

RED DE POLÍTICAS DE INTERNET Y JURISDICCIÓN
Y COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE (CEPAL)

INFORME SOBRE LA SITUACIÓN REGIONAL

2020



NACIONES UNIDAS

CEPAL



INTERNET &
JURISDICTION
POLICY NETWORK



A large, abstract network graphic composed of numerous small, semi-transparent nodes (circles) and connecting lines (edges) in shades of pink, red, and orange. The network is highly interconnected, forming a complex web that spans the entire page. It is positioned on the left side of the title area.

RED DE POLÍTICAS DE INTERNET Y JURISDICCIÓN
Y COMISIÓN ECONÓMICA PARA AMÉRICA LATINA Y EL CARIBE (CEPAL)

INFORME SOBRE LA SITUACIÓN REGIONAL

2020



CEPAL



Este informe fue encargado por la Secretaría de la Red de Políticas de Internet y Jurisdicción y la Comisión Económica para América Latina y el Caribe (CEPAL) y fue elaborado por Carlos Affonso de Souza.

El informe procura elaborar un mapa del ecosistema y las tendencias actuales del estado de la jurisdicción de Internet en América Latina y el Caribe sobre la base de investigaciones documentales, encuestas y entrevistas a los interesados. No puede garantizarse que la información sea completa, pues este informe es la primera referencia regional sobre el estado de la jurisdicción de Internet.

La CEPAL y la Secretaría de la Red de Políticas de Internet y Jurisdicción agradecen el apoyo financiero e institucional para la elaboración de este informe de la Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), que actúa en nombre del Ministerio de Cooperación y Desarrollo Económicos de Alemania.

Las opiniones expresadas en este documento, cuya versión original en inglés no fue sometida a revisión editorial formal, son de exclusiva responsabilidad de los autores y pueden no coincidir con las de la Secretaría de la Red de Políticas de Internet y Jurisdicción, la CEPAL, los interesados que participan en la Red de Políticas de Internet y Jurisdicción o quienes han brindado apoyo financiero para la elaboración de este informe.

Publicación de las Naciones Unidas
LC/TS.2020/141
Distribución: L
Copyright © Naciones Unidas
Todos los derechos reservados
Impreso en Naciones Unidas, Santiago
S.19-01093

Publicación de Internet & Jurisdiction Policy Network
Copyright © Internet & Jurisdiction Policy Network, 2021
Todos los derechos reservados

Esta publicación debe citarse como: Comisión Económica para América Latina y el Caribe (CEPAL)/Red de Políticas de Internet y Jurisdicción, *Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL): informe sobre la situación regional 2020 (LC/TS.2020/141)*, Santiago, 2021.

La autorización para reproducir total o parcialmente esta obra debe solicitarse a la Comisión Económica para América Latina y el Caribe (CEPAL), División de Documentos y Publicaciones, publicaciones@cepal.org, y a la Red de Políticas de Internet y Jurisdicción, report@internetjurisdiction.net. Se solicita a las entidades interesadas en reproducir esta obra que mencionen la fuente e informen de dicha reproducción a la CEPAL y a la Red de Políticas de Internet y Jurisdicción. Los Estados Miembros de las Naciones Unidas y sus instituciones gubernamentales pueden reproducir esta obra sin autorización previa. Solo se les solicita que mencionen la fuente e informen a la CEPAL de tal reproducción.

Í N D I C E

Agradecimientos.....	5
Prólogo	9
Presentación.....	11
Método	13
Resumen ejecutivo.....	15
Introducción.....	21

CAPÍTULO I

Tendencias generales.....	29
A. El aumento de la conectividad es necesario pero puede reforzar las desigualdades socioeconómicas.....	31
B. El cambiante panorama tecnológico	33
1. Cambios en las percepciones: de la euforia tecnológica a la reacción negativa ante la tecnología (techlash).....	33
2. El transnacionalismo es una nueva dinámica emergente	34
3. Las empresas multinacionales extranjeras son influyentes en la región.....	34
4. El entorno comercial para las empresas emergentes en la región es variable.....	35
C. Las iniciativas regulatorias extranjeras inspiran propuestas regionales y nacionales.....	36
1. Aumenta el apetito por regular el ciberespacio: proliferación de iniciativas.....	37
2. Inspiración legislativa y judicial: ¿intercambio de ideas o mera imitación?.....	38
D. Preocupación por la influencia internacional y la pluralidad normativa.....	39
1. Las normas se establecen para (y por) los grandes agentes internacionales establecidos	39
2. El papel cada vez mayor de las normas de la empresa: el estatus “constitucional” de las condiciones de servicio.....	39
E. El papel de la territorialidad y el ejercicio de la soberanía en una red mundial.....	41
1. El alcance extraterritorial cada vez mayor de las leyes nacionales	41
2. La extraterritorialidad plantea desafíos de ejecución.....	42
F. Nuevas funciones para los intermediarios.....	43
1. Aumento de la responsabilidad de los operadores privados	43
2. Se pide cada vez más a los intermediarios que proporcionen datos para apoyar investigaciones.....	44
3. La transparencia es esencial para aumentar la confianza, pero la implementación varía	45
4. Cada vez se presta más atención al debido proceso en la moderación de contenidos.....	46

CAPÍTULO II

Principales tendencias de actualidad en América Latina y el Caribe	47
A. Expresión	49
1. Noticias falsas y desinformación.....	49
2. Difamación.....	51
3. Acoso en línea.....	53
4. Distribución no consentida de material sexualmente explícito.....	54
5. El “derecho al olvido” se enfrenta a las características particulares de la región.....	56
B. Seguridad.....	58
1. Es necesario aumentar la coordinación de la ciberseguridad para hacer frente a incidentes de alcance generalizado en la región.....	58
2. Investigaciones transfronterizas y pruebas electrónicas.....	59
3. Vigilancia.....	62
4. Ciberseguridad.....	66
C. Economía.....	70
1. Comercio electrónico: la aspiración de un mercado único digital.....	70
2. Propiedad intelectual.....	75
3. Internet de las cosas.....	77
4. Pagos digitales.....	82
5. Cadena de bloques y criptomonedas.....	86
6. Corrientes de datos internacionales y regionales: regímenes de protección de datos.....	88
7. Corrientes transfronterizas de datos internacionales y regionales	91

CAPÍTULO III

Principales enfoques de los dilemas transfronterizos de Internet en América Latina y el Caribe	95
A. Principales tendencias legales	97
1. Los Estados recurren cada vez más a una “doctrina de los efectos” para hacer valer su jurisdicción.....	97
2. La expansión del alcance jurisdiccional.....	99
3. Órdenes de retiro, eliminación y mantenimiento de los tribunales.....	102
4. Multas y sanciones.....	104
5. Las condiciones de servicio están entrelazadas con las leyes nacionales.....	105
B. Principales enfoques técnicos.....	106
1. Tecnologías de geolocalización.....	107
2. El filtrado de contenidos aumenta, a medida que los países luchan contra el discurso de odio y la desinformación	108
3. El Sistema de Nombres de Dominio: suspensiones y bloqueos derivados de notificaciones y órdenes judiciales y administrativas.....	110
4. Bloqueo de sitios y aplicaciones.....	111
5. Cortes de servicio	112
6. Localización obligatoria de los datos	113
Glosario	117

A G R A D E C I M I E N T O S

Este informe fue encargado por la Secretaría de la Red de Políticas de Internet y Jurisdicción y la Comisión Económica para América Latina y el Caribe (CEPAL).

La elaboración de este informe fue posible gracias al aporte financiero de la Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ), que actúa en nombre del Ministerio de Cooperación y Desarrollo Económicos de Alemania, y al aporte de la CEPAL.

EQUIPO DE AUTORES:

AUTOR:

Carlos Affonso de Souza

Universidad del Estado de Río de Janeiro (UERJ)

Director

Instituto de Tecnología y Sociedad de Río de Janeiro (ITS Río)

ASISTENTES DE INVESTIGACIÓN:

Christian Perrone

Doctorando – Becario Fulbright

Investigador senior

Instituto de Tecnología y Sociedad de Río de Janeiro (ITS Río)

Giovana Carneiro

Investigadora júnior

Instituto de Tecnología y Sociedad de Río de Janeiro (ITS Río)

COORDINACIÓN DEL PROYECTO (Internet y Jurisdicción):

Martin Hullin

Director de Operaciones y Asociaciones de Conocimiento

Secretaría de la Red de Políticas de Internet y Jurisdicción

EQUIPO DEL PROYECTO (Internet y Jurisdicción):

Bertrand de la Chapelle

Director Ejecutivo

Secretaría de la Red de Políticas de Internet y Jurisdicción

Paul Fehlinger

Director Ejecutivo Adjunto

Secretaría de la Red de Políticas de Internet y Jurisdicción

EQUIPO DEL PROYECTO (CEPAL)

Edwin Fernando Rojas

División de Desarrollo Productivo y Empresarial

Comisión Económica para América Latina y el Caribe (CEPAL)

Alexis Arancibia

Consultor

Comisión Económica para América Latina y el Caribe (CEPAL)

Alonso Zuñiga Irigoien

Consultor

Comisión Económica para América Latina y el Caribe (CEPAL)

PRODUCCIÓN:

Comisión Económica para América Latina y el Caribe (CEPAL)

Secretaría de la Red de Políticas de Internet y Jurisdicción, París, Francia

EDICIÓN:

Sophie Tomlinson

Manager, Comunicaciones y Divulgación

Secretaría de la Red de Políticas de Internet y Jurisdicción

DISEÑO Y DIAGRAMACIÓN:

Comisión Económica para América Latina y el Caribe (CEPAL)

Se agradecen enormemente el tiempo y las contribuciones de todos los encuestados y entrevistados. Sin sus valiosas opiniones, este informe no podría haberse producido.

Mauricio Agudelo

Coordinador de la Agenda Digital
Banco de Desarrollo de América Latina (CAF)
Colombia

Pablo Bello

Director de Políticas Públicas de Mensajería Privada para América Latina
Facebook
Brasil

Daniel Cavalcanti

Coordinador
Ministerio de Ciencia, Tecnología, Innovación y Comunicaciones
Secretaría de Políticas Digitales
Brasil

María Angélica Chinchilla Medina

Directora de Evolución y Mercado de Telecomunicaciones
Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT)
Costa Rica

Jose Clastornik

Presidente de GovTech Uruguay
Ex Director Ejecutivo
Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento (AGESIC)
Uruguay

Pelayo Covarrubias

Presidente
Fundación País Digital
Chile

Agustina Del Campo

Directora
Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE)
Argentina

César Díaz

Ingeniero
Uruguay

Lester García

Jefe de Políticas Públicas de Conectividad en América Latina
Facebook
México

Raúl Echeverría

Director
Asociación Latinoamericana de Internet (ALAI)
Uruguay

Alexandre Fernandes Barbosa

Director
Centro Regional de Estudios para el Desarrollo de la Sociedad de la Información (CETIC)
Núcleo de Información y Coordinación del Punto BR, NIC.br
Brasil

Matías Fernández Díaz

Gerente de Asuntos Públicos
Mercado Libre
Argentina

Gustavo Gómez

Director Ejecutivo
Observatorio Latinoamericano de Regulación Medios y Convergencia (Observacom)
Uruguay

José Juan Haro

Director de Regulación y Negocios
Mayoristas para Latinoamérica
Telefónica
España

Héctor Huici

Ex Secretario
Secretaría de Tecnologías de la Información y las Comunicaciones
Argentina

Erick Iriarte

Socio
Iriarte & Asociados (IALaw)
Perú

Juan Jung

Ex Coordinador
Centro de Estudios de Telecomunicaciones de América Latina (cet.la)
Uruguay

Yacine Khelladi

Coordinador Regional para América Latina y el Caribe
Alianza para una Internet Asequible (A4AI)
República Dominicana

Juan Carlos Lara

Director de Contenidos
Derechos Digitales
Chile

Carolina Limbatto

Jefa para Las Américas
Cullen International
Bélgica

Omar de León Boccia

Director Ejecutivo
Teleconsult
Uruguay

Lilia Liu

Directora Ejecutiva
Lilia Liu & Associates (LLASO)
Panamá

Maryleana Méndez

Secretaria General
Asociación Interamericana de Empresas de Telecomunicaciones (ASIET)
Costa Rica

Oscar Messano

Presidente
Centro de Capacitación en Alta Tecnología para Latinoamérica y el Caribe (CCATLAT)
Argentina

César Moliné Rodríguez

Director de Ciberseguridad, Comercio Electrónico y Firma Digital
Instituto Dominicano de las Telecomunicaciones (INDOTEL)
República Dominicana

