechos ARCO de la población panameña. En virtud de lo an-

terior, somos de la opinión que se desaprovechó la oportunidad de que a través de la Ley No. 81 de 26 de marzo de 2019, se uniformaran aspectos inherentes a las medidas de seguridad aplicables a los datos de carácter personal atendiendo a su naturaleza, si son datos médicos, sobre el historial crediticio, datos bancarios, etc., puesto que no existe uniformidad entre los diferentes niveles de seguridad para los datos enunciados, cuando son datos sensibles que requieren estrictas medidas de seguridad.

Sin embargo, la realidad es que contamos en nuestro ordenamiento jurídico con la Ley No. 81 de 2019, normativa que consta de siete capítulos y cuyo propósito es establecer principios, derechos, obligaciones y procedimientos que regulen la protección de datos personales. La nueva normativa sobre protección de datos personales establece como regla que se permite el tratamiento de datos personales con apego al contenido de la ley en comento. En este sentido, para una mejor referencia, la Ley No. 81 de 2019 dispone sobre los siguientes aspectos a saber:

- Se incluyen en el artículo 2, los nueve principios inherentes a la protección de datos personales (lealtad, finalidad, proporcionalidad, veracidad y exactitud, seguridad de los datos, transparencia, confidencialidad, licitud, portabilidad).
- La ley dispone las situaciones en las cuales su contenido no es aplicable (art. 3).
- Se incluye un glosario de términos y en el mismo se detallan los actores o sujetos intervinientes en materia de protección de datos personales (artículo 4). En el caso específico de la jurisdicción panameña se describen al responsable del tratamiento, al custodio de la base de datos y al titular de los datos. En este mismo sentido, las responsabilidades para las figuras enunciadas aparecen desarrolladas posteriormente en el artículo 7 para el responsable del tratamiento, en el artículo 14 para el custodio de la base de datos y en artículo 24 para ambas figuras respectivamente.
- Se dispone en el artículo 5 sobre la territorialidad de las bases de datos que se encuentren radicadas en el territorio de la República de Panamá o cuando el responsable del tratamiento este domiciliado en territorio panameño.
- La ley desarrolla las situaciones en las cuales es viable la realización del tratamiento de datos personales, para lo cual requiere del cumplimiento de una serie de condiciones recogidas en el artículo 6.
- Las situaciones en las cuales no se requiere autorización para la realización del tratamiento de datos personales son explyadas en el artículo 8 de la ley.



Es necesario que se organicen jornadas, campañas, actividades, talleres de instrucción, educación y **capacitación para la población** en general, a través de diferentes medios de comunicación, tendentes por un lado a instruir, pero sobre todo a **crear conciencia** de lo relevante que es cuidar nuestra **información personal**.

- En el artículo 9, se instaure el deber de confidencialidad para las personas que tengan acceso o estén involucradas en el tratamiento de datos personales, deber de exigible cumplimiento tanto para organismos públicos como privados.
- Las situaciones en las cuales el tratamiento de datos personales se realice atendiendo a la figura del mandato son expuestas en el artículo 10.
- En el artículo 11 se desarrolla el principio de finalidad, licitud, exactitud aplicable a la protección de datos personales.
- Como regla general se establece en el artículo 13, que los datos sensibles no pueden ser objeto de transferencia. No obstante lo anterior, las excepciones a dicha regla fueron a su vez incluidas en el mencionado artículo de la Ley No. 81 de 2019.
- Se desarrollan los derechos ARCO (acceso, rectificación, cancelación, oposición y portabilidad) son explicados en el contenido del artículo 15.
- Se fijan plazos de tiempo en el artículo 16, para recibir respuesta al ejercitar el titular de los datos sus derechos ARCO. Por ejemplo, el titular de los datos al ejercitar su derecho de acceso ante el responsable del tratamiento debe recibir respuesta a su petición en un plazo no mayor de 10 días hábiles. En tanto para modificar datos erróneos, inexactos, equívocos o incompletos deberá hacerse dentro de los cinco días hábiles siguientes a la solicitud de modificación de conformidad con la redacción del artículo 17.
- En el artículo 18, se le dotan al titular de los datos de los mecanismos de actuación para el correcto ejercicio de sus derechos ARCO. Por consiguiente, el titular debe acudir en primera instancia ante el responsable del tratamiento sea un ente público o privado y este debe responder la solicitud del titular de los datos. De no mediar respuesta a la solicitud del titular de los datos por parte del responsable del tratamiento, entonces el titular puede concurrir ante la ANTAI.
- El derecho a no ser objeto de decisiones individualizadas como consecuencia de la realización de un tratamiento de datos personales es desarrollado en el artículo 19 de la norma en referencia.
- El artículo 20 contempla la autorización para el tratamiento de datos personales que se efectúe en establecimientos de salud públicos o privados.
- De conformidad con el contenido del artículo 21, el ejercicio de los derechos ARCO no puede estar limitado me-

diante ningún acto o convenio entre las partes y de existir dicho acto de limitación se declara nulo.

- Se dispone como regla general que los responsables de los tratamientos solo podrán transmitir información cuando tengan el consentimiento previo, informado e inequívoco del titular de los datos (artículo 25).
- Los operadores que gestionen redes públicas o que presten servicios de comunicación tienen el deber de garantizar la protección de los datos personales que manejen (artículo 26).
- Transcurridos siete años desde que se extingue la obligación legal de conservar los datos, ni el responsable del tratamiento ni el custodio pueden transferir o comunicar dichos datos que se relacionen con una persona identificada o identificable (artículo 28).
- Las entidades públicas que sometan a tratamiento datos personales relativos a condenas por delitos, infracciones administrativas o faltas disciplinarias no podrán comunicarlo, una vez prescrita la acción penal o administrativa o cumplida o prescrita la sanción o la pena salvo autorización expresa por el titular de los datos (artículo 30).
- De conformidad con el artículo 31, se dispone que los responsables y/o custodios de las bases de datos que transfieran datos personales almacenados en bases de datos a terceros llevarán un registro de estas y las mismas deberán estar a disposición de la ANTAI.
- Se establecen en el artículo 33, algunos lineamientos o condiciones para la realización de transferencia de datos personales.
- A través del Capítulo IV, se crea el Consejo de Protección de Datos Personales (artículo 34) y se enuncian los miembros que lo conformarán (artículo 35). Igualmente, se listan las facultades con las que cuenta dicho consejo.
- En el Capítulo V de la ley, denominado Responsabilidad por las Infracciones se dispone que la ANTAI es el ente que fijará los montos por las sanciones aplicables a las respectivas faltas tomando en consideración la gravedad de las mismas. El rango de dichas multas de conformidad con el artículo 36, es de mil (US\$ 1,000.00) a (US\$10,000.00) balboas.
- Se dispone en el artículo 37, que el responsable del tratamiento de datos personales deberá indemnizar el daño patrimonial y/o moral que causara el tratamiento indebido de datos.
- Se realiza una clasificación de las infracciones y sanciones en leves, graves o muy graves en el Capítulo VI de

la ley y se detallan en qué consisten cada una de dichas categorías (artículos 38-41).

- En las Disposiciones Finales de la ley contenidas en el Capítulo VII se dispone que la ley comenzará a regir a los dos años de su promulgación es decir, para el año 2021 (artículo 47).

Aunado al despliegue realizado sobre el contenido de los temas abarcados por la Ley No. 81 de 26 de marzo de 2019, hemos de enunciar que entre las medidas o acciones actuales y reales de protección de los datos personales tenemos que en el caso de bases de datos manejadas por tanto entes públicos o gubernamentales, como entes privados, el titular de los datos puede concurrir ante los entes que estén manejando su información sea por ejemplo, Autoridad Panameña de Crédito, entidades bancarias, clínicas y hospitales a ejercitar sus derechos ARCO. En el caso que el titular de los datos no logre una tutela-protección-respeto, efectiva de sus derechos ARCO puede hacer uso de un recurso de amparo de garantías constitucionales basado en el hecho de que la autodeterminación informativa o libertad informática es un derecho fundamental amparado en la Constitución Política de la República de Panamá.

Debemos ser ciudadanos responsables y cuestionar sobre los destinos de nuestra información, la cual es proporcionada para la realización de nuestras actividades diarias tanto en el mundo real como en el mundo virtual o digital

Por otro lado, y considerando que aún la Ley No. 81 de 2019, no ha empezado a regir, es necesario que se organicen jornadas, campañas, actividades, talleres de instrucción, educación y capacitación para la población en general y sus diversos grupos (empresarios, médicos, banqueros, familias, adolescentes, infantes), a través de diferentes medios de comunicación, tendentes por un lado a instruir, pero sobre todo a crear conciencia de lo relevante que es cuidar nuestra información personal, partiendo de la premisa de que la información es poder y que una vez la información personal es liberada por nosotros, desconocemos los destinos exactos de la misma y el uso que se les dará. En virtud de lo anterior, con la finalidad de reducir las irrupciones no deseadas en nuestra vida privada, debemos ser ciudadanos responsables y cuestionar sobre los destinos de nuestra información la cual es proporcionada para la realización de nuestras actividades diarias tanto en el mundo real como en el mundo virtual o digital.

Voces

Moderación de contenidos en Internet: una propuesta latinoamericana para proteger a los usuarios ante las grandes plataformas

Las grandes plataformas de Internet representan en la actualidad una nueva esfera pública, un espacio de discusión clave para la deliberación democrática y el ejercicio de derechos fundamentales. Allí, la creciente intervención de esos intermediarios en los contenidos en línea mediante la adopción de términos de servicio y la aplicación de políticas empresariales de moderación, tiene repercusiones directas en el ejercicio de derechos de sus usuarios, entre ellos, la libertad de expresión.

En este escenario, OBSERVACOM junto con Intervozes e IDEC de Brasil, Desarrollo Digital de Argentina y expertos nacionales e internacionales, elaboramos un documento con Aportes para una regulación democrática de las grandes plataformas que garantice la libertad de expresión en Internet. La iniciativa plantea una perspectiva latinoamericana sobre la gobernanza de Internet que garantice procesos de moderación privada de contenidos compatibles con los estándares internacionales de derechos humanos.

Es importante que las plataformas cuenten con mecanismos para permitir un efectivo derecho a defensa y reparación de sus usuarios. (...) Deberían notificar y ofrecer una justificación clara en casos de remoción o restricción de contenidos, así como poner a disposición información sobre cómo recurrir.

La propuesta postula un modelo de co-regulación para el establecimiento de criterios de regulación asimétrica y progresiva que tome en cuenta el poder de mercado significativo de las plataformas. Desde el punto de vista de los derechos de los usuarios hay tres aspectos que queremos destacar en esta iniciativa: los referidos a los términos y condiciones de servicio; la transparencia; y el derecho a defensa. En relación con los términos y condiciones de servicio, postulamos que éstos deberían ser claros, precisos, accesibles y estar alineados con los estándares y principios internacionales de derechos humanos. Además, no deberían conceder poder ilimitado y discrecional a las plataformas para determinar la idoneidad del contenido generado por el usuario. En este sentido, las plataformas no deberían implementar filtros automáticos que eliminen contenidos publicados por sus usuarios, excepto en aque-



Una colaboración de Ana Bizberge, editora de contenidos de OBSERVACOM

llos casos que se trate de contenidos manifiestamente ilegales que, al mismo tiempo, sean reconocidos como limitaciones legítimas a la libertad de expresión en las declaraciones o tratados internacionales de derechos humanos.

Otra excepción para la remoción de contenidos puede ser cuando se trata de contenidos que -aún cuando no sean reconocidos como ilegales-, causen daños serios, inminentes e irreparables o de difícil reparación a otras personas, o cuando se trata de contenidos que podrían afectar a públicos específicos como niñas, niños y adolescentes. En cualquier caso, la restricción de contenidos se realizaría como medida cautelar, no definitiva, sujeta a revisión.

Es así que la toma de decisiones sobre contenidos por parte de las plataformas debería respetar el principio de progresividad y proporcionalidad, garantizando el respeto al debido proceso y adoptando medidas menos onerosas que la remoción, optando por mecanismos de aviso o notificación u otras.

En materia de transparencia, la propuesta regulatoria postula que cuando el contenido es restringido, el intermediario debería exhibir un aviso claro explicando qué contenido se eliminó y por qué. En el caso de contenido comercial, patrocinado o político, debería ser claramente identificado, y las plataformas deberían informar a sus usuarios, de forma clara, explícita y accesible sobre el tipo de contenido prohibido, criterios de curaduría y moderación.

Es importante que las plataformas cuenten con mecanismos para permitir un efectivo derecho a defensa y reparación de sus usuarios. En este sentido, todas las plataformas de contenido deberían notificar a los usuarios y ofrecer una justificación clara en casos de remoción o restricción de contenidos, así como poner a disposición información sobre cómo recurrir la decisión. Para eso es central que los usuarios puedan acceder a recursos legales en su país para responder a las decisiones y contar con mecanismos de reparación frente a la eventual violación de sus derechos.