Gonzalo Navarro

Director Ejecutivo
Asociación Latinoamericana de Internet (ALAI)
Uruguay

Rodrigo de la Parra

Vicepresidente, Participación de las Partes Interesadas y Director Gerente - América Latina y el Caribe
Corporación para la Asignación de Nombres y Números en Internet (ICANN)
México

Sissi de la Peña

Gerente de Comercio Digital y Organismos Internacionales
Asociación Latinoamericana de Internet (ALAI)
México

Eric Ramírez

Director
Secretaría de Innovación, Gobierno de El Salvador
El Salvador

Rodrigo Ramírez Pino

Presidente
Cámara Chilena de Infraestructura Digital (IDICAM)
Chile

María Eunices Rivas Robleto

Secretaría Ejecutiva
Consejo Nicaragüense de Ciencia y
Tecnología (CONICYT)
Nicaragua

Beatriz Rodríguez

Presidenta
Capítulo Uruguay de la Internet Society
(ISOCUY)
Uruguay

Jorge Romo

Coordinación de Estrategia Digital Nacional
(CEDN)
Oficina de la Presidencia
México

Eduardo Salido

Director de Asuntos Públicos y Políticas para
América Latina
Telefónica
España

Andrés Sastre

Director Regional para el Cono Sur
Asociación Interamericana de Empresas de
Telecomunicaciones (ASIET)
Uruguay

Thiago Luis Sombra

Socio
Mattos Filho, Veiga Filho, Marrey Jr y
Quiroga Abogados
Brasil

Paloma Szerman

Gerente Senior de Política Regulatoria
GSMA América Latina
Argentina

Fernanda Teixeira Souza Domingos

Fiscal Federal
Ministerio Público Federal
Brasil

Berioska Torres

Subsecretaria
Oficina de la Subsecretaría para Sociedad de
la Información y Gobierno en Línea
Ministerio de Telecomunicaciones y de la
Sociedad de la Información (MINTEL)
Ecuador

Paloma Villa Mateos

Gerente de Políticas Públicas
Telefónica
España

Juan Manuel Wilches Duran

Consultor de telecomunicaciones y
transformación digital
Colombia

Cristina Zubillaga

Consultora Sénior
Ex Directora Adjunta
Agencia de Gobierno Electrónico y Sociedad
de la Información y del Conocimiento
(AGESIC)
Uruguay

PRÓLOGO

ALICIA BÁRCENA

Secretaria Ejecutiva

Comisión Económica para América Latina y el Caribe (CEPAL)

Mientras América Latina y el Caribe se enfrentan a la crisis sanitaria y humanitaria más grave del último siglo, han quedado al descubierto las desigualdades que permean la región. Así como la pandemia de la enfermedad por coronavirus (COVID-19) ha revelado las consecuencias de un acceso desigual a la atención sanitaria, a un sistema de educación de alta calidad y a las oportunidades económicas, la profunda brecha digital se ha hecho más evidente. Más del 60% de los habitantes de la región tiene una conexión a Internet, pero existen marcadas desigualdades en la conectividad según los ingresos, la zona urbana o rural en que se encuentren y su origen étnico, entre otros factores. En algunos países, la brecha de conectividad entre los quintiles más ricos y más pobres de la población es de hasta 60 puntos porcentuales. Para hacer frente a la crisis y reconstruir mejor, es esencial avanzar hacia la conectividad universal y un mayor acceso a las herramientas digitales. Esto solo será posible con marcos normativos fuertes.

La pandemia de COVID-19 aumenta la necesidad de una mayor coordinación en aras de la coherencia de las políticas entre los países de la región en temas como la transferencia transfronteriza de datos, la armonización regulatoria, la privacidad y la seguridad de los datos. La implementación de tecnologías que requieren la rápida transferencia de grandes cantidades de nuevos datos entre numerosos actores para combatir la propagación del coronavirus exige normas comunes e interoperabilidad jurídica. La creciente importancia de las iniciativas de trabajo y aprendizaje a distancia requiere

soluciones de conectividad segura para que nadie se quede atrás.

En su calidad de Secretaría Técnica de la Conferencia Ministerial sobre la Sociedad de la Información de América Latina y el Caribe, la Comisión Económica para América Latina y el Caribe (CEPAL) ha estado trabajando en coordinación con las partes interesadas de los gobiernos y los representantes observadores del mundo académico, la industria, la comunidad técnica y las organizaciones multilaterales para preparar una agenda digital regional, dando prioridad a los temas relacionados con el desarrollo digital de nuestra región durante más de 15 años. A medida que desarrollamos la Agenda Digital para América Latina y el Caribe (eLAC2022), la creación de un mercado digital regional constituye una de las iniciativas de prioridad máxima. El mercado digital regional tiene por objeto fortalecer la integración digital de América Latina y el Caribe, aprovechando la proximidad geográfica y los intereses similares de los países de la región.

Este informe pionero es el primer mapeo integral de su tipo en América Latina y el Caribe y constituye una sólida base empírica que servirá de apoyo al desarrollo de la Agenda Digital para América Latina y el Caribe (eLAC2022). El informe revela y aborda las principales tendencias en el ámbito de la política digital regional en rápido crecimiento y orienta el camino a seguir. Esta contribución vital al debate sobre políticas iluminará algunos de los desafíos que enfrentamos y las oportunidades que podemos aprovechar para acercarnos a un mercado digital regional más integrado y armonizado.

P R E S E N T A C I Ó N

Bertrand de La Chapelle

Director Ejecutivo

Paul Fehlinger

Director Ejecutivo Adjunto

Secretaría de la Red de Políticas de Internet y Jurisdicción

La transformación digital de las economías, los gobiernos y las sociedades de América Latina y el Caribe se está acelerando marcadamente en 2020, catalizada aún más por la pandemia de la enfermedad por coronavirus (COVID-19). Con el aumento de los servicios y las corrientes de datos transfronterizos, aumenta la necesidad de una mayor interoperabilidad y coordinación jurídicas. La acción descoordinada de una amplia gama de actores e iniciativas puede poner en riesgo la digitalización. Para proporcionar un mapeo y análisis indispensable del ecosistema regional de América Latina y el Caribe, la Red de Políticas de Internet y Jurisdicción, en coordinación con la Comisión Económica para América Latina y el Caribe (CEPAL), elaboró este primer *Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL): informe sobre la situación regional 2020*. Se trata de una edición regional del innovador *Internet & Jurisdiction Global Status Report 2019*. El informe se basa en la singular metodología de la Red de Políticas de Internet y Jurisdicción para poner en común el conocimiento de los principales interesados de los Estados, las empresas, los operadores técnicos, las organizaciones internacionales, el mundo académico y la sociedad civil mediante entrevistas y encuestas.

Un mensaje clave del informe sobre la situación regional es que se necesita una mayor coherencia en materia de políticas para construir un ecosistema digital regional próspero e integrado. Al presentar las principales tendencias con respecto al tratamiento de los desafíos jurídicos en el continente, el informe tiene por objeto permitir a los encargados de la formulación de políticas mejorar su comprensión de la

gran cantidad de acontecimientos que se producen a un ritmo acelerado para permitir la innovación de las políticas con una base empírica y avanzar en la interoperabilidad jurídica en el ciberespacio. Al tender un puente entre los campos de la economía digital, la seguridad y los derechos humanos, el informe arroja luz sobre el cambiante panorama tecnológico y normativo de la región. Ofrece la sinopsis más actualizada de la pluralidad de iniciativas de política nacionales y privadas, así como la jurisprudencia que establece las normas para las interacciones, los servicios digitales y las corrientes de datos en línea. El informe revela las últimas tendencias en temas clave que van desde las empresas emergentes, la inteligencia artificial, la Internet de las cosas, la expresión y la privacidad hasta el papel de los intermediarios. Además, muestra la extensión geográfica y el impacto de las medidas nacionales tomadas en la región, así como la influencia de las medidas regulatorias públicas y privadas adoptadas fuera de ella.

Este importante mapeo para los encargados de la elaboración de políticas y la toma de decisiones se realizó gracias a la sólida alianza entre la Red de Políticas de Internet y Jurisdicción y la Comisión Económica para América Latina y el Caribe (CEPAL) en el marco del memorando de entendimiento quinquenal suscrito en 2019. El informe sobre la situación regional constituye un hito en la labor de la Red de Políticas de Internet y Jurisdicción para trazar el mapa del ecosistema jurídico transfronterizo mundial a fin de ayudar a elaborar mejores políticas y soluciones. Esperamos que pueda contribuir a fomentar la coordinación sobre los desafíos jurídicos transfronterizos y la cooperación digital en América Latina y el Caribe y más allá.

MÉTODO

El método elegido para elaborar el presente informe responde a la necesidad de garantizar la comprensión global de un ecosistema sumamente complejo y dinámico, compuesto por múltiples actores, iniciativas y tendencias en diferentes “silos” de políticas de la economía digital, los derechos humanos y la seguridad.

Esto ha llevado a la adopción de un diseño de investigación cualitativo flexible que permite una exploración en profundidad de las preguntas de investigación. Utilizando el método de investigación multifacético aplicado por primera vez para la elaboración del pionero Internet & Jurisdiction Global Status Report 2019, este informe incorpora un innovador proceso de examen y contribución colaborativo a gran escala sin precedentes en América Latina y el Caribe.

En este proceso se aprovecharon los conocimientos especializados combinados de los principales interesados de la Red de Políticas de Internet y Jurisdicción y la CEPAL, así como otros interesados, mediante entrevistas semiestructuradas, examen por homólogos y procedimientos de recolección de datos, combinados con una detallada y amplia investigación documental.

Investigación documental

La investigación documental se basó en métodos convencionales de investigación jurídica y consistió principalmente en un estudio y análisis exhaustivos de la jurisprudencia, la legislación y otras normativas pertinentes, así como de la bibliografía, incluidos libros, artículos de revistas, documentos de conferencias publicados y publicaciones del sector. Esto se complementó con un estudio detallado de una variedad de valiosos informes y otros materiales de diversos organismos elaborados en los últimos años.

La investigación documental se benefició en gran medida de las publicaciones producidas por la CEPAL y la amplia colección de documentos pertinentes de la Red de Políticas de Internet y Jurisdicción que se encuentra disponible en la I&J Retrospect Database. Esta es la publicación emblemática de libre acceso de la Red de Políticas de Internet y Jurisdicción, en la que se documentan las novedades en materia de política, decisiones judiciales, acuerdos internacionales y otros casos que reflejan las tensiones jurisdiccionales en materia de Internet transfronteriza. Esta importante colección proporcionó conocimientos actualizados sobre las principales tendencias, actitudes, novedades e iniciativas actuales. Los materiales contenidos en I&J Retrospect Database también proporcionaron importantes conocimientos sobre los actuales enfoques jurídicos y técnicos de las soluciones, así como sobre lo que en este informe se define como “tendencias generales”.

Encuesta a los interesados

El primer método para recabar la opinión de los interesados consistió en una encuesta en línea compuesta por 15 preguntas sobre diversos temas pertinentes para las preguntas de la investigación. Al considerar la mejor manera de reunir datos de encuestas para responder a las preguntas de la investigación, se tuvo mucho cuidado en formular preguntas

que pudieran ser respondidas por cualquiera de los interesados pertinentes. Esto aseguró que todos los participantes en la encuesta estuvieran expuestos al mismo conjunto de preguntas. La Secretaría de la Red de Políticas de Internet y Jurisdicción y la CEPAL identificaron a los participantes en la encuesta para que representaran a todos los grupos de interesados de la Red de Políticas de Internet y Jurisdicción, es decir, el mundo académico, la sociedad civil, los gobiernos, las organizaciones internacionales, las plataformas de Internet y la comunidad técnica. Los participantes fueron seleccionados específicamente para garantizar la diversidad geográfica en América Latina y el Caribe. Además, la selección de los participantes en la encuesta fue deliberada, pues se los seleccionó específicamente sobre la base de su considerable experiencia y conocimientos. En total, se recibieron contribuciones de más de 40 participantes en la encuesta durante el período comprendido entre el cuarto trimestre de 2019 y el segundo trimestre de 2020. Los participantes expresaron sus opiniones a título personal, más que como representantes de una organización concreta. Los datos obtenidos de las encuestas solo se han utilizado sin atribución. La aportación de los expertos obtenida en el estudio fue inestimable. Además de llamar la atención sobre las principales tendencias de actualidad, los enfoques de las soluciones, las tendencias generales y las preocupaciones generales del ecosistema, los resultados de la encuesta contribuyeron a proporcionar tanto un contexto como una comprensión más matizada de los entornos operativos a los que se enfrentan la sociedad civil, los gobiernos, las organizaciones internacionales, las plataformas de Internet y la comunidad técnica. Los resultados de la encuesta se utilizan a lo largo del informe para mostrar, en cifras, las preocupaciones y actitudes del ecosistema de los interesados encuestados. Asimismo, los comentarios de los interesados encuestados se utilizan para poner de relieve argumentos, observaciones y preocupaciones particularmente importantes.

Entrevistas con las partes interesadas

Se organizaron entrevistas semiestructuradas entre una amplia gama de interesados a fin de complementar los conocimientos adquiridos mediante las respuestas a la encuesta y la investigación documental. Al igual que en las encuestas, se tuvo mucho cuidado en asegurar la inclusión y la diversidad: los expertos entrevistados seleccionados representaban al mundo académico, la sociedad civil, los gobiernos, las organizaciones internacionales, las plataformas de Internet y la comunidad técnica, con diversidad geográfica. Estos interesados se seleccionaron tanto dentro como fuera de la Red de Políticas de Internet y Jurisdicción y la CEPAL.

En promedio, cada entrevista duró más de 30 minutos. Las entrevistas se realizaron de manera confidencial y, por lo tanto, no se grabaron. Sin embargo, se cotejaron notas detalladas y se registraron las observaciones de manera estructurada, lo que facilitó las referencias cruzadas y el análisis detallado. Las entrevistas semiestructuradas permitieron una flexibilidad considerable y la formulación de preguntas complementarias basadas en las conversaciones con el entrevistado. Esto, combinado con la garantía de confidencialidad, contribuyó a crear un entorno en el que los interesados entrevistados pudieron poner de relieve las cuestiones importantes para ellos dentro de los temas debatidos. En muchos casos, los entrevistados también pudieron aportar perspectivas, conocimientos e información que los investigadores no habrían podido obtener de otro modo. De esta manera, parte del propósito de las entrevistas fue reducir las lagunas regionales y temáticas en la investigación documental. En total, se realizaron más de 30 entrevistas entre el cuarto trimestre de 2019 y el segundo trimestre de 2020. Los interesados entrevistados expresaron sus opiniones a título personal, más que como representantes de una organización concreta. Los datos obtenidos de las entrevistas solo se han

utilizado sin atribución. Al igual que los comentarios de los interesados encuestados, los comentarios de los interesados entrevistados fueron vitales y se utilizan a lo largo del informe para poner de relieve argumentos, observaciones y preocupaciones especialmente importantes.

Limitaciones del estudio

Un estudio de investigación de esta naturaleza conlleva ciertas limitaciones. En primer lugar, el alcance del informe se delinea en referencia al mandato de la Red de Políticas de Internet y Jurisdicción y la CEPAL. Por lo tanto, no se trata de un informe de situación regional sobre Internet en general, sino que se centra específicamente en cuestiones jurídicas transfronterizas en relación con Internet. En segundo lugar, a pesar de las medidas señaladas anteriormente, hay que reconocer el riesgo inevitable de que se produzcan lagunas. No debe exagerarse la relevancia estadística de las investigaciones exploratorias que se basan, en parte, en un número limitado de participantes en las encuestas y de expertos entrevistados. Además, la mayoría de las formas de investigación documental pueden implicar sesgos que son difíciles de eliminar por completo a pesar de los mejores esfuerzos.

A la luz de lo anterior, en el presente informe se hace lo mejor posible por presentar un panorama y una documentación muy generales, aunque exhaustivos, de las tendencias pasadas, actuales y emergentes, los actores pertinentes y las soluciones propuestas para los principales desafíos de política jurídica transfronteriza a los que se enfrenta nuestra sociedad conectada a partir del 1 de junio de 2020. Como tal, es una instantánea oportuna del entorno normativo y crea una primera base de referencia regional en América Latina y el Caribe con respecto a la cual se podrán realizar futuros estudios.

RESUMEN EJECUTIVO

El informe *Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL): informe sobre la situación regional 2020* es el primer ejercicio exhaustivo de la región para trazar las diferentes tendencias de política relativas al carácter transfronterizo de Internet y la forma en que afecta a los diferentes actores, como los gobiernos, las empresas y la sociedad civil.

¿De qué manera las diferentes normas nacionales y regionales pueden crear barreras al comercio electrónico transfronterizo y la inversión en los mercados digitales? ¿Qué beneficios económicos y sociales podrían obtenerse mediante la armonización de los marcos jurídicos en toda la región? Una mejor comprensión de esta situación es fundamental para fomentar la confianza de los inversionistas, promover la innovación y la diversificación económica, incrementar la confianza en el comercio electrónico e impulsar un mercado de más de 600 millones de personas, creando una serie de oportunidades para las empresas, en particular para las pequeñas y medianas empresas.

Al mismo tiempo, la acción descoordinada de una amplia gama de actores e iniciativas supone el riesgo de obstaculizar la digitalización de las economías, los gobiernos y las sociedades. A fin de ayudar a los encargados de la formulación de políticas a navegar por los desafíos que se avecinan, la Red de Políticas de Internet y Jurisdicción presenta este informe en coordinación con la Comisión Económica para América Latina y el Caribe (CEPAL).

El informe tiene por objeto: i) el mapeo y la consolidación de la información pertinente para América Latina y el Caribe y el mercado digital regional; ii) la creación y el fortalecimiento de redes regionales de contribuyentes; y iii) el desarrollo de la capacidad de los interesados en temas jurídicos transfronterizos relacionados con la transformación digital.

En las encuestas y entrevistas realizadas para el informe a algunos de los principales expertos de la región, el 78% de los encuestados convino en que los desafíos jurídicos transfronterizos relacionados con Internet se agudizarían cada vez más en los próximos tres años. Al mismo tiempo, el 73,17% de las partes interesadas entrevistadas estaba de acuerdo o muy de acuerdo en que se necesitaba coordinación para hacer frente a los desafíos jurídicos transfronterizos, mientras el 60,98% consideraba que todavía no existían las instituciones necesarias para hacer frente a esos desafíos.

¿Cree que los desafíos jurídicos transfronterizos relacionados con Internet se agudizarán en los próximos tres años?



Fuente: Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL).

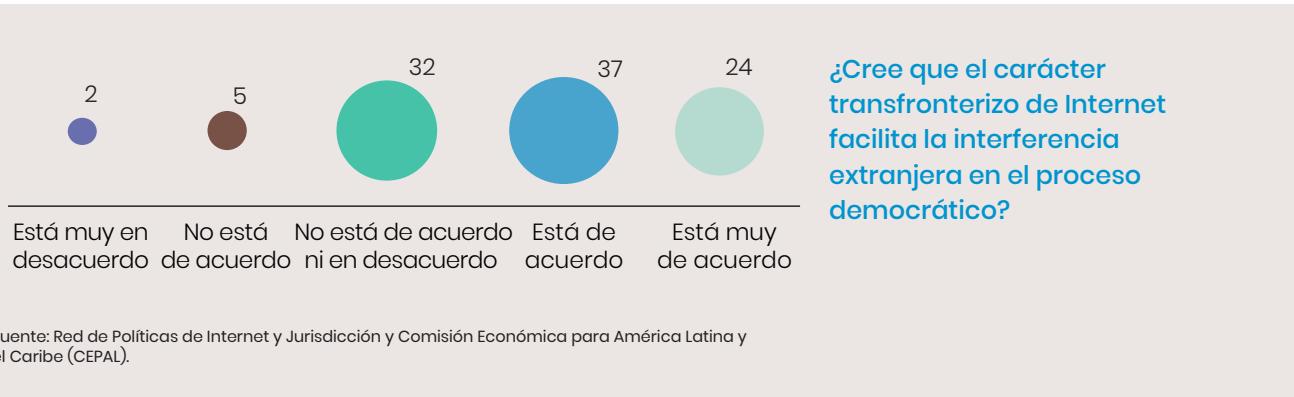
Con miras a analizar las tendencias únicas que se observan en la región, en el informe se investiga la manera en que un panorama tecnológico cambiante potencia la idea de las actividades transnacionales como una nueva dinámica emergente que no solo involucra a las grandes empresas multinacionales, sino que también crea un marco idóneo para el crecimiento acelerado de las empresas emergentes regionales.

En el informe se indica la forma en que los marcos regulatorios regionales y nacionales podrían inspirarse en las iniciativas extranjeras, especialmente las que surgen en los Estados Unidos y la Unión Europea. Es el caso del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, que provocó varios cambios legislativos en América Latina y el Caribe. ¿Hay margen para el intercambio de ideas o se trata de una mera imitación?

A medida que las principales empresas de Internet tratan de adaptarse a las expectativas cambiantes de los gobiernos y del público en general, que suponen cada vez más demandas de mayor responsabilidad, la pluralidad de normas predispone a la región a los conflictos jurisdiccionales, poniendo a prueba los límites de la aplicabilidad y el alcance de las leyes nacionales.

En este informe, las principales tendencias de actualidad en América Latina y el Caribe se organizan en tres grupos: expresión, seguridad y economía. Si bien no faltan tendencias que son exclusivas de la región, hay otras que también se presentan a escala mundial.

Una de las tendencias más apremiantes en materia de expresión es la forma en que la lucha contra la desinformación y las denominadas noticias falsas está llevando a muchos países a adoptar nuevas normas que pueden tener repercusiones mucho más allá de sus fronteras. El 60,98% de las partes interesadas entrevistadas está de acuerdo o muy de acuerdo en que el carácter transfronterizo de Internet facilita la interferencia extranjera en el proceso democrático. No son raros en la región los casos en que cuentas automatizadas de medios sociales creadas en un país terminan desempeñando un papel en las elecciones de otro.



La misma demanda de cooperación entre los países para hacer frente a los problemas jurisdiccionales ha surgido en la región durante la investigación de diversos escándalos de corrupción. Para obtener pruebas localizadas en diferentes países, los organismos encargados de hacer cumplir la ley de América Latina y el Caribe presionan para que haya más cooperación, a fin de crear las condiciones para la estandarización de las transferencias transfronterizas de datos en la región.

La coordinación es indispensable para crear un mercado único digital en América Latina y el Caribe. Un tema que se destacó claramente en las entrevistas y encuestas realizadas para el informe fueron los efectos económicos de un enfoque regional sobre temas como la difusión de la tecnología financiera (fintech) en la región. Los interesados expresaron un apoyo considerable a las soluciones regulatorias innovadoras y el 82,92% estuvo de acuerdo o muy de acuerdo en que la implementación de marcos innovadores, como los entornos de prueba regulatorios (regulatory sandboxes) contribuía a fomentar el crecimiento económico.

En el informe también se destaca la forma en que importantes enfoques de los dilemas transfronterizos de Internet en América Latina y el Caribe podrían provenir de la legislación o del desarrollo de instrumentos tecnológicos, como el bloqueo geográfico y el filtrado de contenidos, con todas las controversias que esos recursos pueden acarrear.

El informe *Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL): informe sobre la situación regional 2020* tiene por objeto proporcionar instrumentos para la innovación de políticas con base empírica y brindar a todos los interesados la información que necesitan para elaborar marcos y normas de política para la sociedad digital en la región. El informe contiene las siguientes observaciones principales:

Principales aspectos transversales de las tendencias y soluciones: tendencias generales

- **La conectividad está aumentando.** Varios países de la región están experimentando un aumento significativo en los niveles de inclusión digital, pero la reducción de la brecha digital y la lucha contra las desigualdades socioeconómicas estructurales siguen siendo importantes desafíos para el desarrollo y la innovación.
- **El panorama está cambiando.** La euforia respecto de una tecnología idealizada ha dado lugar a una fuerte y generalizada reacción negativa ante el poder y la influencia crecientes de las grandes empresas de tecnología (techlash), desencadenada por la preocupación por el discurso de odio, la desinformación y la ciberdelincuencia (con un reciente período de intensidad tecnológica en respuesta a la pandemia de COVID-19 y como parte de la lucha contra ella). Las interacciones transnacionales son una nueva dinámica emergente, la influencia de las empresas multinacionales es fuerte y el entorno empresarial de las empresas emergentes regionales está creciendo.
- **Las iniciativas regulatorias extranjeras han influido en las propuestas regionales y nacionales.** Si bien aumenta el deseo de regular el ciberespacio, como demuestra la proliferación de iniciativas, ¿constituyen estas inspiraciones legislativas y judiciales un útil intercambio de ideas o una mera imitación?
- **Existe preocupación por la influencia externa y la creciente pluralidad normativa.** Las normas se establecen para —y por— los grandes actores internacionales establecidos y el papel de las normas de las empresas aumenta a medida que sus condiciones de servicio alcanzan un estatus “constitucional” en los espacios digitales que controlan.
- **Se cuestiona cada vez más el papel de la territorialidad y la soberanía en una red mundial.** Las leyes nacionales tienen un alcance extraterritorial cada vez mayor, pero esto plantea problemas de aplicabilidad.
- **Se espera que los intermediarios desempeñen nuevos papeles.** Se pide a los operadores privados que asuman cada vez más responsabilidades; los intermediarios se ven llamados a prestar el principal apoyo en las investigaciones administrativas y judiciales; la transparencia es vital para aumentar la confianza, pero la implementación varía; existe una creciente preocupación por las garantías procesales debidas en las actividades de moderación de contenidos.