La propuesta “Aportes para una regulación democrática de las grandes plataformas que garantice la libertad de expresión en Internet”, se puede consultar en español, inglés y portugués en el sitio web de OBSERVACOM. Actualmente, el documento está abierto a comentarios hasta el 15 de octubre. También se reciben firmas de organizaciones que actúen sobre el tema en América Latina. Se pueden realizar comentarios y adhesiones por mail a contacto@observacom.org

Contenido mediapartner

Digital Policy & Law

Derechos de los usuarios y nueva Norma Oficial de protección en México

Colaboración de **Jorge Bravo**, Director General de **Digital Policy & Law**



México tiene una nueva Norma Oficial (NOM-184-SCFU-2018) que regula la comercialización y/o prestación de servicios de telecomunicaciones, que entró en vigor en septiembre de 2019.

Dicha NOM-184, que cancela la de 2012, establece los elementos normativos y las obligaciones específicas que los proveedores de servicios de telecomunicaciones deben cumplir en la comercialización y/o prestación de los servicios de telecomunicaciones, así como los requisitos mínimos que deben contener los contratos de adhesión que los operadores utilicen con los consumidores en sus relaciones comerciales. Lo anterior, para garantizar la protección de los derechos de los consumidores y para que éstos cuenten con la información suficiente para tomar las decisiones que más convengan a sus intereses.

Corresponde a la Secretaría de Economía y a la Procuraduría Federal del Consumidor (Profeco) vigilar y verificar el cumplimiento de NOM-184, así como sancionar el incumplimiento de sus disposiciones con base en la Ley Federal de Protección al Consumidor. Por su parte, el Instituto Federal de Telecomunicaciones es el responsable de vigilar la calidad de los servicios de telecomunicaciones, conforme a la legislación en la materia.

Al primer trimestre de 2019, México tenía 118.6 millones de líneas de telefonía móvil, una penetración de 95 por ciento. Asimismo, 88 millones de líneas de servicio móvil de acceso a Internet (prepago y pospago), equivalentes a 70 accesos por cada 100 habitantes.

Por su parte, el total de líneas de telefonía fija alcanzó 21.1 millones o 61 líneas por cada 100 hogares. En cambio, el total de accesos del servicio fijo de Internet superó las 18.6 millones de líneas, una penetración de 54 por ciento.

Derechos de los usuarios

Debe recordarse que en 2013 se aprobó y publicó en México una reforma constitucional en materia de telecomunicaciones y competencia económica. Entre otros temas, en ella se menciona que la ley establecerá los derechos de los usuarios de telecomunicaciones, de las audiencias, así como los mecanismos para su protección. La Ley Federal de Telecomunicaciones y Radiodifusión se publicó en el Diario Oficial de la Federación el 14 de julio de 2014. El Título Noveno de la mencionada ley reúne un catálogo de 21 derechos de los usuarios de los servicios de telecomunicaciones en México, los cuales se condensan en la siguiente tabla.

Derechos de usuarios de telecomunicaciones de México

1. Consultar gratuitamente el saldo en el caso de servicios móviles de prepago sin condicionamiento a comprar saldo adicional.
2. Protección de los datos personales.
3. Portabilidad numérica gratuita dentro del plazo de 24 horas.
4. Elegir libremente al proveedor de servicios.
5. Contratar y conocer las condiciones comerciales de los contrato de adhesión, registrados ante la Profeco.
6. Libre elección y no discriminación en el acceso a los servicios de Internet.
7. Provisión de servicios de telecomunicaciones conforme a los parámetros de calidad contratados.
8. Notificación de cualquier cambio en las condiciones originalmente contratadas.
9. Exigir el cumplimiento forzoso del contrato cuando el proveedor del servicio modifique las condiciones originalmente contratadas.
10. Rescindir el servicio contratado o cambiar de paquete o plan, en forma anticipada pagando, en su caso, el costo remanente del equipo.
11. Solicitar y obtener el desbloqueo del equipo terminal cuando concluya la vigencia del contrato o se haya liquidado su costo.
12. Desbloqueo del equipo terminal móvil cuando lo pague de contado, liquide su costo o venza el plazo inicial de contratación.
13. Bonificación o descuento por fallas en el servicio o cargos indebidos.
14. Prohibida toda discriminación motivada por origen étnico o nacional, género, edad, discapacidades, condición social, de salud, religión, opiniones, preferencias sexuales, estado civil o cualquier otra que atente contra la dignidad humana.
15. A la manifestación de las ideas, acceso a la información y a buscar, recibir y difundir información e ideas.
16. A que en los servicios móviles de prepago el saldo no consumido a la fecha de su expiración, le sea abonado en las recargas que se lleven a cabo dentro del año siguiente a dicha fecha.
17. A que cuando se haya suscrito un contrato de adhesión, sólo se pueda cambiar a otro por acuerdo de las partes.
18. Cancelar el contrato sin necesidad de recabar autorización del concesionario ni penalización alguna cuando el plazo pactado concluya.
19. No recibir llamadas de promoción de servicios o paquetes a menos que expresamente manifieste su consentimiento.
20. A que cuando se renueve el contrato de servicios móviles y no adquiera un nuevo equipo, la mensualidad se integre exclusivamente por el cobro de los servicios sin pago del equipo.
21. A que en los contratos de servicios móviles se transparente, en el pago mensual, la parte que corresponda al costo de los servicios y la que corresponda al costo del equipo o instalaciones.

Con el objetivo de garantizar los derechos de los usuarios de servicios de telecomunicaciones, la NOM-184 incorpora las disposiciones en materia de regulación asimétrica en beneficio de todos los consumidores. En la elaboración de la Norma Oficial participaron instituciones como la Asociación Nacional de Telecomunicaciones (Anatel) de México, la Asociación Mexicana de Internet (Amipci), la Cámara Nacional de la Industria Electrónica de Telecomunicaciones y Tecnologías de la Información (Canieti), además del Instituto Federal de Telecomunicaciones (IFT) y la Profeco.

La NOM-184 contempla disposiciones generales, elementos informativos a favor del consumidor contratante, condiciones de los contratos de adhesión, aspectos referentes a la atención al consumidor, las características que deben contener las facturas, las causas de suspen-

sión e interrupción del servicio, sobre las devoluciones y bonificaciones, así como garantías de los equipos terminales de telecomunicaciones.

La reforma constitucional en materia de telecomunicaciones y competencia económica menciona que la ley establecerá los derechos de los usuarios de telecomunicaciones, de las audiencias, así como los mecanismos para su protección

Información para decidir mejor

La Norma busca garantizar que el proveedor preste los servicios de telecomunicaciones de acuerdo con los términos y condiciones ofrecidos o convenidos con el consumidor, o que se encuentren implícitos en la publicidad del propio operador. En caso de incumplimiento, el usuario puede exigir el cumplimiento, aceptar otro bien o servicio equivalente de igual o mayor calidad o precio, la rescisión del contrato o la devolución o ajuste en la factura de la cantidad pagada o por pagar.

El consumidor tiene derecho de dar por terminado de forma anticipada el contrato de adhesión en cualquier momento, pero sujetándose a las penas convencionales establecidas en el mismo, las cuales deben ser razonables, recíprocas, equitativas y proporcionales. Corresponde a la Profeco resolver y definir esos criterios.

La Norma busca garantizar que el proveedor preste los servicios de telecomunicaciones de acuerdo con los términos y condiciones ofrecidos o convenidos con el consumidor, o que se encuentren implícitos en la publicidad del propio operador.

Los operadores siempre deben proveer una factura, recibo o comprobante donde consten los datos específicos de comercialización. Siempre que un consumidor desee contratar algún servicio, el proveedor debe entregar una Carta de Derechos Mínimos de los Usuarios de los Servicios Públicos de Telecomunicaciones al Consumidor.

El estado de cuenta o factura debe contener de manera desglosada la descripción de los cargos, costos, conceptos y naturaleza de los servicios, y darla a conocer a los consumidores por lo menos diez días naturales antes de la fecha de vencimiento, incluidos los lugares en los cuales puede efectuarse dicho pago.

En el caso de que el usuario haya contratado servicios adicionales al de telecomunicaciones, los prestadores deben desglosar los conceptos de cada uno de los servicios en la factura. Para los proveedores de Internet, éstos deben proporcionar el consumo de datos en el periodo de facturación. Obviamente, el proveedor no puede cobrar tarifas o conceptos diferentes a los previstos en las condiciones contratadas.

En términos informativos, el proveedor está obligado a informar y explicar el contenido del contrato de adhesión, previo a la contratación. Asimismo, el cliente tiene dere-



cho a conocer si el equipo que adquirirá se encuentra bloqueado, cómo desbloquearlo (sin costo) en un plazo máximo de 24 horas y sin exigir mayores requisitos, así como las condiciones de garantía del equipo. El usuario tiene derecho a utilizar un equipo terminal propio para recibir el servicio, en tanto que el proveedor debe informar si dicho dispositivo cumple con las características mínimas necesarias para recibir la prestación del servicio, así como sus consecuencias.

En lo que se refiere a la publicidad relacionada con la prestación del servicio de telecomunicaciones que difunda el proveedor, debe ser en español, veraz, comprobable y exenta de textos, diálogos, sonidos, imágenes, marcas, denominaciones de origen y otras descripciones que induzcan o puedan inducir a error o confusión por engañosas o abusivas.

Respecto de los planes o paquetes de servicios de telecomunicaciones, el proveedor también tiene algunas obligaciones, entre ellas: los servicios que incluye el plan; la descripción, características, contenido y restricciones de cada uno de los servicios; los principales cargos adicionales; los servicios gratuitos y el plazo de los mismos; los requisitos de cancelación (mediante mecanismos expeditos) y los ajustes por la cancelación de uno o más servicios de telecomunicaciones que formen parte del plan o paquete.

Los proveedores deben proporcionar a sus consumidores, cuando éstos lo requieran y de forma gratuita, el saldo disponible, vigencia y condiciones de uso y el consumo realizado de todos los servicios. Cuando el consumidor realice una recarga de saldo, el operador debe informar el monto de la recarga y su fecha de expiración.

Contratos de adhesión

Los contratos de adhesión son el instrumento legal que incluye los términos y condiciones aplicables a la comer-



cialización y/o la prestación del servicio de telecomunicaciones, los cuales deben estar registrados ante el IFT y la Profeco. Dichos documentos deben incluir los datos del proveedor, los del consumidor, la descripción del servicio a prestarse, las tarifas previamente registradas ante el regulador, el plazo de contratación, el equipo terminal provisto, el método de pago, las penas convencionales, entre otras condiciones.

En ningún caso los contratos deben contener cláusulas que le permitan al operador modificar o sustraerse unilateralmente de sus obligaciones; trasladar la responsabilidad del proveedor a terceros que no formen parte del contrato de adhesión; obligar al consumidor a renunciar a la protección de la legislación o a sus derechos; que lo sometan a la competencia de tribunales extranjeros; condicionar la prestación del servicio a la adquisición de algún bien, producto o servicio adicional; y realizar prácticas desleales, abusivas o discriminatorias por parte del operador.

El objetivo es proteger los derechos de los consumidores y facilitarles elementos informativos para tomar decisiones a la hora de contratar servicios de telecomunicaciones.

Específicamente en los contratos referentes al esquema de prepago, el usuario debe conocer los medios para hacer recargas y consulta de saldo, los servicios de roaming internacional, la cobertura y las causales de suspensión o interrupción del servicio, incluidas las fortuitas y de fuerza mayor. Asimismo, el consumidor debe poder consultar el Aviso de Privacidad; los medios para la aten-

ción de consultas, reclamaciones y/o quejas; así como el derecho a la portabilidad numérica y las vías para reportar el robo o extravío de la línea y/o el equipo terminal.

En caso de que el servicio no se preste o proporcione en la forma y términos expuestos en la publicidad, el operador debe compensar al consumidor la parte proporcional del precio del servicio que se dejó de prestar y, como bonificación, al menos 20 por ciento del monto del periodo de afectación en la prestación del servicio contratado. Asimismo, el proveedor debe efectuar la devolución de los cargos que realice de forma indebida dentro de los cinco días hábiles siguientes a la reclamación correspondiente.

Atención al consumidor

Los proveedores deben contar con sistemas o mecanismos de atención al cliente o consumidor, con personal debidamente capacitado y que brinde un trato respetuoso. El usuario debe poder elegir el mecanismo de su preferencia para recibir y atender dudas, aclaraciones y reclamaciones, siempre de forma gratuita, tales como número telefónico, correo electrónico, establecimientos y/o a través de medios físicos o digitales.