Principales tendencias de actualidad en América Latina y el Caribe

Expresión:

- Las noticias falsas y las campañas de desinformación suscitan llamados a tomar medidas regulatorias;
- Los gobiernos están imponiendo normas más estrictas para la moderación y eliminación de contenidos en las plataformas en línea;
- La distribución no consentida de material sexualmente explícito (“pornografía de venganza”) no conoce fronteras y puede perpetuar los daños.
- El caso de Google España en el Tribunal de Justicia de la Unión Europea desencadenó un debate regional sobre el “derecho al olvido”: si bien los expertos reconocen el alcance mundial de este derecho, la experiencia regional con las leyes de amnistía y la noción de un “derecho a la memoria” crearon una reacción contra la aplicación de un derecho al olvido general;
- Los casos de difamación están provocando debates sobre los efectos transfronterizos de la protección de la reputación de una persona. Además, la difamación es un delito tanto civil como penal en muchos países de la región, lo que plantea otras interrogantes sobre la forma en que la protección de la reputación podría limitar la libertad de expresión (por ejemplo, en los casos de periodistas y blogueros).

Seguridad:

- Existe una creciente aspiración y necesidad de coordinación en materia de ciberseguridad para hacer frente a incidentes de alcance generalizado en la región;
- Los casos de corrupción transfronteriza en América Latina y el Caribe han alimentado un complejo debate sobre las prácticas de investigación multijurisdiccional;
- Las dificultades para acceder a pruebas digitales en múltiples jurisdicciones determinan la necesidad de examinar las prácticas de investigación actuales en la región;
- Los interesados regionales no abogan por la revisión general del sistema de asistencia judicial recíproca, sino que apoyan su adaptación a la era digital. Sin embargo, los organismos encargados de hacer cumplir la ley en la región tratan cada vez más de acceder a datos de usuarios por fuera de la estructura de los tratados de asistencia judicial recíproca.
- Los interesados regionales coinciden en que el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) es un paso en la dirección correcta para facilitar las investigaciones transfronterizas, pero no resuelve completamente los problemas del sistema de asistencia judicial recíproca.
- Los interesados reafirman que las “puertas traseras” socavan la confianza en los sistemas cifrados;
- Los países de la región aún no han adaptado plenamente su legislación a las exigencias de la lucha contra la ciberdelincuencia;
- El reconocimiento recíproco de las identidades digitales sería un impulso positivo a la integración regional y económica, sobre todo para un mercado único digital.

Economía:

- Inspirados por el Reglamento General de Protección de Datos (RGPD) de la Unión Europea, los países de América Latina y el Caribe están creando o mejorando sus reglamentos nacionales de protección de datos.
- Si bien la mitad de los países de la región cuenta con una reglamentación específica de protección de datos, todavía es posible mejorarla y aumentar la coordinación para lograr un marco verdaderamente regional para la protección de datos;
- Las iniciativas regionales están fomentando la estandarización de las transferencias de datos transfronterizas;
- Existe una demanda para la creación de un mercado único digital en la región;
- Los interesados indicaron que la protección de los consumidores y los datos, los pagos digitales y los regímenes fiscales, entre otras áreas, son fundamentales para la creación de un mercado único digital en la región.
- La región tiene una sólida cultura de derechos del consumidor, que constituye una base útil para la creación de un mercado único digital;
- Las cláusulas de elección de la ley y la jurisdicción aplicables suelen ser mal vistas en el comercio electrónico debido a las normas de protección del consumidor a nivel nacional
- La Internet de las cosas no conoce fronteras y requiere una estandarización, pero los interesados están divididos en cuanto a la necesidad de regulación específica
- Hay varios desafíos y oportunidades para las ciudades inteligentes en la región;
- La agricultura inteligente amplía el conjunto de actores internacionales y es un paso natural para la región;
- Los avances en materia de pagos digitales en la región coexisten con una población no bancarizada, una baja penetración de las tarjetas de crédito internacionales, una cultura del dinero en efectivo difícil de abandonar y la volatilidad de las divisas;

- Las tecnologías financieras están revolucionando los servicios financieros en la región, pero son objeto de un tratamiento regulatorio heterogéneo a nivel nacional
- Los problemas jurisdiccionales transfronterizos afectan cada vez más las actividades del sector de las tecnologías financieras en la región;
- Los interesados muestran un gran entusiasmo por la adopción de soluciones reguladoras innovadoras, como los entornos de prueba regulatorios (*regulatory sandboxes*);
- Las cadenas de bloques y las criptomonedas se consideran facilitadores del comercio transfronterizo (pero también de la delincuencia).

Pincipales enfoques de los dilemas transfronterizos de Internet en América Latina y el Caribe: tendencias legales

- Los Estados recurren cada vez más a una “doctrina de los efectos” para hacer valer su jurisdicción;
- La afirmación de una jurisdicción de gran alcance geográfico puede no conducir a la aplicación efectiva de la ley;
- Los tribunales superiores de la región se han abstenido hasta ahora de adoptar decisiones de alcance mundial;
- Los tribunales nacionales están emitiendo cada vez más órdenes de retiro, eliminación y mantenimiento de contenidos publicados en línea a las plataformas;
- Además de la responsabilidad civil, los países recurren cada vez más a sanciones administrativas para imponer el cumplimiento de las normas sectoriales;
- Las condiciones de servicio de las empresas interactúan con las leyes nacionales, reforzando o contradiciendo las disposiciones que regulan el comportamiento de los usuarios;
- Los efectos de la controvertida actualización de la Directiva sobre los derechos de autor y derechos afines en el mercado único digital de la Unión Europea ya se pueden sentir en la región;
- Los mercados en línea están implementando sistemas de solución de controversias a medida que los gobiernos presionan por la corregulación de la venta de productos falsificados;
- En aras de la protección del consumidor, los tribunales de la región tienden a no sustentar las cláusulas de elección de la ley y la jurisdicción aplicables en las condiciones de servicio de las plataformas internacionales de Internet.

Pincipales enfoques de los dilemas transfronterizos de Internet en América Latina y el Caribe: instrumentos

- El uso de datos personales para mapear y controlar la pandemia de COVID-19 consolidará el debate sobre las tecnologías de geolocalización en la región;
- El bloqueo geográfico y el precio geográfico plantean preocupaciones sobre la protección antimonopolio, del consumidor y de los datos;
- El filtrado de contenidos aumenta, a medida que los países luchan contra el discurso de odio y la desinformación;
- El bloqueo de aplicaciones ha pasado de ser un último recurso a ser una práctica común, con la posibilidad de importantes efectos a través de las fronteras;
- Si bien algunos gobiernos ordenan el bloqueo del Sistema de Nombres de Dominio, no se trata de una práctica generalizada;
- Las interrupciones de Internet no son comunes, pero pueden ocurrir en tiempos de disturbios sociales;
- La localización obligatoria de los datos se ha adoptado por diversas razones en algunos países, pero plantea gran preocupación entre los interesados.

INTRODUCCIÓN

¿POR QUÉ ES NECESARIO UN INFORME SOBRE LA SITUACIÓN REGIONAL?

El presente informe es la primera versión regional del pionero *Internet & Jurisdiction Global Status Report 2019*, que la Red de Políticas de Internet y Jurisdicción presentó en el Foro para la Gobernanza de Internet (FGI) de las Naciones Unidas, celebrado en Berlín en noviembre de 2019, y que proporciona por primera vez una base de referencia mundial para el ecosistema transfronterizo de la jurisdicción de Internet. Este informe regional se basa en la metodología probada del informe mundial de 2019.

Los objetivos del informe Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL): *informe sobre la situación regional 2020* son los siguientes:

- Mapeo y consolidación de la información pertinente para América Latina y el Caribe y el mercado digital regional. El informe ofrece, por primera vez, un panorama regional completo y documentación de las tendencias pasadas, actuales y emergentes, los principales actores y las soluciones propuestas para los principales desafíos de política jurisdiccional transfronteriza a que se enfrentan los interesados en América Latina y el Caribe.
- Investigación de las tendencias y los desafíos de política más relevantes de la sociedad y la economía digitales. En el informe se amplían en particular las conclusiones y cuestiones abarcadas por los tres programas de la Red de Políticas de Internet y Jurisdicción, a saber: el acceso transfronterizo a los datos de los usuarios, las restricciones de contenido transfronterizas y las suspensiones de dominio. En el informe también se examinan los temas y debates emergentes más importantes, incluidos la Internet de las cosas, el comercio digital y las cadenas de bloques, a fin de trazar un mapa de los próximos desafíos en materia de políticas.
- Establecimiento y fortalecimiento de redes regionales de contribuyentes. El informe proporciona una base consolidada para la creación de capacidad mediante el intercambio de conocimientos y la facilitación de la toma de decisiones bien informadas, utilizando un innovador proceso de examen y contribución colaborativo a gran escala para crear una red regional de contribuyentes y aprovechar la experiencia combinada de los interesados mediante entrevistas estructuradas y actividades de recolección de datos.
- Desarrollo de la capacidad de los principales interesados en temas jurídicos transfronterizos relacionados con la transformación digital. Este amplio panorama y análisis de las tendencias e iniciativas proporciona a los encargados de la toma de decisiones una interpretación de las cuestiones sustantivas sumamente complejas y a menudo técnicas involucradas y contribuye al desarrollo de una taxonomía común muy necesaria para el ecosistema de políticas. El objetivo del informe es contribuir a la mitigación de los conflictos jurisdiccionales agudos, apoyar la elaboración de soluciones operacionales concretas y dotar a los actores de política de la información que necesitan para evitar que se pierdan los beneficios de una Internet abierta, interoperable y transfronteriza.

Este documento constituye una guía para los especialistas sobre algunos de los temas más urgentes en torno a la formulación de políticas y el carácter transfronterizo de Internet en América Latina y el Caribe.

A. Internet: un panorama regulatorio en rápida evolución

Durante más de dos décadas se ha debatido sobre la posibilidad y la forma de regular Internet. Sin embargo, antes de llegar a un acuerdo sobre estas cuestiones, es importante reflexionar sobre lo que realmente significa la regulación de Internet. La regulación asume muchas formas diferentes y una ley impuesta por el Estado no es la única manera en la que el comportamiento puede estimularse o

desalentarse. En 1999, Lawrence Lessig sugirió que el tira y afloja regulatorio podría ser más complejo cuando se trata de abordar la manera en que la tecnología afecta el comportamiento humano. Las normas jurídicas no iban a ser la única fuente de regulación. En su lugar, tendrían que enfrentarse a fuerzas en competencia como el mercado y su lógica económica, las limitaciones sociales y, por último, la propia tecnología, cuya arquitectura podría permitir o impedir un determinado tipo de comportamiento¹.

El escenario descrito por Lessig revela que los cambios en la cultura, las fuerzas del mercado o la arquitectura tecnológica podrían ser más eficaces que los cambios legislativos en la configuración de las relaciones y el comportamiento humanos. En consecuencia, para entender el futuro de la regulación de Internet, el análisis debe incluir la acción del Estado, pero no limitarse a esta.

Es indudable que los Estados desempeñan un papel importante al establecer las normas jurídicas, pero también tienen una función de coordinación, al promover la inclusión y la alfabetización digitales en una sociedad determinada y alinear los incentivos de mercado. Sin embargo, el Estado por sí solo no puede controlar plenamente la regulación de Internet o los resultados finales.

Con respecto al tema de la desinformación, por ejemplo, es cada vez más evidente que los incentivos económicos de los modelos de monetización aplicados por las plataformas pueden repercutir en los tipos de contenido desarrollados para la distribución en línea². Las características y los criterios de los algoritmos de selección influyen en el consumo o no de discursos controvertidos, discutidos o que incluso favorecen la polarización en las redes sociales³. La alfabetización mediática y la etiqueta social también desempeñan un papel importante⁴. Todos estos factores contribuyen a frenar la difusión de la desinformación tanto como las normas jurídicas, y a veces incluso más.