Con excepción de los establecimientos físicos, los mecanismos electrónicos deben brindar atención las 24 horas del día los 365 días del año. También se deben de poder realizar cancelaciones de servicio u obtener información sobre tarifas, condiciones de planes, promociones u ofertas y realizar trámites relacionados con sus servicios.

En caso de suspensión del servicio, el consumidor debe ser notificado, incluida la causa que lo ocasiona. Cuando la causa que originó la suspensión temporal del servicio por falta de pago sea imputable al consumidor y haya sido solventada, la reanudación del servicio de telecomunicaciones debe realizarse en un periodo máximo de 48 horas, debiendo pagar los cargos por reconexión, los cuales deben de ser razonables y proporcionales.

Como se aprecia en este apretado resumen, la Ley Federal de Telecomunicaciones y Radiodifusión de 2014 plasma los derechos de los usuarios de servicios de telecomunicaciones en México. Por su parte, la NOM-184 actualiza la Norma Oficial anterior e incorpora no sólo los derechos de los usuarios, sino las disposiciones regulatorias en la materia, hace convivir en el instrumento legal a las autoridades de protección al consumidor y regulatoria de telecomunicaciones y, finalmente, establece las condiciones, obligaciones específicas y requisitos mínimos que los proveedores de servicios deben cumplir en la comercialización y/o prestación de los servicios de telecomunicaciones. El objetivo es proteger los derechos de los consumidores y facilitarles elementos informativos para tomar decisiones a la hora de contratar servicios de telecomunicaciones.

OPINIÓN



Andrés Sastre

Director Regional
de ASIET

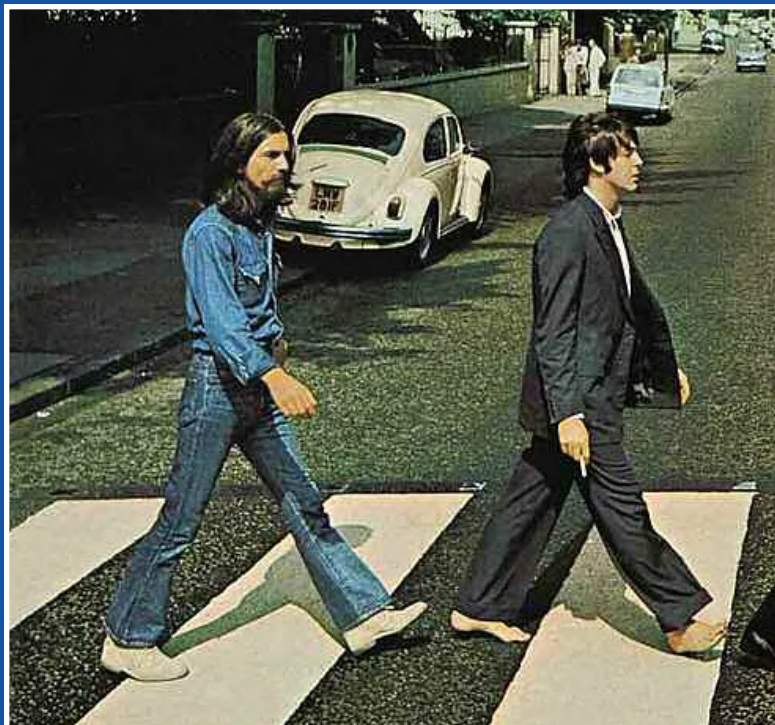
@asaspor

Something in the way

«... la verdad, cuya madre es la historia, émula del tiempo, depósito de las acciones, testigo de lo pasado, ejemplo y aviso de lo presente, advertencia de lo por venir» El ingenioso hidalgo Don Quijote de la Mancha. Miguel de Cervantes.

Este mes de septiembre se cumplen 50 años del lanzamiento del disco de los Beatles "Abbey Road", más allá de lo excepcional del famoso LP, su portada es una sátira en reacción a una extendida leyenda urbana de la época. Aquella "fake news" aseguraba que Paul McCartney había fallecido en un accidente de tráfico y había sido sustituido en la banda por William Campbell. En la icónica imagen se observa a un John Lennon vestido de clérigo presidiendo de blanco inmaculado una procesión seguida por Ringo con traje de funerario, y Paul a paso cambiado y descalzo, que sería el muerto; cerrando la comitiva aparece un George Harrison como enterrador. Ni que decir tiene que antes de esta existieron cientos de noticias falsas con bastante más mala intención y peores consecuencias que esta, incluso políticas, Dreyfus por poner un ejemplo, o violentas como las persecuciones a los judíos en la Edad Media.

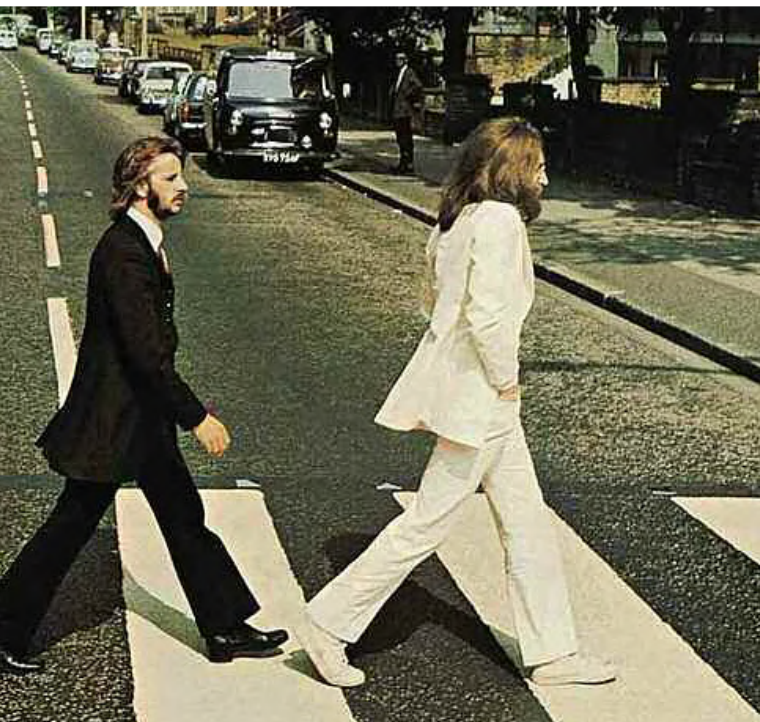
Entonces no existía Internet. La desinformación y las noticias falsas no son consecuencia de la red ni sus plataformas, pero su actual capacidad de difusión las viraliza con mayor intensidad que en el pasado, y hace más dificultoso su combate, porque incluso puede generarse información sesgada a la carta. Su alcance y efecto por tanto son hoy mucho mayores. Últimamente nos hemos limitado a ob-



servar cómo su capacidad de influencia en procesos electorales y decisiones de estado ha ido aumentando, e incluso han ayudado a aupar a movimientos y decisiones de corte populista e ideología ultra que incluso discuten postulados sobre los que hemos construido las bases de nuestros actuales estados de derecho. Se trata de un problema de gravedad que a día de hoy no deja fácil solución sin que en el mal que se pretende solucionar no se lleve por delante otro tipo de libertades fundamentales, sobre todo aquellas relacionadas con la libertad de expresión.

Por supuesto no existe una conspiración o ejército de bots unificado bajo un único comandante que de forma coordinada fabriquen noticias falsas para la desestabilización del sistema. Así bien tenemos que hablar de agentes diversos que se sirven de la capacidad de difusión y llegada a los ciudadanos que tienen las grandes plataformas y redes sociales para lanzar sus campañas, con menos esfuerzo y presupuesto del que antaño hubiese sido necesario.

Acertadamente en un principio, para que el desarrollo de las aplicaciones fuera viable y seguro se asentó la base de que los intermediarios no debían tener responsabilidad sobre lo que se publicaba en sus sitios. Más allá de que ante un contenido ilegal u ofensivo y previa solicitud éste fuera removido, quedaba claro que los intermediarios no debían de actuar como policías en la web, siendo que su tarea no era dedicarse a analizar el contenido que albergan. Es evidente que los recientes acontecimientos en procesos electorales mediante campañas de desinformación, unida a la proliferación de delitos de odio y violencia en vivo han hecho replantearse el grado de inmunidad de



las mismas, y pasar a exigir soluciones más proactivas de estas empresas por su capacidad de influencia a nivel global. Escándalos como el de Cambridge Analytica han provocado que desde las mismas empresas se busque una solución consensuada y escenarios estables que otorguen un marco de actuación seguro.

La rápida difusión y asimilación de noticias falsas se ve favorecida por el hecho de que en redes sociales, generalmente, el usuario agrega a aquellas personas con las que tiene más cercanía personal y afinidad ideológica, lo que ayuda a que la información que se comparte tienda a aceptarse como veraz y reafirmar ideas preconcebidas. Los algoritmos de las redes sociales han favorecido la consolidación de esta afinidad; el hecho de acceder solo a noticias de nuestro agrado o que confirmen nuestras posiciones, por más que estas noticias sean de dudoso origen o confiabilidad. El resto de noticias tienden a desaparecer.

En redes de mensajería instantánea el problema se multiplica, a información se viraliza rápidamente en grupos cerrados y el efecto burbuja es más potente aún, siendo el combate contra la desinformación todavía más complejo, puesto que una intervención en conversaciones privadas sería una vulneración muy grave de derechos fundamentales. La naturaleza transfronteriza de internet junto al hecho de que no tiene por qué haber correlación entre el lugar donde se genera la noticia y el lugar donde hace efecto, la difícil prevención de la difusión de contenido ilícito en vivo, dificultan además cualquier tipo de control sobre estos mensajes.

La solución no es fácil y tampoco va a ser única y completa. No es posible tolerar que aquellos que, amparándose en la protección ante este tipo de noticias, emitan regulaciones excesivas que lleven a una censura de facto en la red. Debemos avanzar hacia marcos de actuación conjuntos que delimiten de manera garantista y transparente, tanto para los usuarios como para las plataformas, la forma en la que se remueven contenidos con material ofensivo o delictivo. Los delitos de odio, el racismo, o la violencia en línea, son, dentro de la dificultad, más claramente combatibles, mientras que la falsedad o veracidad de una noticia a veces no es algo tan claro, y puede haber una delgada línea entre opinión y mentira. Nunca se va a poder impedir por completo la difusión de noticias falsas, no se pudo impedir antes de internet, menos en este momento tecnológico, pero sí podemos mitigar su efecto mediante el establecimiento de cánones de conducta, compromiso conjunto y patrones de actuación.

Avanzar en líneas como la creación de registros de portales de noticias que se tiene comprobado difunden contenido abusivo, falso e injurioso, y que hasta la fecha se lucran con ingentes cantidades derivadas de la publicidad, para precisamente cortar esa vía de financiación resulta necesario.

Las noticias de que recientemente twitter ha eliminado cientos de miles de cuentas que difundían contenidos falsos, que redes de mensajería instantánea como Whatsapp han reducido a 15 usuarios la posibilidad de compartir contenidos de forma simultánea, o avances en la transparencia respecto del origen de la publicidad en campañas electorales, van en la buena dirección sin duda. No obstante, esto debía quedar reflejado en la existencia de marcos de actuación armonizados a nivel global, para la propia tranquilidad de las empresas y también de cara a la transparencia de los comportamientos de las mismas ante los usuarios. Sin embargo, la proposición del parlamento brasileño de condenar hasta con 8 años de cárcel a quienes compartan información falsa; o la propuesta de regulaciones que coarten la libertad de expresión en función de un bien superior, no están en el camino adecuado, por su inviabilidad y peligrosidad para las libertades. Ni que decir tiene que no hacer nada o seguir amparándose en la falta de responsabilidad hacia lo que ocurre en tu interior hace tiempo que no es una opción.

Nos encontramos ante un problema grave del que quizás todavía estamos viendo los primeros coletazos, la buena noticia es que muchos han comenzado a ser conscientes de la situación. Efectivamente, no vamos a poder terminar con la difusión de información falsa, pero debemos procurar que el problema no ponga en jaque los estados de derecho tal y como los entendemos.

OPINIÓN



PALOMA SZERMAN

Senior Public
Policy Manager
en GSMA Latam

Los nuevos desafíos de privacidad y protección de datos personales en la era del 5G

No es exagerado decir que hay un *hype* alrededor de 5G; a la vez, es imposible negar que la llegada de la red móvil de próxima generación representa el desarrollo más significativo en la historia de las comunicaciones móviles. A diferencia de las transiciones de 2G a 3G y de 3G a 4G, 5G será más que un salto tecnológico.

La quinta generación permitirá una conexión confiable y flexible, a velocidades de gigabit/seg y con muy baja latencia. Las redes se adaptarán a las diversas necesidades. Esto se verá reflejado en nuevas aplicaciones de realidad virtual y aumentada, el uso expandido de inteligencia artificial, la realización de procedimientos quirúrgicos a distancia, el uso de vehículos autónomos y la digitalización de procesos productivos, por ejemplo.