Para citar otro ejemplo, la protección de la propiedad intelectual en línea ha avanzado mucho debido a un cambio en el mercado. El procedimiento tradicional de localizar a los delincuentes reincidentes (tanto los que publican material protegido por derechos de autor como los que acceden a este constantemente) y luego cerrar sus cuentas, multarlos o, en algunos casos, incluso encarcelarlos, tiene sus límites. Sin embargo, el surgimiento de plataformas de emisión en directo de videos y música tuvo un gran impacto y el consumo de contenido pirata en línea se redujo drásticamente⁵.

No obstante, justo cuando los consumidores habían empezado a adquirir nuevos hábitos, la multitud de plataformas de emisión en directo terminó por crear nuevas limitaciones económicas, que incrementan el costo para los usuarios de acceder a todos los contenidos que desean. Algunos ven esto como el comienzo de una nueva fase de acceso ilegal generalizado a contenidos en línea protegidos por derechos de autor⁶.

En América Latina y el Caribe, donde los recursos para la aplicación de la ley y la supervisión general son escasos, es aún más importante que las normas jurídicas tengan en cuenta las diferentes fuerzas que intervienen en la regulación de Internet y se beneficien de ellas. El presente informe se basa, pues, en el conocimiento de las tendencias en las cuatro áreas: normas jurídicas, incentivos económicos, normas sociales y tecnología. La idea es extraer conclusiones de su interacción y destacar la manera en que los cuatro puntos del tira y afloja inciden en la regulación transfronteriza.

B. Los intereses en competencia son difíciles de conciliar a través de las fronteras

A nivel básico, el propósito de la regulación de Internet es contrarrestar el abuso, proteger los derechos individuales y salvaguardar la innovación y la economía digital, en particular el acceso al mercado. Sin embargo, desde el punto de vista de la región, es necesario considerar otras dimensiones.

¹ Véase L. Lessig, "The Law of Horse; what CyberLaw might teach", *Harvard Law Review*, vol. 113, N° 501 [en línea] <https://cyber.law.harvard.edu/works/lessig/finalhls.pdf>.

² Véase V. Bakir y A. McStay, "Fake news and the economy of emotions: problems, causes, solutions", *Digital Journalism*, vol. 6, N° 2, 2018 [en línea] <https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1345645>.

³ Véase S. Bradshaw, "Disinformation optimized: gaming search engine algorithms to amplify junk news", *Internet Policy Review*, vol. 8, N° 4, 2019.

⁴ Véase F. Saurwein y C. Spencer-Smith, "Combating disinformation on social media: multilevel governance and distributed accountability in Europe", *Digital Journalism*, vol. 8, 2020.

⁵ Véase M. Freixo Nunes, "On-demand music streaming and its effects on music piracy", tesis de Magister Internacional en Ciencias de Gestión, Universidad Católica Portuguesa, 2018.

⁶ Véase Intelligencer, "Piracy is Back", 26 de junio, 2019 [en línea] <https://nymag.com/intelligencer/2019/06/piracy-is-back.html>.

A pesar de las similitudes percibidas, los países de América Latina y el Caribe son muy diversos en términos de tamaño, desarrollo económico e incluso raíces sociales y culturales. Esta diversidad conduce a complicadas alineaciones de intereses. Existen muchas conexiones y alianzas nacionales, subnacionales y subregionales diferentes, y todas ellas están influidas también por intereses extrarregionales, ya sean los de países y regiones importantes como los Estados Unidos, Europa o China, o los de empresas y organizaciones multinacionales que ejercen presión sobre los encargados de la toma de decisiones a nivel nacional y regional, aparte de las rivalidades fomentadas por un entorno más competitivo que cooperativo.

Todo esto proporciona un difícil telón de fondo para la resolución de dilemas jurídicos transfronterizos. Por una parte, en la región existen normas diferentes e incluso contradictorias, algunas de ellas intrínsecas al sentido de identidad o al orden o la lógica jurídica de cada país. Por otra, la presión de los diferentes grupos de interés puede conducir al trasplante de conceptos jurídicos y a la aplicación inadecuada o inapropiada de soluciones jurídicas.

Este contexto se vuelve particularmente difícil en ausencia de un mecanismo internacional que pueda proporcionar una orientación clara, coordinar la acción y resolver las contradicciones. En busca de eficacia, y a pesar del conflicto de intereses, varios Estados se han arrogado la tarea de resolver los problemas de Internet unilateralmente. Esto se ha traducido en afirmaciones de soberanía sobre el ciberespacio, la aplicación extraterritorial de la legislación nacional e incluso decisiones administrativas y judiciales de alcance mundial (todos estos temas se examinan en el presente informe). El resultado puede ser un mayor potencial de conflictos, una mayor competencia entre los Estados e incluso la exacerbación de las diferencias en el alcance y la capacidad de los Estados, a menos que esos problemas se aborden mediante la cooperación y la coordinación.

C. Las empresas, los gobiernos y las personas están cada vez más preocupados por los abusos en línea

Existe una creciente preocupación por los abusos en línea (desinformación, discursos de odio, acoso, ciberdelincuencia, piratería informática, violaciones de la privacidad y fraude, entre otros). La sensación general es que el rápido aumento de la conectividad ha ido acompañado de oportunidades de comportamiento poco ético e ilegal en línea.

Esta opinión se ve reforzada por la percepción de que la naturaleza sin fronteras del ciberespacio dificulta la labor policial, obstaculiza las investigaciones y limita el alcance de la acción gubernamental. La regulación estatal parece porosa e incapaz por sí sola de abarcar o responder adecuadamente a las actividades que afectan la vida y los bienes de los ciudadanos.

Los interesados encuestados señalaron que esas preocupaciones tenían por lo menos tres dimensiones diferentes: i) las personas que actúan solas o en coordinación pueden causar un gran daño sin estar en ningún momento físicamente presentes en un país, lo que hace más cierto que nunca que el delito y el fraude no conocen fronteras; ii) las empresas internacionales se ven presionadas a tomar medidas y no siempre se sienten obligadas a observar las especificidades de las normas nacionales, en particular cuando los requisitos locales son contrarios a las obligaciones jurídicas de su lugar de constitución; y iii) la influencia extranjera en diferentes formas y grados incide tanto en la sustancia de las respuestas jurídicas locales como en su capacidad para lograr sus objetivos, con desequilibrios de poder entre los países que pueden hacer que la acción nacional sea menor a la ideal.

Además, los escándalos internacionales como las revelaciones de Snowden⁷, el caso Cambridge Analytica⁸ y la publicación de los llamados “documentos de Panamá”⁹ han demostrado hasta qué punto las situaciones que se producen en un país pueden repercutir en el tejido mismo del orden político de otro país. Los instrumentos jurídicos disponibles no abordan o no pueden abordar plenamente los problemas.

⁷ Véase L. M. Austin, “Lawful Illegality: What Snowden Has Taught us about the Legal Infrastructure of the Surveillance State”, abril de 2014 [en línea] <https://ssrn.com/abstract=2524653>.

⁸ Véase F. González y otros, “Global Reactions to the Cambridge Analytica Scandal: A Cross-Language Social Media Study”, 2019 [en línea] https://www.researchgate.net/publication/333066944_Global_Reactions_to_the_Cambridge_Analytica_Scandal_A_Cross-Language_Social_Media_Study.

⁹ Véase L. J. Trautman, “Following the Money: Lessons from the Panama Papers, Part I: Tip of the Iceberg”, *Penn State Law Review*, vol. 807, 12 de mayo de 2017 [en línea] <https://ssrn.com/abstract=2783503>.

Algunos de los interesados entrevistados señalaron que esos incidentes internacionales habían ido a menudo acompañados de agitaciones internas. Un experto observó que muchos gobiernos habían capitalizado esas respuestas emocionales, recurriendo al derecho penal y a la criminalización del comportamiento en línea con diversos grados de éxito. Otro mencionó la tendencia a ampliar el alcance de las leyes nacionales, ya sea aplicándolas extraterritorialmente o creando una forma artificial de localización, en particular al tratar de acceder a datos para investigaciones criminales o con fines de seguridad nacional.

D. Abordar los problemas jurisdiccionales transfronterizos es fundamental para fomentar la confianza en una red mundial

La naturaleza global de Internet es inherente a la manera en que se ha diseñado el ciberespacio. La palabra “mundo” (*world*) en “World Wide Web” no está ahí por casualidad. La capa lógica de Internet está diseñada para no tener fronteras. Sin embargo, el orden mundial internacional está estructurado sobre un principio muy diferente, en el que la igualdad soberana de los Estados hace del Estado nación y de su territorio geográfico el principal centro de regulación¹⁰. Es de esperar que haya diferentes enfoques e incluso prioridades. Así, la regulación tiende a no ser constante ni uniforme.

La gestión de la coexistencia de leyes y métodos regulatorios tan heterogéneos como los que se aplican a la Internet transfronteriza es uno de los mayores desafíos de política del siglo XXI. No es posible formular soluciones de política escalables y coherentes sin una comprensión cabal de este ecosistema sumamente complejo y dinámico, que comprende múltiples actores, iniciativas y tendencias de todos los “silos” de políticas de la economía digital, los derechos humanos y la seguridad.

Esta paradoja de regulación primaria local y espacio global (ciberespacio), sumada a la multiplicidad de actores, suele conducir naturalmente a la fragmentación. Hay dos fenómenos que pueden afectar Internet en la situación actual. El primero es su tendencia a fragmentarse, recreando las fronteras del mundo físico en el ciberespacio. El segundo son las iniciativas de las instituciones nacionales para ejercer una influencia extraterritorial en un intento de regular la Internet mundial desde un punto de vista unilateral y nacional. Ambas dinámicas socavan la utilidad y la confianza en la Internet mundial.

La historia de la lucha contra la colonización en América Latina y el Caribe y el consiguiente surgimiento del principio internacional de no intervención tienden a reforzar ambos fenómenos: la fragmentación y las iniciativas para ampliar el alcance de la legislación nacional de manera extraterritorial. Sin embargo, las diferencias de tamaño, poder y eficiencia administrativa han significado diversos grados de éxito.

En todo caso, los expertos encuestados señalaron la tendencia de los países de la región a regular Internet y a afirmar su soberanía sobre el ciberespacio. Esto parece ser particularmente cierto en lo que respecta a los datos y se traduce en reivindicaciones relativas a la soberanía de los datos y su localización (como se analiza en el capítulo III.B.6) y en aplicaciones extraterritoriales de la legislación sobre protección de datos (como se analiza en el capítulo II.C.6).

Para avanzar en el debate regional sobre el diseño y la aplicación de la legislación en línea y catalizar la elaboración de un marco compartido, es importante que los interesados entablen diálogos permanentes para ayudar a definir los retos y fomentar la coordinación de las diferentes iniciativas y propuestas de política. Obtener información de calidad mediante la investigación y la documentación pertinentes es fundamental para apoyar los procesos de toma de decisiones y estimular la innovación de políticas con base empírica. En este informe se presentan el estado actual del debate y las tendencias en curso, proporcionando la base para una reflexión muy necesaria sobre la forma de abordar adecuadamente el aspecto de la coordinación de la jurisdicción y las preocupaciones transfronterizas.

¹⁰ Véase M. Kettemann, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*, Oxford University Press, 2020 [en línea] https://www.hans-bredow-institut.de/uploads/media/default/cms/media/ijp5yvb_Kettemann_The-Normative-Order-of-the-Internet.pdf.

Desde el punto de vista de la región, la integración digital es sin duda una oportunidad. Es una parte indispensable de la labor para diversificar las economías regionales. Hay pruebas del enorme potencial para que el comercio intrarregional avance hacia una canasta de exportación más intensiva en conocimientos. En 2018, el 54% del valor de las exportaciones intrarregionales consistió en manufacturas de alta, media y baja tecnología¹¹. Al mismo tiempo, el rápido crecimiento del comercio electrónico transfronterizo ofrece grandes oportunidades a las pequeñas y medianas empresas (pymes) para comerciar a nivel internacional.

Se estima que 155,5 millones de personas en América Latina compraron bienes y servicios en línea en 2019, lo que supone un aumento sustancial del 22% con respecto a los 126,8 millones que lo hicieron en 2016. Sin embargo, el promedio anual de transacciones en línea per cápita en América Latina fue el más bajo del mundo en 2016, con solo 9,2 por año¹².

En la región se han registrado importantes avances en materia de legislación relativa a Internet. En 2017, más del 80% de los países de América Latina y el Caribe contaba con algún tipo de legislación sobre transacciones electrónicas y firma electrónica y el 90% tenía normas sobre propiedad intelectual.