Pero no se trata solo de aplicaciones y personas. 5G es la primera generación de red móvil diseñada para la comunicación máquina a máquina (M2M) y del Internet de las Cosas (IoT), dando lugar a una amplia gama de nuevos casos de uso que cambiarán la forma en que vivimos. De acuerdo a GSMA Intelligence, las conexiones de IoT a nivel mundial pasarán de 9.1 mil millones en 2018 a 25.2 mil millones para 2025.

Las aplicaciones nacidas del 5G llevarán a capturar y compartir una cantidad exponencialmente mayor de datos personales, muchos de los cuales pueden no haber sido capturados digitalmente con anterioridad. Es el caso de los dispositivos wearables, la información relativa a vehí-

culos conectados o las aplicaciones de smart cities. A su vez, al ser la primera generación diseñada para la comunicación M2M/IoT, los dispositivos en 5G podrán “hablar entre sí”.

“Las aplicaciones nacidas del 5G llevarán a capturar y compartir una cantidad exponencialmente mayor de datos personales, muchos de los cuales pueden no haber sido capturados digitalmente con anterioridad”

Ahora bien, ¿cuáles son los desafíos de privacidad y protección de datos personales en esta nueva era de conectividad ubicua? Desde la GSMA creemos que una regulación de privacidad inteligente, que permita desarrollar los nuevos modelos de negocios, tecnologías y capacidades de 5G a través de la innovación basada en datos, es aquella que empodera a los individuos y les otorga la confianza suficiente de que sus datos personales son utilizados de modo justo y seguro. Para ello, el establecimiento de mecanismos claros de rendición de cuentas –lo que en inglés se conoce como *accountability*– debe ser la piedra angular.

A la vez, un marco regulatorio de privacidad inteligente





está basado en principios flexibles. Es un marco horizontal, que se enfoca en abordar los riesgos de seguridad para los usuarios, siendo aplicable a todos los sectores de la economía y no estableciendo obligaciones o prescripciones específicas a una determinada tecnología. Estas características le permiten ser apto para el mercado M2M/IoT y el despliegue de redes 5G.

Por último, dentro de este marco general, tres áreas requieren mayor atención para que el ecosistema M2M/IoT pueda crecer y ofrecer funcionalidades a sus usuarios, sin descuidar su privacidad y seguridad:

- **¿Cuándo los datos recolectados por dispositivos M2M/IoT pueden ser considerados datos personales?** En el contexto de M2M/IoT adquiere relevancia la definición sobre qué se considera un dato personal. Es necesario tener en cuenta que incluso aquellos dispositivos que no son de uso personal pueden recolectar información de carácter personal –en general, aquella que de modo directo o indirecto puede servir para identificar a un usuario específico-. Esto tiene incidencia indirecta en posibles riesgos de seguridad o privacidad.
- **¿Quién es considerado el responsable del tratamiento, en contraposición a ser un mero encargado?** Dado que existen obligaciones tanto de confidencialidad como de protección de datos personales (en contraposición a datos no personales) a considerar, un marco regulatorio inteligente debe ser claro en los principios de atribución de responsabilidades aplicables a los distintos actores del ecosistema y la cadena de valor de datos de M2M/IoT.

- **¿Cómo y cuándo pueden los usuarios expresar su consentimiento y control sobre sus datos personales?** Una regulación de privacidad basada en principios deberá considerar de modo flexible cómo se notifica y obtiene el con-

“Una regulación de privacidad inteligente, que permita desarrollar los nuevos modelos de negocios, tecnologías y capacidades de 5G a través de la innovación basada en datos, es aquella que empodera a los individuos y les otorga la confianza suficiente de que sus datos personales son utilizados de modo justo y seguro”

sentimiento de usuarios en el uso de M2M/IoT cuando hay una recolección pasiva de datos, cuando no hay una pantalla o aplicación por medio de la cual el usuario otorgue su consentimiento y el proveedor notifique al usuario, y/o cuando no hay una relación en primera persona, sino indirecta, con el usuario. Es por eso que los marcos regulatorios deben proveer una variedad de bases legales para el procesamiento de datos personales, incluido el "interés legítimo".

Contenido Mediapartner

BN AMERICAS

Confianza. En el mundo de los servicios financieros, es un commodity valioso

Colaboración de **Allan Browne, BN AMERICAS**

Esto es particularmente cierto en el segmento de los consumidores, en que los bancos generalmente son vistos como depósitos seguros de datos de los consumidores en un mundo donde la información personal se disemina por el ciberespacio a raudales.

La banca puede atraer con esta fortaleza. Y los bancos de Chile, así como las aseguradoras locales, no son la excepción. De hecho, en términos de protección de datos, los chilenos confían más en su banco y proveedor de seguros que en las empresas de pagos en línea, compañías tecnológicas, minoristas o redes sociales, según la empresa de servicios profesionales Accenture. Y eso a pesar de varios ciberdelitos que han acaparado los titulares. Este nivel de confianza también sustenta un apetito saludable entre los chilenos por servicios bancarios y de seguros personalizados que se brindan a través de canales digitales.

Los bancos también pueden usar su sólida reputación en la protección de datos en la competencia contra quienes recién ingresan a la esfera de los servicios financieros

Según el estudio 2019 sobre consumidores de servicios financieros de Accenture, los chilenos se sienten más atraídos por los servicios personalizados que el promedio mundial. También están más abiertos a compartir datos personales adicionales con su banco o aseguradora a cambio de beneficios como asesoramiento personalizado o servicios premium, más rápidos y de menor costo. El 64% de los 2.000 encuestados en Chile dijeron que compartirían datos adicionales frente al promedio global de 55%.

La directora de servicios financieros de Accenture Chile Rosario Castro dijo que el desafío que enfrentan los bancos es aprovechar al máximo los datos. "El desafío no es pedir más datos, sino usar la información que hoy tiene la banca y las compañías de seguros", dijo Castro durante una presentación de las conclusiones en Santiago. "Finalmente, son industrias que tienen muchísima información de nosotros, pero no están aprovechando esa información", indicó, y agregó que, por ejemplo, podrían aprovechar los datos para conectarse con el ecosistema y ofrecer

productos y servicios empaquetados a medida a los clientes.

Los bancos también pueden usar su sólida reputación en la protección de datos en la competencia contra quienes recién ingresan a la esfera de los servicios financieros, como las fintechs, dijo el mes pasado Julio José Prado, presidente ejecutivo de la asociación ecuatoriana Aso-banca, durante una conferencia por internet que organizó la federación latinoamericana Felaban. "La privacidad es un área en la que los bancos —que son en sí mismos los representantes de la confianza de las personas al depositar su dinero o sacar un crédito— tienen que capitalizar este tema de mucho mejor forma", dijo Prado en ese momento. De hecho, Castro destacó las nuevas oportunidades comerciales que presenta la era digital actual.

En Chile y otros países, el flujo e intercambio de datos dentro del segmento de los servicios financieros se acelerará a medida que los bancos expandan sus ecosistemas; en otras palabras, se vinculen con terceros para proporcionar servicios personalizados y de valor agregado y reducir la fricción. Esto, a su vez, es parte de los esfuerzos para atraer y retener clientes en un mercado que algún día podría verse afectado por la llegada de un gigante tecnológico internacional como Amazon o Google.

Entre los líderes regionales está Colombia, ya que la aplicación de reparto a pedido Rappi y el banco local Davivienda se asociaron, lo que permitió que este último incorporara su solución de billetera móvil DaviPlata a la billetera móvil de la unicornio RappiPay. Otro pionero es Argentina, cuyo Banco Patagonia formó una alianza en tarjetas con el gigante regional de comercio electrónico MercadoLibre. También en Argentina, el banco Masventas se asoció con la firma local de tecnología blockchain Bitex para ofrecer un servicio de transferencia de dinero basado en bitcoin, el primero de su tipo en el país.

El sector bancario de Chile avanza por esta senda también. En junio, el grupo matriz de Banco Consorcio acordó inyectar US\$500.000 en la fintech local Pago Fácil, la primera maniobra corporativa de este tipo en el país. El grupo también lanzó un fondo de capital de riesgo corporativo por US\$20mn con la firma chileno-estadounidense HCS Capital Partners para buscar startups de servicios financieros en Chile, Colombia, Perú y México.

Voces

El papel de los *medios alternativos* de conectividad para cerrar la brecha de género

Por **Karla Prudencio Ruiz**, Miembro de **Conectadas.mx** y estudiante de la maestría en Derecho, Ciencia y Tecnología de la Universidad de Stanford.

Los datos que evidencian la brecha de género son contundentes. En este interesante artículo, María Elena Estavillo hace un recuento de algunas de las principales estadísticas en la materia y, citando al Foro Económico Mundial, concluye que “la velocidad del avance para Latinoamérica significa que tendrían que pasar 74 años al ritmo actual, para que se cierre la brecha de género”.

Para acelerar la reducción de esta brecha, es necesario impulsar la generación de datos más confiables, no sólo del sector público, sino también del sector privado y social. Esto significa básicamente que se tomen en cuenta a las mujeres cuando se analicen y diseñen las estructuras que soportan nuestra sociedad.

Transversalizar la perspectiva de género resulta más fácil o evidente en algunos sectores que en otros. Específicamente en el sector tecnológico, la aparente e “inherente” neutralidad de las tecnologías hace que el análisis de género no se considere o se relegue siempre a un segundo plano. No obstante, a medida que las tecnologías avanzan, esta presunta neutralidad de la tecnología es cada vez menos evidente. Ahora muchas de las tecnologías con las que nos relacionamos son capaces de “pensar” y de tomar ciertas decisiones por sí mismas, replicando el comportamiento humano y con ello sus estereotipos y patrones discriminatorios.

Lo anterior sólo es reflejo de que todavía no resolvemos lo más básico en esta materia. Por ejemplo, a la fecha, no hemos logrado que el acceso a internet no sea un problema que replique las desigualdades de género. Las soluciones tradicionales han servido de poco, sabemos que la brecha entre mujeres y hombres conectados sigue siendo significativa [1]. Si vemos estos datos con mayor capilaridad observamos que la brecha se acrecienta cuando analizamos el tipo de tecnologías a las que tienen acceso, el uso de las mismas y la producción de contenidos.

Si queremos alcanzar el cierre de la brecha de género tenemos que pensar en soluciones alternativas. Es necesario repensar estas tecnologías y su regulación desde una perspectiva que nos permita medir el impacto que tienen en la vida de todas las personas. Las redes comunitarias son una excelente alternativa a la idea tradicional de conectividad. Su cercanía con lo local permite el análisis de necesidades reales,



pero también del territorio en el que se desarrollan y de las dinámicas que promueven o inhiben. Aunque este tipo de redes pueden replicar patrones de desigualdad, como detalla Karla Velasco en esta presentación, también muestran esfuerzos locales por descentralizar el poder y el uso de las tecnologías.

Un ejemplo de cómo la construcción local de iniciativas puede comenzar a abonar a la inclusión es la Intranet colocada por Xamoneta, un colectivo conformado por mujeres pertenecientes a la comunidad purépecha Cherán K’eri. En sus palabras, el proyecto les permitió pensar no sólo en el resultado, sino en “cómo lo queremos organizar y sobre todo para qué”. Ellas no son sólo toman decisión sobre el acceso y los contenidos, sino también sobre el lugar de la instalación, las posibles personas usuarias y el fin que le darán. El acceso a esta toma de decisiones (que se llevó a cabo también dentro de lo comunitario) es una manera de apropiarse no sólo de la herramienta, sino del territorio, del aire y del suelo, de lo que es de todas y todos.

[1] Según datos de la UIT, la brecha de género aumentó de 2013 a 2016. En la actualidad, existen más de 250 millones menos de mujeres que hombres en línea en todo el mundo. Información disponible este enlace.

ENTREVISTA

“Sin un acceso a internet asequible y fácil de usar, las personas no pueden disfrutar de sus derechos y participar en las decisiones que les afectan ”

Valeria Betancourt, dirige el Programa de Política de Información y Comunicaciones de APC

Cuéntenos acerca de la Asociación para el Progreso de las Comunicaciones, su función y proyectos en marcha, además de sobre su responsabilidad dentro de la Asociación.

La Asociación para el Progreso de las Comunicaciones (APC) es una red y organización internacional que trabaja para apoyar a organizaciones, movimientos sociales e individuos en el uso de las tecnologías de información y comunicación para crear comunidades e iniciativas que contribuyan al desarrollo, la justicia social, la participación política y la sostenibilidad ambiental. Trabajamos por un futuro en el que todas las personas tengan un acceso fácil y de bajo costo a una internet libre y abierta. Nuestros

miembros son grupos que trabajan en sus países para promover la misión que comparten con APC.

La red global de miembros y el equipo de la organización está altamente calificado en el ámbito de las políticas y prácticas de Internet a nivel nacional, regional y global. Esta identidad coloca a APC en una posición para efectuar cambios de políticas de alto nivel mientras tiene una comprensión bien arraigada de lo que está sucediendo en el terreno. La experiencia de APC en la implementación de iniciativas nacionales, regionales y globales nos permite desarrollar soluciones innovadoras y de acceso comunitario y de conectividad, abogar por un enfoque basado en los derechos para el acceso y la gobernanza de internet, desarrollar capacidades en el movimiento de mujeres y otros movimientos sociales y trabajar en asociación con una amplia gama de personas e instituciones. APC fue establecida como red internacional en 1990 y tiene estatus consultivo ante Naciones Unidas.

Entre los proyectos más paradigmáticos que al momento implementa APC, se cuentan, entre otros:

- **El Monitor mundial sobre la sociedad de la información (GISWatch).** Se trata de un informe anual producido por la red de APC y sus aliados, que explora el progreso alcanzado en la creación de una sociedad de la información exclusiva en todo el mundo (en especial en la implementación de los objetivos de la CMSI), promueve el debate crítico y fortalece el trabajo en red y la incidencia por una sociedad de la información justa e inclusiva.

- **Conectar a los no conectados:** apoyo a las redes comunitarias y otras iniciativas de conectividad con base en la comunidad. El proyecto contribuye a la formación de un ecosistema propicio para el surgimiento y el crecimiento



VALERIA BETANCOURT

de redes comunitarias y otras iniciativas de conectividad con base en la comunidad en países en desarrollo.

- **Escuela Africana de Gobernanza de Internet**, es un curso residencial anual de cinco días orientado a dotar a actores africanos de diversos sectores de habilidades para participar en estructuras de gobernanza de internet locales e internacionales y dar forma al futuro del panorama de internet para el desarrollo de África.

- **Desafiar las narrativas de odio y las violaciones de la libertad religiosa y de expresión en línea en Asia**, un proyecto que se construye sobre análisis previo y busca proteger y promover el respeto por la libertad religiosa y la libertad de expresión en internet, en particular oponiéndose al discurso en línea que incita al odio sobre bases religiosas y generando narrativas que defiendan las opiniones seculares y diversas referidas a la religión. Este proyecto se concentra en cinco países del Sur y Sudeste de Asia: Bangladesh, India, Indonesia, Myanmar y Pakistán, que se caracterizan por la presencia de comunidades religiosas mayoritarias y plantean desafíos para secularistas y minorías.

- **Red de investigación por una internet feminista**, que se enfoca en crear una internet feminista lo suficientemente crítica como para producir cambios en las estructuras de poder ya imbuidas de cuestiones de género que existen en línea y fuera de línea. Los miembros de la red realizarán investigaciones basadas en datos que brinden pruebas suficientes como para provocar un cambio político y legal, así como cambios en el discurso en torno a los derechos en internet. El objetivo más amplio es asegurar que se tengan en cuenta las necesidades de las mujeres, las personas de género diverso y las personas queer a la hora de los debates sobre políticas de internet y la toma de decisiones.

- **¡Dominemos la tecnología!**, es un llamado a todas las personas, sobre todo mujeres y niñas, a tomar el control de la tecnología para terminar con la violencia contra las mujeres. Se trata de un proyecto de campaña global y colaborativo que pone en relieve el problema de la violencia contra las mujeres relacionada con la tecnología, junto con la presentación de resultados de investigación y soluciones en el mundo entero.

- **GenderIT.org** es un proyecto y espacio bilingüe de promoción feminista que explora cuestiones relacionadas con el género y las tecnologías de información y comunicación.

- **Garantizar los derechos humanos en línea en África** mediante una red fuerte y activa en torno a la ‘Declaración africana sobre derechos y libertades en internet’, apunta a abordar más efectivamente las amenazas y promover los derechos humanos en la región mediante el fortalecimiento de capacidades del Secretariado, de la

Coalición de la declaración africana y de organizaciones de la sociedad civil para el desarrollo de políticas y en respuesta a violaciones a los derechos humanos en internet.

Mi rol en APC está centrado en la dirección del Programa de Políticas de Información y Comunicación (CIPP), cuyo propósito es responder a problemas relacionados con el acceso, la gobernanza y los derechos en internet de un modo consistente, sistemático e integrado, teniendo en cuenta las particularidades en Asia, África y América Latina y buscando una dinámica multi-direccional entre lo nacional, lo global y lo regional. El programa genera ideas y análisis a través de investigaciones sobre temas clave; facilita interacciones entre movimientos; promueve la autonomía individual y colectiva de personas que defienden los derechos humanos en línea; propone puntos de vista alternativos sobre los efectos transformadores de la tecnología; desarrolla capacidades de la sociedad civil y otros actores para el involucramiento en aspectos y procesos de internet, incluidos los relacionados con políticas; y aboga por opciones políticas y soluciones favorables a los derechos humanos a nivel global, regional y nacional.

“Mi rol en APC está centrado en la dirección del Programa de Políticas de Información y Comunicación, cuyo propósito es responder a problemas relacionados con el acceso, la gobernanza y los derechos en internet de un modo consistente, sistemático e integrado”

Usted ha trabajado intensamente en el tema de la inclusión digital, una cuestión sobre la que ASIET también ha centrado buena parte de su trabajo, ¿considera que el acceso a internet es un derecho, o concretamente, un habilitador de derechos? ¿Cómo podemos avanzar en este sentido?

Desde nuestro punto de vista, el acceso a internet habilita el ejercicio de un amplio rango de derechos humanos en línea y fuera de línea. Sin un acceso a internet asequible y fácil de usar, las personas no pueden disfrutar de sus derechos y participar en las decisiones que les afectan y no pueden ejercer la posibilidad de hacer responsables a los gobiernos y las empresas por la promoción, protección y respeto a los derechos humanos. Sin acceso a internet y sin las habilidades necesarias para aprovechar sus beneficios, no es posible actualmente combatir la discriminación y la desigualdad ni reclamar derechos. En ese sentido, APC entiende el acceso como un tema multi-dimensional que demanda de abordajes y soluciones holísticas.

Para avanzar hacia la inclusión digital es necesario mirar y actuar más allá de la infraestructura de conectividad y centrarse en habilitar condiciones para incrementar la autonomía individual y colectiva y las opciones sobre las maneras en las que las personas pueden conectarse a las tecnologías y espacios digitales. Las personas deben poder determinar las maneras en las que usan, configuran, desarrollan, crean esas tecnologías y esos espacios una vez que están conectadas.

Pensamos que los actuales modelos económicos y regulatorios están exacerbando las desigualdades, la pobreza y la discriminación y es por ello que creemos que es sumamente importante adoptar enfoques y soluciones alternativas y complementarias para lograr cambios en la provisión de servicios de bajo costo. Se precisan de intervenciones integrales para mitigar las barreras políticas, económicas, sociales y culturales que limitan que las personas aprovechen plenamente de los beneficios de la sociedad y economía digital. Nos enfocamos en contribuir a crear un ecosistema habilitador para la emergencia y crecimiento de redes comunitarias y otras iniciativas locales y comunitarias de conectividad en países en desarrollo. Buscamos expandir el impacto, alcance y sostenibilidad del movimiento de redes comunitarias en el Sur global abordando cuestiones de capacidad humana y desafíos de sostenibilidad, así como los obstáculos regulatorios y de política pública que limitan el crecimiento de iniciativas comunitarias de conectividad. Esto incluye, además, promover el acceso a tecnologías digitales abiertas y a espacios libres de censura, vigilancia, acoso y cualquier otra forma de violación de los derechos humanos.

“Para avanzar hacia la inclusión digital es necesario mirar y actuar más allá de la infraestructura de conectividad y centrarse en habilitar condiciones para incrementar la autonomía individual y colectiva y las opciones sobre las maneras en las que las personas pueden conectarse a las tecnologías y espacios digitales”

En ocasiones pareciera que internet es una realidad paralela donde no se respetan los mismos derechos que en el mundo no virtual, ¿cómo ve esta situación? ¿Cómo valora el estado actual de la privacidad y la protección de los datos personales en la red? ¿Y acerca de la regulación sobre discurso de odio?

Las tecnologías digitales han impactado sustancialmente

la manera en la que experimentamos los derechos en línea y fuera de línea. Lo que sucede en la esfera en línea es reflejo y continuación de lo que sucede fuera de línea y viceversa. Es así que las tecnologías y espacios digitales han sido instrumentales para la incidencia orientada a asegurar el respeto a los derechos humanos pero es innegable que también han allanado el camino para nuevas formas de violaciones a los derechos humanos con consecuencias complejas. La digitalización de los distintos aspectos de la vida de las personas en conjunto con la explotación de los datos presentan un riesgo y un desafío inmenso para los derechos de las personas sobre todo debido a que no se ha comprendido que los derechos de las personas deben estar en el centro del desarrollo, despliegue, uso y regulación de internet y otras tecnologías digitales.

En general, no corren vientos propicios para el disfrute de los derechos humanos tanto en línea como fuera de línea. En múltiples ocasiones, los gobiernos están a la vanguardia del control, de la vigilancia, de la censura, de las interrupciones o cortes parciales o totales de internet con los consecuentes efectos en la habilidad de las personas para ejercer sus derechos. A su vez, es innegable que la influencia corporativa, sobre todo la del Norte global, en la configuración de los tecnologías y espacios digitales ha erosionado el carácter público de internet y los derechos humanos. El control y explotación de los datos y de los contenidos en las plataformas exacerbada, sin duda alguna, la desigualdad, la discriminación, los ataques, la criminalización y deslegitimización de expresiones y acciones. Tampoco se puede dejar de notar que los espacios digitales están cada vez más permeados por el odio y la discriminación y que afecta de manera particular a personas que están en situación de vulnerabilidad o marginalidad. No dejo de insistir, cada vez que puedo, que los Estados en muchos casos, se han convertido en fuente de inseguridad a través del control y el monitoreo de las conductas, las actividades y los contenidos en línea y que esto se complejiza aún más cuando esos poderes son transferidos a las corporaciones privadas. Se hace caso omiso de las responsabilidades que tienen los Estados de garantizar que ellos, como actores públicos, se ajusten al derecho internacional y a los estándares internacionales de derechos humanos y la responsabilidad que tienen de asegurar que los actores privados actúen en concordancia con ellos.

Se torna necesario reconocer que el panorama de la protección y promoción de los derechos humanos se ha modificado y que los actores privados median y arbitran, en gran medida, los derechos de las personas. Las respuestas, por tanto, deben replantearse también y debe verse una mirada renovada sobre los mecanismos que se precisan para asegurar y reforzar el ejercicio de derechos en el entorno digital.

“La digitalización de los distintos aspectos de la vida de las personas en conjunto con la explotación de los datos presentan un desafío inmenso para los derechos de las personas”

¿Cómo puede ayudar Internet y las TIC al desarrollo humano y la lucha contra la desigualdad? ¿Cómo observa el papel de la red hoy respecto a la participación del debate público? ¿Y respecto al empoderamiento femenino y el cierre de las brechas de género?

La exclusión, la desigualdad, los desbalances de poder, la discriminación y, en general, todas las formas de opresión, se expresan en la esfera digital no solo como extensión de la dimensión fuera de línea si no que adquieren, además, nuevos matices. Sin embargo, el espacio y las tecnologías digitales ofrecen también la oportunidad de amplificar las voces de los menos aventajados en términos sociales y económicos, de reforzar el sistema democrático, de habilitar la participación ciudadana y de fortalecer la esfera pública. Ya los documentos de la Cumbre Mundial sobre la sociedad de la información lo señalaban: la clave está en colocar a las personas y sus derechos en el centro y orientar el acceso y uso de internet en particular hacia la realización de esos derechos y hacia la construcción de ciudadanía crítica.

Es esencial reconocer que el impacto de la tecnología en las sociedades se enmarca en estructuras de poder existentes y cambiantes y en las inequidades que configuran las realidades sociales, culturales, económicas y políticas. Múltiples factores y fuerzas interactúan en conjunto para reforzar condiciones de inequidad, opresión, exclusión y violencia. La brecha de género y la violencia en línea contra la mujer, por ejemplo, son solo unas de las expresiones de ello. El acceso a los recursos y a las condiciones para ejercer derechos dentro y fuera de línea está determinado por las intersecciones de los distintos factores que constituyen las estructuras de poder, las matrices patriarcales y de injusticia, las normas y estereotipos que perpetúan y exacerban la inequidad. En APC pensamos que es esencial adoptar un enfoque feminista de internet que apunte a examinar las diferentes facetas de la intersección entre las tecnologías digitales en red y el feminismo en las áreas de la economía, el acceso, la expresión, la autonomía, la construcción de movimientos, entre otras.