Estas cifras ponen de relieve la importancia de promover un marco jurídico y regulatorio armonizado para ayudar a eliminar las barreras al comercio electrónico transfronterizo y la inversión en los mercados digitales. La armonización de los marcos normativos en toda la región podría crear importantes beneficios económicos y sociales que podrían incrementar la confianza de los inversionistas y la inversión extranjera directa y promover la innovación y la diversificación económica. También podría fomentar la confianza en el comercio electrónico e impulsar un mercado de más de 600 millones de personas, creando al mismo tiempo una serie de oportunidades para las empresas, incluidas en particular las pequeñas y medianas empresas.

E. Se necesita coordinación para hacer frente a este desafío que se ha pasado por alto

Los países de la región son cada vez más conscientes de la dimensión internacional de los retos planteados por Internet. Ha quedado claro que el carácter mundial de la World Wide Web es una fuente tanto de fortaleza, pues ofrece muchas oportunidades sociales y económicas, como de dificultades, en particular la interacción entre la acción local y el impacto internacional y viceversa.

Sin embargo, las estructuras gubernamentales nacionales parecen insuficientes por sí solas para hacer frente a muchos de los problemas que plantea Internet. Con la eficacia de la acción de los Estados cuestionada de esta manera, las nociones de soberanía y de no injerencia parecen adquirir connotaciones diferentes.

Esta percepción se ve reforzada por el poder relativo y el impacto potencial de los países de América Latina y el Caribe. Los entrevistados hablaron de la impresión de que no todos los Estados pueden tener la misma influencia en la forma en que se regula Internet o en la forma en que estos y sus ciudadanos se ven afectados por su estructura y sus mecanismos de gobernanza.

1. La necesidad de un diálogo entre múltiples interesados en la región

La comunidad internacional reconoce desde hace tiempo la necesidad de un diálogo entre múltiples interesados para examinar la gobernanza de Internet. El Foro para la Gobernanza de Internet (FGI) es la plataforma preeminente para ese diálogo. Sin embargo, en el informe del Secretario General de 2020 del Panel de Alto Nivel sobre la Cooperación Digital se señalaron los desafíos y las lagunas de los acuerdos de cooperación digital existentes y se propusieron tres posibles arquitecturas para esa cooperación a escala mundial¹³. Así, los actuales mecanismos de toma de decisiones sobre la gobernanza de Internet están en proceso de mejora.

¹¹ Véase Comisión Económica para América Latina y el Caribe (CEPAL), *Perspectivas del Comercio Internacional de América Latina y el Caribe*, 2018 (LC/PUB.2018/20-P), Santiago, 2018.

¹² Véase Statista, *E-commerce in Latin America* [en línea] <https://www.statista.com/study/14764/e-commerce-in-latin-america-statista-dossier/>.

¹³ Véase Naciones Unidas, *The Age of Digital Interdependence. Report of the UN Secretary-General's High-level Panel on Digital Cooperation*, 2020, págs. 22-29 [en línea] <https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf>.

El primer Foro de Gobernanza de Internet de América Latina y el Caribe (LACIGF) se celebró en 2008 por iniciativa de la Asociación para el Progreso de las Comunicaciones (APC), el Registro de Direcciones de Internet para América Latina y el Caribe (LACNIC) y la Red de Informaciones para el Tercer Sector (RITS). Entre mayo de 2019 y julio de 2020, el Comité de Programa del LACIGF realizó una revisión del LACIGF a fin de formular propuestas concretas para elaborar y evaluar puntos de acción para mejorar los foros¹⁴. Las partes interesadas mencionaron que el LACIGF ofrece una importante oportunidad para el mapeo colectivo de los problemas y la elaboración de políticas públicas comunes, incluso en ausencia de decisiones vinculantes. También es importante velar por que esos mecanismos de coordinación tengan en cuenta la diversidad e incluyan a los jóvenes, las mujeres y los pueblos indígenas, aumentando al mismo tiempo la representación subregional de América Latina y el Caribe. A nivel nacional, no todos los países de América Latina y el Caribe cuentan con un programa activo de temas relacionados con la gobernanza de Internet. Tomando las iniciativas nacionales del FGI (iniciativas nacionales y regionales del FGI) como punto de partida para el análisis, el primer evento nacional sobre la gobernanza de Internet se celebró en el Brasil en 2011. En el momento de redactar el presente informe, las actividades nacionales del FGI en América Latina y el Caribe se llevan a cabo en: Argentina, Barbados, Bolivia (Estado Plurinacional de), Brasil, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Haití, Honduras, México, Panamá, Paraguay, Perú, República Dominicana, San Vicente y las Granadinas, Trinidad y Tabago, Uruguay y Venezuela (República Bolivariana de)¹⁵.

Como demuestra la rápida difusión de esta iniciativa, el debate sobre la gobernanza de Internet ha ido cobrando fuerza en la región. Esto pone de relieve la forma en que las iniciativas de algunos países pueden servir de inspiración y alentar a otros países de América Latina y el Caribe a fortalecer el debate nacional sobre temas relacionados con Internet. Aunque no se trata de un paso necesario para la coordinación regional, los avances a nivel nacional también son importantes porque aumentan el capital humano y la capacidad de los encargados de la formulación de políticas de trabajar a escala regional y mundial. Los interesados describieron a la Comisión Económica para América Latina y el Caribe (CEPAL) como una pionera y un importante órgano de gobernanza que cuenta con la infraestructura necesaria no solo para promover las iniciativas de creación de capacidad en los países donde todavía no se ha trabajado mucho en estos temas, sino también para desempeñar un papel activo como catalizadora de la transformación de manera más amplia.

Los interesados mencionaron entidades regionales que podrían abordar algunas de las cuestiones que se tratan en el presente informe, como la Comisión Interamericana de Telecomunicaciones (CITEL) y el Foro Latinoamericano de Entes Reguladores de Telecomunicaciones (REGULATEL), pero observaron que aún faltaba mucho para lograr una cooperación y armonización regional genuina y significativa. Las políticas implementadas presentan un problema de continuidad, que sugiere la necesidad de políticas de mediano y largo plazo en la región.

2. Una creciente aspiración a la cooperación y la coordinación

La cooperación y la coordinación se han convertido en objetivos importantes y tal vez necesarios para hacer frente a los desafíos transfronterizos. El argumento a favor de una acción coordinada parece sólido a la luz de los potenciales beneficios para la economía (en términos de escala, acceso a los mercados y tecnología) y para la seguridad (ciberseguridad y protección de los servicios básicos y la infraestructura crítica). La cooperación y la coordinación también tienen un papel importante que desempeñar para abordar grandes problemas sociales como la desinformación y la ciberdelincuencia.

¹⁴ Véase LACIGF, "Proposed first consultation for the review of LACIGF", 2020 [en línea] <https://lacigf.org/propuesta-de-primer-a-consulta-para-revision-del-lacigf/>. Véase más información en R. Echeberría, *Review of the Latin American and Caribbean Internet Governance Forum (LACIGF), Public Consultation Process, Report and Conclusions*, 2020 [online] <https://lacigf.org/en/revision-del-lacigf/>.

¹⁵ IGF, Latin American and Caribbean Regional Group (GRULAC) [online] <https://www.intgovforum.org/multilingual/content/latin-american-and-caribbean-regional-group-grulac>; también C. Aguirre y otros, *Mapping National Internet Governance Initiatives in Latin America*, Universidad de Pennsylvania 2018 [en línea] http://globalnetpolicy.org/wp-content/uploads/2018/06/Latin-American-Report_IPO_final.pdf.

La acción descoordinada de una amplia gama de actores e iniciativas puede llegar a obstaculizar la digitalización de las economías, los gobiernos y las sociedades. El 73,17% de los interesados entrevistados está de acuerdo o muy de acuerdo en que existe una necesidad de coordinación para abordar los desafíos jurídicos transfronterizos.

Esa cifra por sí sola es suficiente para establecer la dirección de este informe, presentado por la Red de Políticas de Internet y Jurisdicción en coordinación con la CEPAL para proporcionar un mapeo y análisis indispensables del ecosistema regional de América Latina y el Caribe.



Dado el objetivo de América Latina y el Caribe de desarrollar un mercado único digital, las partes interesadas encuestadas para este informe trasmítieron un mensaje contundente, pues el 78,04% estuvo de acuerdo en que se necesitaría un esfuerzo considerable para armonizar las normas a fin de lograr ese objetivo. Como destacó uno de los interesados encuestados:

“Creo que los países del MERCOSUR y de América Latina deberían encontrar la manera de participar en una amplia regulación transfronteriza, que podría fomentar la economía digital en la región. Hoy en día, el marco jurídico es muy escaso y carece de puntos en común. Esta falta de uniformidad está comprometiendo el desarrollo de la región”.

En un mundo en transición hacia una nueva década, los países de América Latina y el Caribe se enfrentan a la oportunidad de fomentar la integración regional en un momento en que los países necesitan reinventar sus papeles en el escenario mundial después de la pandemia de COVID-19. Las repercusiones sociales y económicas serán graves y comprender la manera en que las diferentes decisiones de política sobre Internet (y la tecnología en general) pueden afectar a otros países será fundamental para los nuevos marcos que puedan surgir de la crisis.

CAPÍTULO

**TENDENCIAS
GENERALES**

La combinación de una detallada investigación documental y las contribuciones de los interesados (mediante la encuesta y las entrevistas) puso de relieve varias tendencias generales que son fundamentales para cualquier debate sobre los desafíos jurídicos transfronterizos relacionados con Internet en su conjunto. Algunas de esas tendencias reflejan claramente las descritas en el *Internet & Jurisdiction Global Status Report 2019*¹⁶. En este informe se destaca la forma en que se están desarrollando específicamente en América Latina y el Caribe. Estas tendencias generales dan forma a las tendencias de actualidad (véase la sección IV) y, en cierta medida, establecen los parámetros dentro de los cuales se pueden explorar los enfoques jurídicos y técnicos (véase la sección V).

A. El aumento de la conectividad es necesario pero puede reforzar las desigualdades socioeconómicas

Aunque las diversas repercusiones jurisdiccionales del carácter transfronterizo de Internet tienen consecuencias similares en todo el mundo, el número de casos, sus efectos y la viabilidad de las posibles soluciones variarán según el grado de inclusión digital en un país determinado. En América Latina y el Caribe, el 67% de la población es usuaria de Internet, con diferencias regionales y nacionales que varían según el nivel socioeconómico y la ubicación geográfica¹⁷.

En las iniciativas de inclusión digital y desarrollo tecnológico se deberían tener en cuenta ciertas desigualdades, especialmente las relacionadas con los ingresos, el género, las diferencias entre las zonas urbanas y rurales, la forma en que las comunidades indígenas acceden a Internet y el grado de accesibilidad y comprensión de los recursos en línea para la población mayor¹⁸.

El grado en que las estrategias nacionales de desarrollo digital tienen en cuenta cada uno de estos factores varía. Por ejemplo, en una comparación entre 14 estrategias nacionales de la región, se comprobó que solo 4 daban prioridad al aumento del acceso de las personas de menor nivel socioeconómico, lo que significa que se necesita una nueva agenda política centrada en la reducción de las asimetrías en el acceso a Internet¹⁹. Al mismo tiempo, al menos 12 países abordan la brecha digital desde tres perspectivas importantes: i) el desarrollo de una infraestructura sólida para una conectividad digital de alta calidad, ii) la promoción del uso de las tecnologías de la información y las comunicaciones (TIC) en la vida diaria y iii) el desarrollo económico con el uso de plataformas y servicios digitales²⁰.

Cuando Internet resultó ser la principal vía para que los ciudadanos trabajaran, estudiaran y accedieran a los servicios básicos durante la crisis del COVID-19, distintos agentes regionales reconocieron que un ecosistema digital desarrollado estaba intrínsecamente relacionado con el desarrollo social y económico y que Internet era un instrumento necesario para diversas actividades cotidianas como el trabajo, el estudio, el comercio y las comunicaciones. Los países con una mayor brecha digital han sufrido más consecuencias negativas que aquellos que tienen una menor. Entre 2004 y 2018, el ecosistema digital de América Latina y el Caribe se desarrolló menos que en cualquier otra región en desarrollo, a excepción de los Estados Árabes²¹. En general, la penetración de Internet ha aumentado considerablemente en los países de América Latina y el Caribe, pero sigue habiendo diferencias entre

¹⁶ Véase [en línea] <https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report>.

¹⁷ Véase Banco de Desarrollo de América Latina (CAF) y otros, *Las oportunidades de la digitalización en América Latina frente al COVID-19*, Santiago, 2020, pág. 9.