El **enfoque feminista para el internet** es un llamado para la participación de diversos actores, particularmente del movimiento feminista y de las mujeres, en todos los aspectos relativos al diseño, acceso, uso y desarrollo de la tecnología, particularmente de internet. Para el efecto, a través de encuentros globales con feministas alrededor

del mundo, se formularon los principios feministas para internet. No se trata de un conjunto de reglas o recomendaciones si no de un ejercicio de interrogación basado en la articulación de temas desde una postura feminista. Los principios feministas para internet nombran el tipo de internet que nos gustaría tener y al que estamos contribuyendo a configurar. Una internet feminista trabaja hacia y por el empoderamiento de más mujeres y personas queer en sus diversidades para disfrutar a plenitud de los derechos.

Se trata, en definitiva, de un cuestionamiento a las estructuras de poder. En esa medida, ofrecen un punto de entrada para que los movimientos de mujeres, los movimientos feministas articulen y exploren temas relacionados con la tecnología y aborden los derechos humanos en internet a través de una mirada interseccional de género, que de cabida y que responda a las necesidades de las mujeres, los diversidades de género, las personas queer. Se trata de una herramienta para la reflexión teórica y la acción práctica orientada a transformar el internet generando los cambios necesarios a través del cruce entre derechos, feminismo e internet.

¿Cree necesarios avances regulatorios en el sentido de que existan marcos de actuación a nivel global o regional sobre derechos digitales? ¿Cómo valora el estado actual de los mecanismos de gobernanza, están teniendo un impacto efectivo en las políticas públicas -con especial relevancia a protección de los DDHH). ¿cómo podemos mejorar este impacto?

Respecto del tema regulatorio, conviene notar que no siempre las soluciones propuestas para responder a problemas generados por el uso de la tecnología son adecuadas y que más bien conducen a nuevos problemas. Es necesario distinguir que algunos problemas demandan soluciones de tipo estructural mientras que otros precisan respuestas de tipo operacional. En todo caso, es imperativo asegurar que independientemente del tipo de respuesta regulatoria, normativa o de política pública que se ofrezca, se conciba y se aplique en alineación con los estándares establecidos de derechos humanos.

No se puede disociar el ejercicio de derechos humanos de la gobernanza de internet. Si los arreglos sobre la gobernanza de internet no se hacen a partir del reconocimiento de que el internet es un bien público global y que debe ser manejado de manera inclusiva, transparente y democrática, será muy difícil que el resultado sea el reforzamiento del ejercicio de derechos humanos. Es necesario, por tanto, reforzar el carácter público de internet y demandar el establecimiento y fortalecimiento de mecanismos participativos, inclusivos, pluralistas, con rendición de cuentas, transparentes de decisiones políticas sobre internet. En general, las estructuras democráticas deben ser reforzadas y para ello es preciso que se fortalezca el Estado de Derecho.

Contenido Mediapartner

TELESEMANA

¿Y si eligiéramos las empresas por sus **políticas de privacidad y uso de datos personales?**Por **Leticia Pautasio**, Editora en Jefe de **Telesemana.com**

5.000 millones de dólares es lo que deberá pagar Facebook tras el escándalo de Cambridge Analytica que destapó más que una preocupación por el uso que hacen las grandes compañías de los datos de sus usuarios. La multa es el resultado de un acuerdo entre la red social y la Comisión Federal de Comercio (FTC) de los Estados Unidos en el marco de una investigación sobre si la compañía compartió indebidamente los datos de usuarios. La noticia, que se conoció en junio, se suma a otras multas que la red social había tenido que afrontar en el pasado por el mismo caso.

A esta noticia se suma que en junio se conoció que empleados de Google escuchan un pequeño porcentaje — algo así del 0,2 por ciento— de las conversaciones que los usuarios tienen con los dispositivos de la marca. Si bien se trata de un porcentaje menor en comparación con la cantidad de datos que tiene la compañía procesa de sus usuarios, no sorprende que la publicación de esta práctica por parte de Google despertara nuevas preocupaciones sobre el uso que hacen las empresas de toda la información que se comparte por Internet.

Es difícil saber hoy a ciencia cierta si las noticias de uso indebido de información de los usuarios o, incluso, las noticias falsas que circulan sobre las plataformas de compañías digitales, logran cambiar el hábito de consumo.

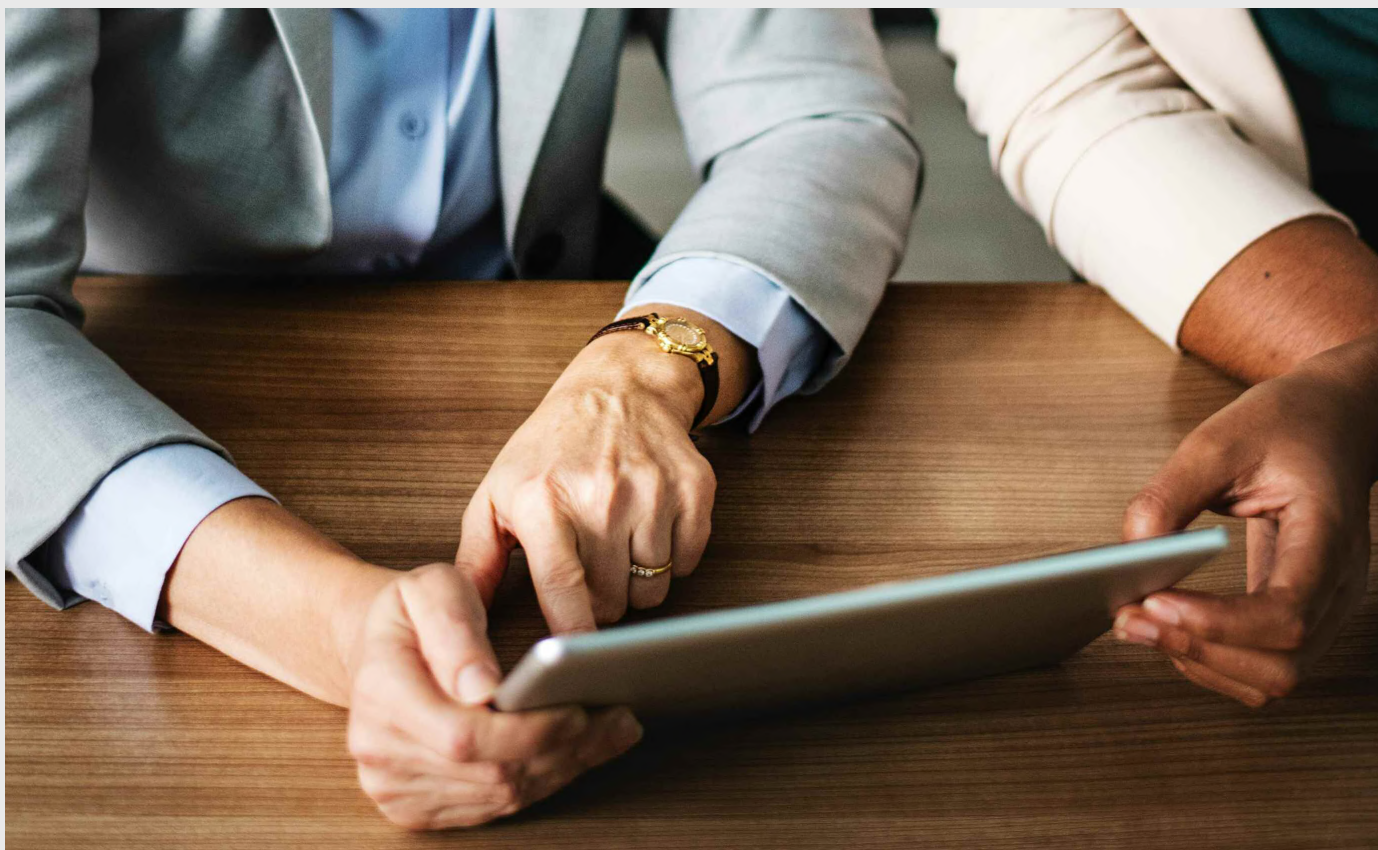
Como si esto fuera poco, la aplicación que permite incorporar filtros de envejecimiento en retratos también está siendo puesta en la mira por no tener suficientes garantías de la privacidad de las fotos que se suben a su plataforma. En un mundo donde el desbloqueo facial empieza a ser relevante, la llamada de atención aparece en cada artículo periodístico dónde se comenta sobre este nuevo fenómeno viral.

El foco en la privacidad y los datos personales ha puesto en el pasado a los operadores en alerta. En un intento de diferenciarse, generar confianza y captar a los usuarios, los operadores intentaron posicionarse o bien como garantes de la seguridad o bien como empresas transparentes, generando herramientas que permiten a los usuarios controlar el uso que hacen de sus datos. En la percepción general, las compañías digitales están en la mira mientras que los operadores (todavía) pueden acomodarse en ese espacio de confianza que supieron construir.

No obstante, un ranking que se realiza todos los años y que intenta medir los términos de condiciones de servicio, estándares y políticas en relación a la libertad de expresión y privacidad demuestra que la industria todavía tiene trabajo por realizar. En un ranking en el cual el puntaje máximo es 100 puntos, la compañía mejor posicionada detenta 62. Y, curiosamente, no es un operador de telecomunicaciones sino una empresa “digital”: Microsoft. Por detrás se ubica Google y Verizon Media (ex Yahoo) cada una con 61 puntos. A este trinomio le sigue Facebook con 57 puntos. El ranking de operadores de telecomunicaciones es liderado por Telefónica con 57 puntos —el mismo puntaje que Facebook—, seguido de Vodafone (52) y AT&T (48). La lista de operadores la completan, entre otros, Telcel, Deutsche Telekom, Orange y América Móvil, en ese orden.

De las doce compañías de telecomunicaciones analizadas, solo dos superan los 50 puntos. En tanto, en la lista de compañías digitales son la mitad las que se ubican por sobre esa media. Curiosamente, por debajo se ubican compañías como Apple (46), una de las empresas que más se jactan de resguardar la privacidad —y justamente en ese ítem pelea el segundo puesto junto con Google pero falla en otros ítems del ranking, lo que degrada el puntaje general—.

El ranking de Derechos Digitales de 2018 —que cuenta con el apoyo de Ford Foundation, Open Society Foundations, el Departamento de Democracia, Derechos Humanos y Trabajo de los Estados Unidos y la Fundación Mozilla, entre otros— no debería considerarse como definitivo



Es posible que en el futuro seamos más conscientes y que los temas de privacidad y derechos humanos sean la vara con las que medirán a las compañías a la hora de elegir un servicio o producto. Para ese mundo es el que las empresas deberían estar preparadas.

sobre cómo están los operadores y las compañías digitales en términos de gobernanza, uso de información de usuarios, derechos humanos y privacidad, pero sí como un acercamiento a cómo medir los esfuerzos realizados por las empresas.

En la percepción general, las compañías digitales están en la mira mientras que los operadores pueden acomodarse en ese espacio de confianza que supieron construir

Es difícil saber hoy a ciencia cierta si las noticias de uso indebido de información de los usuarios o, incluso, las noticias falsas que circulan sobre las plataformas de compañías digitales, logran cambiar el hábito de consumo.

Por ahora, todo parecería indicar que ninguna de estas empresas han perdido terreno luego de haberse conocido los peligros de compartir información con ellas. Tampoco se puede constatar que Telefónica haya ganado clientes por haberse mostrado más transparentes en el uso de los datos y hasta haber publicado un Manifiesto para el Mundo Digital —y otro para el uso de la inteligencia artificial—.

Por ahora, rankings como el mencionado no aparecen en los grandes titulares de los periódicos. De hecho, el que se menciona en esta nota había pasado desapercibido para este medio cuando se publicó en mayo de este año. Lo que sí aparecen en los titulares son los escándalos como el de Cambridge Analytica o Google. Es posible que en el futuro los seres humanos sean más conscientes y que los temas de privacidad y derechos humanos sean la vara con las que medirán a las compañías a la hora de elegir un servicio o producto. Para ese mundo es el que las empresas deberían estar preparadas. Los operadores que quieran aprovechar el Big Data y jugar en la economía digital deberían estar sintiendo la respiración en la nuca de las multas que Facebook tiene que pagar.

LA CASA DE INTERNET



**DIEGO R.
CANABARRO**

Gerente de Políticas
Públicas, América Latina y
Caribe Internet Society



IoT: un proceso multisectorial para garantizar la protección de los consumidores y la resiliencia de la red en Uruguay

Internet es una red abierta, globalmente conectada, confiable y segura para todas las personas. Y debe seguir siéndolo. El avance de tecnologías emergentes, sus impactos en el funcionamiento técnico, en la operación y en el uso de la red, así como las respuestas en el campo de las políticas públicas pueden impactar positiva o negativamente el futuro de Internet y afectar de manera directa a sus usuarios. En ese sentido, Internet Society trabaja para proteger las cualidades fundamentales que han impulsado el desarrollo de Internet y para garantizar que su evolución esté alineada con las contribuciones generadas por la red para la innovación, la economía, la cultura y para la vida de las personas en general.

La llamada Internet de las cosas (IoT) presenta una enorme cantidad de beneficios a los consumidores, al sector privado y a los gobiernos. Para 2020, se proyecta que IoT admitirá decenas de miles de millones de dispositivos interconectados. En un futuro lejano, hogares enteros, los sistemas públicos de transporte y otros servicios en verdaderas "ciudades inteligentes", e incluso los cuerpos de los seres humanos, serán parte del mismo espacio común integrado que convergerá en Internet.

Más allá de las promesas y de la realidad de una vida interconectada, IoT representa un campo en el cual las distintas dimensiones técnicas, económicas y sociopolíticas del desarrollo tecnológico, así como sus desafíos, se presentan y se cruzan. El tema tiene que ver con los incentivos a la inversión y e innovación, con la protección de los derechos de los consumidores, y con la seguridad y resiliencia de Internet cuando es utilizada cuando se la utiliza como interfaz para los distintos sistemas de IoT. Por eso, Internet Society (que ya había creado una "Alianza de confianza en línea" para identificar y promover las mejores prácticas de seguridad y privacidad que fomentan la confianza del consumidor en Internet) ha impulsado un

proceso de diálogo de múltiples partes interesadas en países como Francia, Senegal, Filipinas y Canadá) para que se produzca un conjunto de recomendaciones sobre el tema de seguridad de IoT. Eventualmente, tales recomendaciones podrán guiar la elaboración de políticas públicas y regulatorias cuando sea necesario. En la región de América Latina y el Caribe, un proceso similar se desarrolla desde Julio de 2019 en Uruguay bajo la coordinación de la Agencia de Gobierno Electrónico y la Sociedad de la Información y el Conocimiento de Uruguay (AGESIC).

Con el apoyo de la Oficina Regional para América Latina y el Caribe de Internet Society, AGESIC creó dos grupos de trabajo integrados por más de 60 personas de instituciones públicas y privadas, de la comunidad técnica y de organizaciones de la sociedad civil del país. Un grupo fue encargado de los aspectos de IoT capaces de afectar la seguridad de los consumidores, su privacidad y la protección de datos personales. El otro se enfocó en el tema de la seguridad de la red (que suele ser atacada por dispositivos IoT comprometidos). El trabajo de ambos grupos tuvo como punto de partida las siguientes consideraciones:

- El ahorro de recursos y las presiones por economizar en el desarrollo de productos y servicios de IoT (principalmente por actores sin ninguna experiencia en el campo de seguridad de redes) no siempre toman en cuenta buenas prácticas, como pueden ser aquellas relacionadas con la protección de la privacidad y de los datos personales, la autenticación de las relaciones cliente-servidor o el enrutamiento seguro, entre otras.
- No existen estándares internacionales sobre seguridad en IoT, lo que causa dificultad al momento de identificar y comparar los diferentes niveles de seguridad de dispositivos, productos y servicios de IoT. Además, la mayor parte de los productos y servicios de IoT están dirigidos a



consumidores que suelen no conocer los riesgos y amenazas existentes, ni tomar en cuenta las cuestiones de seguridad como un requisito de compra.

- Al mismo tiempo, no existen acuerdos sobre el papel de los distintos actores en la cadena productiva de IoT y no hay un conjunto de principios comunes sobre el nivel de soporte que los fabricantes y vendedores deben dar a los usuarios. Entre estos aspectos se incluye la duración de la garantía, la frecuencia de las actualizaciones de seguridad y la puesta a disposición de parches de seguridad.

- La complejidad de los sistemas de IoT hace con que se pueda distribuir el control y la operación de los componentes estructurales a varios actores, en varias jurisdicciones distintas. Esto provoca que no exista claridad respecto a los regímenes de responsabilidad legal que se deben aplicar al tema.

Es necesario involucrar a todos los países para alcanzar soluciones coordinadas y convergentes a nivel mundial para proteger a la red y a sus usuarios para que Internet siga siendo el motor que hoy conocemos para el desarrollo económico y sociocultural de todas las personas.

Los grupos han trabajado presencial y remotamente en la producción colaborativa de un borrador que sigue en discusión hasta el 25 de septiembre. A pesar de que el proceso uruguayo no haya llegado a su fin, es posible adelantar las líneas generales de lo que ha sido producido hasta hoy. En el caso de la protección del consumidor, el grupo de trabajo plantea un conjunto de recomendaciones para que los usuarios: (a) sepan cómo adquirir de manera informada productos y servicios de IoT y tengan detalle sobre su funcionamiento, sus características y las políticas de seguridad empleadas en su desarrollo, pro-

ducción y operación; (b) puedan constatar fácilmente el nivel de seguridad asociado a un dispositivo o servicio de IoT y elijan qué comprar con base en estándares conocidos; (c) sepan cómo proteger su privacidad y proteger los flujos de datos y de información que generan, y mantengan la costumbre de actualizar sus dispositivos; y (d) adopten buenas prácticas de seguridad para minimizar los riesgos. En el caso de la resiliencia de la red, el grupo de trabajo produjo un conjunto complejo de recomendaciones que tocan no sólo a los dispositivos y a la conducta de los usuarios, sino también a toda la cadena de soporte a los productos y servicios de IoT, que incluye el transporte de la información de extremo a extremo, el tratamiento y las modalidades de acceso a la misma, así como los mecanismos de recuperación de datos e información almacenada.

Los dos grupos de trabajo consideraron todas las capas y etapas de la cadena productiva en el campo de IoT: desde los fabricantes de dispositivos a los proveedores de servicios de IoT, pasando por los desarrolladores de aplicativos, y llegando hasta los comerciantes y los canales de distribución. El conjunto final de recomendaciones, previsto para ser publicado a fines de Octubre, trata también de lo que se espera de usuarios individuales y corporativos en sus prácticas diarias; de la comunidad técnica e instituciones académicas en el desarrollo de la tecnología; y de la sociedad civil en sus actividades de concientización y de fiscalización de las actividades de instituciones públicas y privadas.

Más allá de las recomendaciones producidas en Uruguay y en los otros países mencionados anteriormente, el desafío sigue. No sólo para Internet Society, sino para los diversos actores directa o indirectamente involucrados con el tema de la cooperación digital. Es necesario involucrar a todos los países para alcanzar soluciones coordinadas y convergentes a nivel mundial para proteger a la red y a sus usuarios para que Internet siga siendo el motor que hoy conocemos para el desarrollo económico y sociocultural de todas las personas, en todos los lugares.

LA CASA DE INTERNET



**LUIS ARANCIBIA
MEDINA**

Miembro del Consejo Directivo
de la Asociación de ccTLD de
América Latina y el Caribe



Nombres de dominio, Whois y datos personales. Novedades desde Chile.

El año 2018 ciertamente será recordado como un año decisivo en la protección de datos en todo el mundo. A partir de enero de 2018, más de 100 países promulgaron sus legislaciones de protección de datos, y alrededor de 40 países estaban tramitando proyectos de leyes en la materia. Chile no está ajeno a dicho proceso. El 15 de mayo de 2018 se aprobó una reforma a la Constitución Política por la cual se estableció explícitamente el derecho a la protección de datos personales como un derecho de rango constitucional. Al mismo tiempo, se encuentra en discusión actualmente el proyecto de ley para una nueva ley de datos personales, que sustituirá el régimen establecido por la ley 19.628 sobre Protección de Datos de Carácter Personal de agosto de 1999.

En este contexto se despliega — si es que acaso no es el gatillador de dicho proceso— el Reglamento de Protección de Datos de la Unión Europea, también conocido como GDPR, el cual se ha convertido claramente en un modelo

NIC Chile decidió voluntariamente efectuar adecuaciones a su política de acceso a los datos de registro, elevando el nivel de protección reconocido a todos sus usuarios

para el resto del mundo. El GDPR es, sin duda, el desarrollo regulatorio más importante en materia de protección de datos personales vigente hasta la fecha. Basado en un mecanismo detallado y protector, está influyendo en el uso de los datos personales y a muchas legislaciones en todo el mundo. Entendido correctamente, el GDPR alentará a las empresas a desarrollar marcos precisos y explícitos de gestión de la información, a utilizar los datos personales en base a una práctica que las obligará a man-

tener a los titulares de los datos informados sobre la toma de decisiones respecto de ellos. Para alcanzar estos objetivos, el GDPR utiliza criterios y herramientas jurídicas y procedimentales, que serán los factores estructurales que facilitarán la comprobación de violaciones y brechas, a la vez que pondrá en tela de juicio a algunos modelos de negocio concebidos en base al uso intensivo de información de personas. Si bien se trata de una norma europea, su alcance se ha extendido mucho más allá, porque se aplica en todos los casos en que se procesan los datos personales de personas naturales que permanezcan en la Unión Europea, independiente del lugar del mundo en el que se hace dicho procesamiento. Lo anterior ha obligado a muchos servicios de Internet a actualizar sus políticas de privacidad para adecuarse a dicha norma. En el ámbito de nombres de dominio, muchos Registros y empresas registradoras del mundo han tenido que cambiar sus políticas para los servicios de consulta -lo que se denomina WHOIS- que son los que proveen acceso a los datos de registro de los dominios, limitando la información que se publica.

En el caso de NIC Chile, solo una muy pequeña fracción de sus usuarios estarían cubiertos por las disposiciones de GDPR. No obstante lo anterior, dado que el GDPR se ha transformado en un importante referente mundial en el ámbito de protección de datos personales, NIC Chile decidió voluntariamente efectuar a contar del 25 de mayo de 2018 adecuaciones a su política de acceso a los datos de registro, elevando el nivel de protección reconocido a todos sus usuarios.

A través de establecer una Política sobre publicación de datos del Registro de Nombres de Dominio .CL, se fijó las condiciones bajo las cuales la información de los nombres de dominio están disponibles para su consulta pública en la base de datos de nombres de dominio bajo .CL. La referida Política se ocupa de fijar limitaciones al uso de la

información que proporciona, por cuanto los datos asociados a un dominio .CL se proveen exclusivamente para fines relacionados con la gestión del servicio de nombres de dominio .CL, la operación del DNS y la resolución de controversias por nombres de dominio.

Junto a lo expresado, la Política se hace cargo de reducir los datos disponibles de los nombres de dominio, determinando que el conjunto que publicará estará acotado al nombre de dominio, el estado del registro, la fecha de creación y expiración de la inscripción, el agente registrador, nombre o razón social del titular y el nombre de los servidores DNS. Se eliminó información de contacto del titular, contacto administrativo y técnico, entre otros. Tomando como referencia recomendaciones de ICANN, se diseñó un formulario para que los interesados que se identifiquen debidamente puedan comunicarse con los contactos de un dominio. NIC Chile se hace cargo de enviar la comunicación a los contactos correspondientes y será decisión de ellos responder a dicha comunicación. Con la finalidad de evitar los abusos en la utilización del formulario, se obliga a todo interesado en utilizarlo a declarar que no hará uso del servicio para el envío de correos no solicitados (spam), ni cualquier otro uso contrario a las condiciones señaladas en la Política. Sin perjuicio de lo anterior, los datos de inscripción de un dominio podrán ser entregados a requerimiento formal de cualquier autoridad judicial o administrativa facultada legalmente para requerirla y de conformidad con las leyes de la República de Chile. Adicionalmente y para asegurar el uso adecuado y pertinente de la información del servicio de publicación de datos de nombres de dominio, NIC Chile podrá adoptar todas las medidas que estime necesarias para el resguardo y uso legítimo de la información de la que es depositario. Podrá decidir, entre otras, que los usuarios deban leer y aceptar los Términos de uso de la información; introducir el uso de captcha, poner límites a las consultas para evitar la extracción indebida de datos; fijar un plazo a partir de la cual la información podrá estar disponible, etcétera, así como proveer un mecanismo para que los destinatarios de estas comunicaciones puedan reportar eventuales abusos.

A más de un año de vigencia de los cambios en el servicio de información de los dominios, se ha podido constatar una reducción sustancial de los reclamos de los clientes de NIC Chile por abuso de la información que se hacía por spam u otros usos no consentidos por ellos. Asimismo, los cambios están sintonizados con los resultados del estado del proceso de discusión sobre el servicio de Whois que estaba teniendo lugar en la industria de los nombres de dominio con ocasión del GDPR, y seguimos atentos a la evolución de ese proceso, que aún continúa. En paralelo, se ha puesto la protección de los datos personales de los usuarios de NIC Chile como centro de las preocupaciones del Registro, a la espera de las futuras adecuaciones que podrían tener lugar con la nueva legislación en la materia.