¹⁸ Véase Martínez, A. Palma y A. Velásquez, "Revolución tecnológica e inclusión social: reflexiones sobre desafíos y oportunidades para la política social en América Latina", serie *Políticas Sociales*, N° 233 (LC/TS.2020/88), Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), 2020.

¹⁹ Ibídem, pág. 57.

²⁰ Ibídem, pág. 55.

²¹ Asia y el Pacífico: 9,39%; África: 8,27%; Europa Oriental: 6,89%; América Latina y el Caribe: 6,21% (Banco de Desarrollo de América Latina (CAF) y otros, *Las oportunidades de la digitalización en América Latina frente al COVID-19*, Santiago, 2020, pág. 5).

ellos. En el Ecuador, el 60,67% de la población tenía acceso a Internet en 2018, cifra que aumentó al 68,09% en 2020. En Honduras, esa proporción se incrementó del 34,06% en 2018 al 39,33% en 2020²².

También es importante señalar que la inclusión digital es un concepto que va más allá del acceso a Internet *per se*. Un estudio del Banco de Desarrollo de América Latina (CAF) ha determinado que los instrumentos de comunicación y los medios sociales representan el grueso del uso de Internet en la región²³. Esto indica la necesidad de un ulterior desarrollo para liberar el pleno potencial de la inclusión digital en sus aspectos sociales y económicos.

En cualquier caso, poner Internet a disposición de todos los ciudadanos es una preocupación importante y forma parte de la Agenda 2030 para el Desarrollo Sostenible. La meta 9.c consiste en “Aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020”. Según un estudio de la Comisión Económica para América Latina y el Caribe (CEPAL) de 2020 sobre escenarios y proyecciones considerando la pandemia de COVID-19, la región “alcanzaría la meta con la tendencia actual”²⁴.

Un marco digital y conectado también tiene un papel que desempeñar en el desarrollo de otras tecnologías que son particularmente importantes en la región, como la agricultura inteligente. Cuanto más desconectada está una zona rural, más lejana es la perspectiva de una agricultura conectada y eficiente. El desarrollo ya puede observarse en las iniciativas de inclusión digital centradas en la logística y las cadenas de suministro agroindustriales²⁵.

Además, a medida que los países desarrollan sus estrategias de gobierno digital y ofrecen cada vez más servicios públicos parcial o totalmente por Internet (por ejemplo, solicitudes de prestaciones sociales, bases de datos de presentación de impuestos y de registro), la inclusión digital significa cada vez más el disfrute de los derechos básicos de los ciudadanos. La expansión de las iniciativas de identidad digital es también un buen ejemplo de esta tendencia.

En estudios comparativos recientes sobre los países de América Latina y el Caribe se ha reconocido la importancia de las políticas públicas para reducir la brecha digital en la región²⁶. Esas políticas suelen incluir no solo el acceso a la red propiamente dicha, sino también disposiciones relativas a la infraestructura, la fabricación de dispositivos y el desarrollo de aptitudes digitales. Los avances difieren en la región, pero a continuación se mencionan algunos aspectos destacados.

- En agosto de 2020, se promulgó en la Argentina el Decreto núm. 690/2020, mediante el que se declara que los servicios de tecnología de la información y las comunicaciones (TIC) son servicios públicos sujetos a reglas administrativas más estrictas²⁷. En el decreto también se dispuso que no se aumentaran los precios de esos servicios, incluidos los de radio y telefonía (móvil o fija), hasta el 31 de diciembre de 2020.
- En el Perú, Telefónica, Facebook, el Grupo BID y el Banco de Desarrollo de América Latina (CAF) se asociaron para crear el proyecto Internet para Todos (IpT). Hasta 2020, el proyecto ha conectado a más de 1,5 millones de peruanos en zonas rurales con la tecnología 4G. Para 2021, la meta es proporcionar acceso a Internet a 30.000 comunidades rurales²⁸. Otro objetivo es ampliar el proyecto a otros países de América Latina y el Caribe²⁹. Esto demuestra el potencial de las alianzas público-privadas para el desarrollo de Internet en la región.

²² Véase Telecom Advisory Services, *El estado de la digitalización de América Latina frente a la pandemia del COVID-19*, Banco de Desarrollo de América Latina (CAF), abril de 2020, pág. 18 [en línea] https://sciooteca.caf.com/bitstream/handle/123456789/1540/El_estado_de_la_digitalizacion_de_America_Latina_frente_a_la_pandemia_del_COVID-19.pdf?sequence=1&isAllowed=y.

²³ Ibídem, pág. 18-21.

²⁴ Véase Comisión Económica para América Latina y el Caribe (CEPAL), *La Agenda 2030 para el Desarrollo Sostenible en el nuevo contexto mundial y regional: escenarios y proyecciones en la presente crisis* (LC/PUB.2020/5), Santiago, 2020, pág. 64 [en línea] https://repositorio.cepal.org/bitstream/handle/1362/45336/6/S2000208_es.pdf.

²⁵ Véase, por ejemplo, el caso del Perú en Banco de Desarrollo de América Latina (CAF), “Sector público y privado comprometido en hoja de ruta para la digitalización de la cadena agroexportadora en región Ica”, 24 de enero de 2020 [en línea] <https://www.caf.com/es/actualidad/noticias/2020/01/sector-publico-y-privado-comprometido-en-hoja-de-ruta-para-la-digitalizacion-de-la-cadena-agroexportadora-en-region-ica/?parent=6429>. Véase, también, G. Pérez, “Caminos rurales: vías claves para la producción, la conectividad y el desarrollo territorial”, *Boletín FAL*, N° 377, Santiago, Comisión Económica para América Latina y el Caribe (CEPAL), julio de 2020.

²⁶ Véase L. Robinson y otros, “Digital inclusion across the Americas and the Caribbean”, *Social Inclusion*, vol. 8, N° 2, 2020.

²⁷ Argentina, “Decreto 690/2020”, *Boletín Oficial de la República Argentina*, 21 de agosto de 2020 [en línea] <https://www.boletinoficial.gob.ar/detalleAviso/primera/233932/20200822>.

²⁸ Banco de Desarrollo de América Latina (CAF), “Internet para todos’ contribuye a cerrar la brecha digital y ya conecta a más de 1 millón y medio de peruanos en zonas rurales”, 4 de mayo de 2020 [en línea] <https://www.caf.com/es/actualidad/noticias/2020/05/internet-para-todos-contribuye-a-cerrar-la-brecha-digital-y-ya-conecta-a-mas-de-1-millon-y-medio-de-peruanos-en-zonas-rurales/>.

²⁹ Banco Interamericano de Desarrollo (BID), “Internet para Todos: disminuyendo la brecha digital en América Latina”, 2020 [en línea] <https://www.iadb.org/es/mejorando-vidas/internet-para-todos-disminuyendo-la-brecha-digital-en-america-latina>.

- El programa de inclusión digital del Estado Plurinacional de Bolivia incluye la participación de ciudadanos voluntarios en apoyo de las actividades en curso en las comunidades locales³⁰.
- En 2015, el Brasil puso en marcha el proyecto Amazônia Conectada, destinado a ampliar la tecnología de banda ancha en la región amazónica. Aunque se han hecho progresos en la infraestructura de Internet, el proyecto ha sido objeto de considerables críticas y ha sido evaluado negativamente por el Tribunal de Cuentas de la Unión (TCU) debido a fallas técnicas y de implementación³¹.
- En 2019, el Sector de Desarrollo de las Telecomunicaciones (UIT-D) de las Naciones Unidas hizo participar a 75 líderes indígenas de la Argentina, el Estado Plurinacional de Bolivia, Chile, Colombia, Costa Rica, el Ecuador, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá, el Paraguay, el Perú y la República Bolivariana de Venezuela en actividades de desarrollo de la capacidad centradas en instrumentos innovadores³².

La inclusión digital sigue siendo un gran desafío en América Latina y el Caribe y una prioridad al abordar la regulación de Internet. Se debe prestar especial atención a la capa de infraestructura de Internet, donde el carácter transfronterizo de la red tropieza con las necesidades básicas de desarrollo local. Pero, ¿podría haber margen para una mayor cooperación a fin de desarrollar soluciones y formas innovadoras de abordar la brecha digital? Una mayor integración en la región tiene el potencial de fomentar el desarrollo y el intercambio de mejores prácticas para cerrar la brecha digital, así como de conectar a más personas a una única Internet mundial.

B. El cambiante panorama tecnológico

Las percepciones sobre la manera en que Internet ha afectado casi todo, desde las actividades cotidianas triviales hasta los elementos constitutivos de las relaciones internacionales, han cambiado drásticamente en las últimas décadas. América Latina y el Caribe tiene sus propias peculiaridades que invitan a seguir analizando la forma en que los países de la región han integrado el componente digital en sus estrategias nacionales e internacionales. ¿En qué medida el acceso a Internet ha cambiado la vida de los ciudadanos de los países de América Latina y el Caribe? ¿Quiénes son los actores que dan forma a las políticas digitales en la región y cómo afectan a los gobiernos, las empresas y los individuos más allá de las fronteras nacionales?

1. Cambios en las percepciones: de la euforia tecnológica a la reacción negativa ante la tecnología (techlash)

Algunas personas sostienen que, si Internet debe conectarnos a todos, no debería permitirse ningún tipo de regulación en el ciberespacio. En 1996, la conocida “Declaración de independencia del ciberespacio”, de John Perry Barlow, trazó una línea entre los Estados como “cansados gigantes de carne y acero” y el ciberespacio como “el nuevo hogar de la Mente”³³. Al proclamar las virtudes que derivan de la existencia de un espacio virtual para el libre flujo de información, Barlow instó a los Estados a no interferir en el desarrollo de la red mediante regulaciones de ningún tipo.

El debate sobre la regulación de Internet ha cambiado desde finales de la década de 1990. En términos muy generales, la euforia tecnológica de los tiempos de Barlow ha dado paso a una percepción más desalentadora sobre la manera en que Internet se podría utilizar para cometer delitos y difundir desinformación, lo que afecta enormemente el disfrute de los derechos fundamentales y erosiona el discurso político. Lo que comenzó como euforia tecnológica se convirtió en una fuerte reacción negativa ante el poder y la influencia crecientes de las grandes empresas de tecnología (techlash) y dio lugar a importantes iniciativas de regulación.

Sin embargo, el comienzo de la década de 2020 marca un hito importante. A medida que la lucha contra el COVID-19 obligó a los países a cerrar las fronteras e imponer medidas de confinamiento, Internet funcionó como un salvavidas para que las familias, las empresas y los gobiernos siguieran comunicándose en tiempos difíciles. Si bien no es posible volver al período de euforia, el péndulo

³⁰ Estado Plurinacional de Bolivia, “Bolivia: Decreto Supremo N° 3900, 8 de mayo de 2019”, mayo de 2019 [en línea] <https://www.lexivox.org/norms/BO-DS-N3900.html>. Véase también Agencia de Gobierno Electrónico y Tecnologías de Información y Comunicación (AGETIC), “Decreto Supremo N° 3900”, 10 de junio de 2019 [en línea] <https://digital.gob.bo/2019/06/contenido-libre/>.

³¹ A. B. Gomes, F. Duarte y P. Rocillo, *Inclusão digital como política pública: Brasil e América do Sul em perspectiva*, Belo Horizonte, Institute for Research on Internet & Society (IRIS), 2020.

³² Unión Internacional de Telecomunicaciones (UIT), “Indicadores de nuestros programas de capacitación para el fortalecimiento de los pueblos indígenas” [en línea] <https://www.itu.int/en/ITU-D/Digital-Inclusion/Indigenous-Peoples/Pages/Indicadores.aspx>.

³³ Véase J. P. Barlow, “Declaración de independencia del ciberespacio”, Davos, 1996 [en línea] <https://revistas.uca.es/index.php/periferica/article/view/943/796>.

parece oscilar de nuevo y la percepción pública del papel que Internet desempeña en la vida de las personas podría sufrir otra transformación³⁴.

Por paradójico que parezca, el cierre de las fronteras para contener el virus fue acompañado de un aumento de la actividad en línea de los particulares, las empresas y las autoridades. Miles de servicios públicos y privados se vieron obligados a digitalizarse para poder seguir sirviendo al público en general.

Numerosos países han recurrido a la prestación de servicios en línea, desde beneficios de emergencia hasta acciones públicas cotidianas básicas. Incluso los poderes legislativos y judiciales de muchos países han trasladado sus actividades a Internet. En el sector privado, muchas empresas han ofrecido sus servicios en línea para sobrevivir y enviado a todos los empleados cuyas actividades se pueden realizar fuera de sus establecimientos a trabajar desde casa. De repente, millones de personas y miles de empresas tuvieron que adaptarse a la era digital.