ICANN

La ICANN publica su auditoría de operadores de registro para abordar las amenazas de seguridad en el DNS



El 17 de septiembre de 2019, el Departamento de Cumplimiento Contractual de la ICANN publicó el [Informe de la Auditoría de Operadores de Registro \(RO\) para Abordar las Amenazas de Seguridad en el DNS](#). En el informe, se presenta un resumen de los resultados de una auditoría llevada a cabo entre noviembre de 2018 y junio de 2019.

Luego de haber concluido esta auditoría, la ICANN llevará a cabo una auditoría de registradores que también se centrará en las amenazas de seguridad en el DNS.

ACERCA DE LA ICANN

La misión de la ICANN es ayudar a garantizar una Internet global, unificada, estable y segura. Para contactar a otra persona en Internet, debemos ingresar una dirección —un nombre o un número— en nuestra computadora u otro dispositivo. Esa dirección debe ser única para que las computadoras puedan localizarse unas a otras. La ICANN ayuda a coordinar y brindar soporte a estos identificadores únicos en todo el mundo. La ICANN fue creada en 1998 como una corporación de bien público y sin fines de lucro con una comunidad integrada por participantes de todo el mundo.

Centro de estudios de Telecomunicaciones (cet.la)

El **programa de Becas Junior Fellowship** del cet.la, nació con el propósito claro de promover el debate y la generación de conocimientos que contribuyan al desarrollo de las Telecomunicaciones en América Latina. A grandes rasgos, se trata de una beca que financia llevar adelante una investigación alrededor de diversas temáticas relacionadas al sector y contando, a su vez, con el apoyo de los expertos del cet.la. Las investigaciones se presentaron en julio en Córdoba en el foro anual CPR LATAM. Los 5 candidatos electos, que provienen de **Brasil, Colombia, Ecuador, España y México**, junto con los expertos del cet.la, realizaron sus investigaciones, [ya disponibles en nuestro sitio](#). En este número conoceremos la investigación de **Amanda Espiñeira Lemos sobre protección de datos personales**.



ACCESO, USO Y PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA: DISEÑOS METODOLÓGICOS Y TEÓRICOS

Amanda Nunes Lopes Espiñeira Lemos se refiere al Working paper realizado en el marco del Programa de becas Junior Fellowships, llevado adelante por el Centro de Estudios de Telecomunicaciones de América Latina – cet.la. [Descárgalo aquí](#).

El uso de datos se torna cada vez más importante por el desarrollo de una economía global cada vez más digitalizada. La monetización de estos datos hace que su protección sea necesaria para los usuarios de la red. Ante las transacciones transfronterizas se piensa en modelos regulatorios para la resolución de conflictos. Internet ha servido para favorecer y perfeccionar los sistemas de interacción social, teniendo un gran impacto en la esfera económica, dada cuenta del vasto flujo de datos a escala global que ha transformado significativamente la velocidad de las transacciones financieras y, en consecuencia, la acumulación de capital. Además, ha posibilitado la creación de nuevos modelos de negocio basados precisamente en el uso de dichos datos.

El objetivo principal del artículo es señalar los asuntos derivados del tratamiento de datos personales en la economía digital, cuáles son los problemas que se han generado y proponer posibles soluciones, partiendo de los contornos institucionales de la gestión de datos en el ecosistema digital, con las leyes y autoridades de protección de datos

El objetivo principal del artículo es señalar los asuntos derivados del tratamiento de datos personales en la economía digital, cuáles son los problemas que se han generado y proponer posibles soluciones, partiendo de los contornos institucionales de la gestión de datos en el ecosistema digital, con las leyes y autoridades de protección de datos en A. Latina.

en América Latina. La investigación comprende la relación existente entre las culturas locales en lo que se refiere a la regulación de la protección de datos personales y de información.

Este objetivo deriva de una duda acerca de las diferencias sociales que pueden existir en los diversos países cuando tratamos conceptos tan generales como privacidad, datos personales y vida privada. La metodología del estudio busca abarcar una "red conceptual de atributos jurídicos, cuya realidad depende de indicadores de orden normativo (base legal), de orden concreto (implantación de la legislación), de orden institucional (papel de los actores involucrados) y de orden prospectivo (tendencia hacia el futuro)" (ARANHA, 2011, p. 17)

Los temas principales para tratar en modelos regulatorios de protección de datos en los países de América Latina parten del manejo de información personal, y flujo transfronterizo de datos. O sea, de la importancia que los datos tienen en la economía contemporánea, digital. Así tratarse de políticas de consentimiento y responsabilidad de intermediarios, en casos de discurso de odio y uso de datos para elecciones es demasiado importante cuando se piensa en la regulación del tema en Latinoamérica.

La cultura de protección de datos personales en América Latina está creciendo y cada vez más se debate sobre tema.

La transparencia y acceso a los algoritmos de procesamiento, la ruta que recorren los datos, información de quién controla, son algunos de los derechos que deben ser asegurados en una Carta de Derechos para uso de datos personales en América Latina

Así se apunta la necesidad de construir una Carta de Derechos para uso de datos personales en América Latina, teniendo en cuenta la salvaguarda de la seguridad de los usuarios, con la protección contra riesgos de divulgación sin consentimiento, en consecuencia, la limitación de uso con especificación de propósito de uso de los datos. La transparencia y acceso a los algoritmos de procesamiento, la ruta que recorren los datos, información de quién controla, son otros de los derechos que deben ser asegurados en esa carta.

BIBLIOTECA TIC
Nuevo Marco Regulatorio para la Convergencia

Este estudio describe el actual panorama del mercado de servicios de telecomunicaciones y audiovisual, y el estado de obsolescencia de la regulación sectorial, que en muchos casos no contempla la realidad actual a partir de la convergencia de estos servicios, y la irrupción de nuevos players que brindan servicios sobre internet. El informe expone la urgencia acometer transformaciones estructurales asociadas a la convergencia, para crear las condiciones adecuadas que permitan llevar a cabo las inversiones necesarias.



[Descárgalo aquí](#)

La TV por suscripción en un entorno convergente

Este informe hace un análisis comparativo del marco regulatorio y evolución de la televisión por suscripción, y los servicios de vídeo Over the Top (OTT Video) en 10 países representan el 85.6% de la población de América Latina.



[Descárgalo aquí](#)

RED ACADÉMICA

Responsabilidad moral corporativa en la defensa del *Ciberespacio*: Un caso ficticio para ayudar en la reflexión

Por Carlos Cares, Centro de Estudios de Ingeniería de Software, Universidad de La Frontera



Qué duda cabe que el acceso al Ciberespacio es un elemento relevante del estado de bienestar contemporáneo, sin embargo su manipulación dolosa puede causar daño psicológico y/o económico a las personas llegando incluso a impactos sociales, como por ejemplo el impacto en resultados electorales. Adicionalmente, el Ciberespacio es también infraestructura y, por todo lo anterior, ha llegado a ser un blanco estratégico en tiempos de guerra además de ser un blanco permanente de asociaciones criminales.

De hecho, el reciente ataque a las plantas petroleras Abqaiq y Khurais, fue realizado por lo que en otra época hubiésemos llamados periféricos, o de manera contemporánea, un agente ciber-físico, es decir, objetos físicos cuyo comportamiento es controlado, guiado o coordinado desde el o un, eventualmente privado, ciberespacio. Hasta el momento, para este ataque específico, existen diferentes posibles responsables, sin embargo, y al respecto, el gobierno de Arabia Saudita no ha culpado a nadie ya que no existiría evidencia concreta sobre quién es el atacante. Hasta aquí todo real.

En esta columna quiero referirme al tema moral involucrado, y, como es costumbre en todo debate moral, se revisa si los principios defendidos siguen siendo aplica-

bles en situaciones hipotéticas, lo que para todo efecto de discusión, se trata de situaciones ficticias, y es lo que haré en esta reflexión.

El caso ficticio a utilizar será entonces el mismo mencionado, supondremos que el ataque a la planta petrolera fue perpetrado por un grupo de ciberatacantes, con motivos hasta ahora desconocidos, pero con una estrategia de anonimato, ya sea por seguridad propia o de protec-

El Ciberespacio es también infraestructura y, ha llegado a ser un blanco estratégico en tiempos de guerra

ción ante sus eventuales mandantes. En un ciber-café de un pueblo cuyo nombre no revelaremos aquí, se activó un programa que prueba pares usuarios-claves comunes, por ejemplo (root,asd123). El grupo capturó en 3 horas de sesión 12 servidores. Se subió el mismo programa a estos servidores y al día siguiente tenían 134 servidores capturados de diversos proveedores de servidores a nivel mundial. Con esta fuerza computacional se preparó un ataque de fuerza bruta sobre la zona oscura localizada

en la zona geográfica donde el cliente de este grupo deseaba orientar un ciber-ataque. Cabe destacar que una "zona oscura" significa simplemente no visible, no significa no inaccesible. Para mejorar el anonimato se hizo pasar el flujo por un ISP que tenía un software de ruteo que permitía alterar las tablas de IP, elemento clave para perder la traza de una intromisión. Una vez en la zona oscura el hallazgo de la documentación y del propio control de los drones fue una sorpresa. La idea del ataque original cambió: el daño pretendido podría ser físico y político.

Hasta aquí el caso ficticio, pero con un paréntesis de realidad: lamentablemente la factibilidad tecnológica del caso anterior es muy real. Pregunte usted al administrador de sistemas de su compañía sobre la cantidad de intentos de intromisión en sus servidores. Estos intentos pueden ser fácilmente 15.000 en 24 horas. Si le pide que recorra el camino inverso a los ataques y ubique a su atacante, muy probablemente lo hará (es posible). Algunos de estos son prestigiosos proveedores de servicios cloud o prestigiosas empresas de desarrollo de software.

Pregunte usted al administrador de sistemas de su compañía sobre la cantidad de intentos de intromisión en sus servidores. Estos intentos pueden ser fácilmente 15.000 en 24 horas.

Por otra parte, la posibilidad de asignar responsabilidad moral a las organizaciones ha sido un debate contemporáneo en el campo de la ética, que, pese a los argumentos utilizados tanto a favor como en contra de esta posición, la pragmática de las sociedades liberales le ha asignado tareas a corporaciones que tienen relación con proveer a los ciudadanos de servicios considerados parte del estado de bienestar. Si pensamos en el campo de las telecomunicaciones este es un claro ejemplo, existe la misión de comunicar a las personas (y corporaciones), para lo cual normalmente el Estado concede una porción del espectro radio-eléctrico que hace posible la generación de los servicios de comunicación, pero en general no se excluye la provisión de los servicios de conexión de Internet por fibra.

El caso de responsabilidad que deseo exponer no es para el mandante ni para los hackers del caso ficticio, cuya responsabilidad legal es incuestionable, sino que quiero exponer sobre la responsabilidad moral de las empresas utilizadas en el ataque, desde el ciber café, junto a los proveedores de servidores y servicios de comunicación digital.

Quiero exponer sobre la responsabilidad moral de las empresas utilizadas en un ataque, desde el ciber café, junto a los proveedores de servidores y servicios de comunicación digital.

La condición de una responsabilidad moral tiene relación con la valoración social, con un acuerdo que debería estar socialmente legitimado, y por lo tanto dónde se expresa lo que constituye un acción correcta de lo que se deriva, tácita o explícitamente, lo que constituye una acción incorrecta.

La pregunta de la responsabilidad moral corporativa puede expresarse entonces, al menos para este caso, de maneras más concretas como:

¿existe un acuerdo social, entre los pares corporativos, respecto de cuáles serían las conductas correctas para seleccionar un producto de software con un determinado nivel de confiabilidad, seguridad o pertinencia?

¿existe un acuerdo social, entre los pares corporativos, respecto de cuáles serían los procedimientos para disponer de claves segura y detección de vulnerabilidades?

y por último, ¿existe un acuerdo social, entre los pares corporativos, respecto de cuáles deberían ser las acciones de posibles mitigaciones sociales de las acciones corporativas directas o indirectas?

La respuestas a todas estas preguntas es "sí", "sí" y "sí". La norma ISO 25.000 es un acuerdo corporativo de los ítems de calidad que deben ser considerados en una selección de software, incluyendo confiabilidad y seguridad como parte de sus dimensiones. La norma ISO 27.000 establece como control de seguridad de la información la revisión permanente de los procedimientos de asignación de claves seguras así como de inspecciones de posibles vulnerabilidades de los sistemas. Por último, la norma ISO 26.000 establece el comportamiento genérico de responsabilidad social corporativa.

En conclusión, las condiciones para establecer responsabilidad moral corporativa por situaciones de omisión de seguridad del ciberespacio, están dadas e incluso, las normas establecidas pueden considerarse de amplio conocimiento, aceptación y difusión, como es el caso particular de estas tres normas ISO. A este respecto entonces, sólo queda tomar la decisión de hacerlas parte de las políticas de funcionamiento corporativo.

No más media
ni telecom:
la evolución
es digital