Internet ha cobrado relevancia e importancia, mostrando sus aspectos positivos y muchas de sus complejidades. Por una parte, las personas han podido mantener cierto grado de relaciones interpersonales gracias a la red. Por otra, se han vuelto más vulnerables a la desinformación, los fraudes y la ciberdelincuencia, debido asimismo a que Internet se ha convertido en la única opción para acceder a una serie de servicios tradicionalmente prestados fuera de línea.

2. El transnacionalismo es una nueva dinámica emergente

Otro aspecto que la pandemia ha dejado muy claro es que las fronteras son una construcción. También son porosas. La globalización, que en muchos aspectos depende de la manera en que la humanidad aborda la geografía, se ha presentado bajo una luz diferente, a través de un constante flujo internacional de información y servicios³⁵. A pesar de que las fronteras reales están cerradas, Internet permite que las comunicaciones y los datos entren y salgan. Nuestras experiencias compartidas durante este tiempo han reafirmado así una conclusión que puede parecer evidente: Internet ha convertido el transnacionalismo en una nueva dinámica emergente.

América Latina y el Caribe ha acogido el fenómeno de muchas maneras. La naturaleza sin fronteras de Internet ha creado un ambiente perfecto para que las ideas lleguen a un público más amplio. En lo que respecta a los negocios, los países de la región han servido como terreno de prueba para numerosas soluciones inventivas a los desafíos más diversos. Para las grandes multinacionales y las prometedoras empresas emergentes, la región sigue ofreciendo muchas oportunidades.

Sin embargo, la viabilidad de esas oportunidades depende a veces del marco regulatorio nacional y regional. Decidir cómo combinar la inspiración extranjera con la innovación regional es el primer paso para comprender la manera de abordar la política de Internet en América Latina y el Caribe.

3. Las empresas multinacionales extranjeras son influyentes en la región

Las empresas multinacionales de muchos países compiten por la atención de los ciudadanos de América Latina y el Caribe y forman parte de todos los estratos del mercado, desde infraestructura hasta sofisticados servicios de medios de comunicación. El aumento de la conectividad (que se examina con más detalle en la sección III.A) ha convertido a América Latina y el Caribe en uno de los mayores mercados del mundo. La conectividad móvil ha ido aumentando la disponibilidad de los servicios de Internet para una creciente mayoría de sus ciudadanos³⁶.

Las empresas con presencia mundial han participado tanto en el desarrollo del propio mercado como en la exploración de las oportunidades que ofrece América Latina y el Caribe. Sin embargo, esto ha traído consigo sus propios inconvenientes, pues los problemas transfronterizos se han vuelto más frecuentes. Mientras en el mercado físico una empresa necesitaría una presencia sólida en el terreno para suministrar bienes y servicios, las actividades en línea no necesariamente lo requieren. Algunos servicios pueden ofrecerse sin que el proveedor esté presente en la región. Es posible que las empresas extranjeras ni siquiera tengan representación legal y mucho menos una sede o una sociedad constituida legalmente en ninguno de los países de la región. Sin embargo, estas empresas pueden tener un efecto en los mercados o los consumidores de América Latina y el Caribe, que es más difícil de tratar.

³⁴ La Red de Políticas de Internet y Jurisdicción ha preparado tres Framing Briefs sobre el acceso a los datos de los usuarios, los problemas de moderación de contenidos y el abuso a nivel del Sistema de Nombres de Dominio (DNS) en el contexto de la pandemia de COVID-19, respectivamente. Véase [en línea] <https://www.internetjurisdiction.net/publications>.

³⁵ Véase J. Sachs, *The Ages of Globalization: Geography Technology and Institutions*, Nueva York, Columbia University Press, 2020.

³⁶ Véase Internet Live Stats, "Internet users by country (2016)" [en línea] <http://www.internetlivestats.com/internet-users-by-country/>.

Los consumidores, acostumbrados a hacer valer sus derechos en los tribunales de sus propios países, acaban por darse cuenta de que las dificultades pueden ser mucho mayores cuando hay un componente internacional en sus reclamaciones. La necesidad de asistencia judicial internacional aumenta porque es posible que participen los servicios diplomáticos y se destaqueen diferentes estándares en materia de protección y procedimientos jurídicos.

En el otro extremo del espectro, es posible que las empresas extranjeras no necesariamente sepan en qué países viven sus clientes o que no dispongan de los instrumentos necesarios para verificarlo (véase más información sobre las tecnologías de geolocalización en la sección V.B.1). Por consiguiente, el incumplimiento es una posibilidad con varias consecuencias prácticas.

Desde el punto de vista de la administración pública, si las empresas quieren participar en el mercado de la región, tendrán que cumplir sus leyes y estar disponibles para la adjudicación a nivel local. En general no se tienen en cuenta ni las expectativas de la empresa que presta los servicios de Internet ni la conveniencia (o no) del lugar de jurisdicción.

Además, las empresas multinacionales se enfrentan a menudo al predicamento de tener que cumplir con obligaciones legales contradictorias. El alcance extraterritorial o mundial de ciertas leyes nacionales, órdenes judiciales o solicitudes administrativas puede dar lugar a esos conflictos y las empresas se encuentran entonces en la posición de tener que seleccionar la obligación legal que van a cumplir³⁷.

En América Latina y el Caribe, este fenómeno se ha manifestado particularmente en materia de acceso a los datos almacenados en el extranjero. Las empresas multinacionales, en particular las que prestan o utilizan servicios en la nube, almacenan datos fuera del territorio en el que están prestando servicios, potencialmente sometiendo los datos a por lo menos dos jurisdicciones. Cuando el país donde se encuentran los datos tiene lo que se denomina un estatuto de bloqueo que solo permite el acceso a los datos en condiciones particulares, aumenta la posibilidad de conflicto con las leyes de la jurisdicción en la que se prestan los servicios (o se recogen los datos).

Esos enfrentamientos han dado lugar a instancias en que las empresas multinacionales se han negado a cumplir órdenes válidas emitidas con arreglo a las leyes internas de los países de América Latina y el Caribe. Ello ha dado lugar a la aplicación de recursos judiciales que van desde la imposición de grandes multas a las empresas matrices y contra los activos en el país hasta la presentación de cargos penales contra los empleados de las empresas multinacionales.

Las partes interesadas entrevistadas señalaron la armonización de las leyes, la coordinación de las iniciativas y la cooperación entre los Estados como una forma de hacer frente a estos retos. Las normas armonizadas conducen a resultados predecibles, que hacen que las empresas estén mejor preparadas para cumplir con las normas. Del mismo modo, mediante la coordinación y la cooperación, los Estados pueden lograr mejores resultados y fomentar un entorno de cumplimiento general.

4. El entorno comercial para las empresas emergentes en la región es variable

La otra cara de la moneda es que varias empresas de América Latina y el Caribe están aprovechando la oportunidad para expandirse a otros mercados tanto dentro como fuera de la región. Existe una combinación cada vez mayor de oportunidades emergentes para que tanto las empresas establecidas como las emergentes se beneficien de las características transnacionales de Internet. Un experto entrevistado también mencionó la existencia de puntos comunes inexplorados en la región que podrían permitir una rápida expansión de los mercados, como los rasgos culturales ibéricos comunes y el parentesco lingüístico.

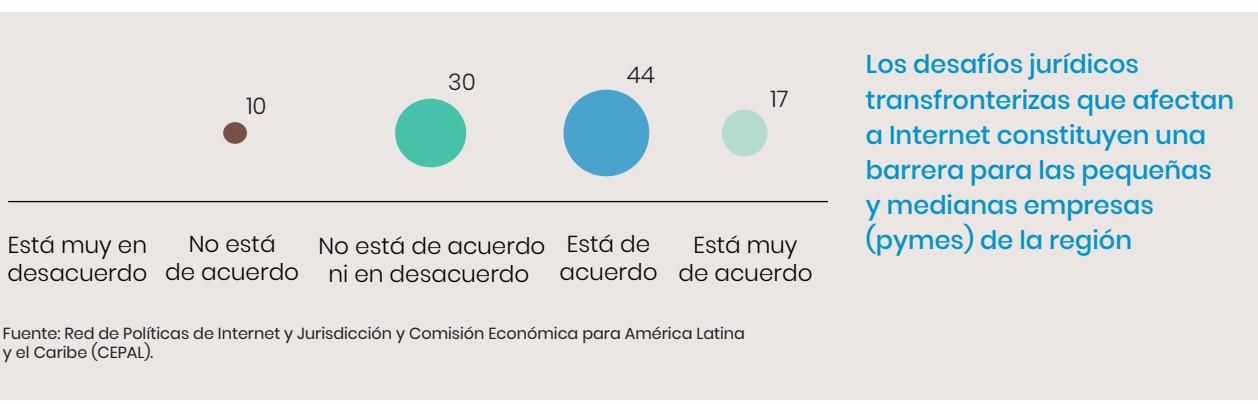
Así pues, existe una tendencia a que los productores regionales de bienes y servicios participen en la economía de plataformas, beneficiándose de los mercados internacionales (plataformas de comercio electrónico) que proporcionan acceso a los clientes en el extranjero. De esta manera, incluso las pequeñas y medianas empresas pueden convertirse en exportadoras y encontrar nuevos clientes fuera de sus mercados habituales³⁸.

³⁷ Véase D. J. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford University Press, 2017.

³⁸ Véase S. Lund y J. Manyika, *How Digital Trade is Transforming Globalisation*, El15 Initiative, Ginebra, Centro Internacional de Comercio y Desarrollo Sostenible/Foro Económico Mundial, 2016. Véanse datos más detallados en eBay "The State of Small Online Businesses: Worldwide Results from eBay's 5-Year Study" [en línea] <https://www.ebaymainstreet.com/facts-and-figures/state-small-online-businesses-worldwide-results-ebays-5-year-study>.

No solo se está expandiendo el entorno empresarial nacional en muchos países de la región, en particular en lo que respecta a las empresas emergentes tecnológicas, sino que también se están expandiendo varias empresas en toda la región e incluso a nivel internacional. Un experto observó que varias empresas emergentes financieras y proyectos posibilitados por la tecnología de cadenas de bloques se estaban ampliando rápidamente y tenían que hacer frente a las crecientes dificultades que ello conllevaba (véase más información sobre las tecnofinanzas en la sección IV.C.4).

Sin embargo, la mayoría de los expertos encuestados (60,97%) opinó que los desafíos jurídicos constituyan una barrera para las empresas de Internet transfronterizas, en particular las pequeñas y medianas empresas (pymes). Mencionaron que esas empresas regionales se enfrentaban ahora a varios retos al tratar de expandirse, entre ellos: i) reglamentos y normas diferentes, ii) ser objeto de una adjudicación inesperada, iii) obstáculos regulatorios, iv) incoherencia fiscal y v) cargas logísticas y administrativas.



Al examinar el nuevo papel que las empresas de la región están desempeñando y las oportunidades que tienen en línea, es importante señalar que los desafíos jurídicos transfronterizos pueden o no ser un obstáculo para la competencia. La región tiene una gran oportunidad para facilitar esta tendencia expansiva mediante una mayor cooperación e integración, que puede adoptar la forma de un mercado único digital (que se aborda con más detalle en la sección IV.C.1).

C. Las iniciativas regulatorias extranjeras inspiran propuestas regionales y nacionales

Si bien Internet no se diseñó teniendo en cuenta las fronteras de los países, la regulación de la red tiene repercusiones mucho más allá de las fronteras de un solo Estado. Este impacto transfronterizo puede surgir porque el ámbito de aplicación de las políticas nacionales a menudo abarca actividades que tienen lugar más allá de las fronteras territoriales. Las leyes de un país también pueden servir de modelo o fuente de inspiración para otros³⁹.

La abrumadora mayoría de los encuestados afirmó que los enfoques normativos extranjeros repercutieron en las iniciativas nacionales en América Latina. En cifras, el 80,5% de las partes interesadas indicó que las iniciativas de regulación nacionales se inspiraban “en gran medida” o “bastante” en las extranjeras, el 17% declaró que se inspiraban “en cierta medida” y solo el 2,5% expresó que se inspiraban “solo un poco”. Ninguno de los encuestados declaró que las iniciativas extranjeras no fueran una fuente de inspiración. En sus observaciones, los interesados señalaron que las iniciativas de los Estados Unidos y Europa eran las que más influían en la elaboración y aplicación de marcos jurídicos internos en los países de América Latina y el Caribe.

³⁹ Véase A. Bradford, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

¿En qué medida los enfoques regulatorios de otras regiones y países extranjeros como la Unión Europea o los Estados Unidos inspiran las iniciativas nacionales sobre gobernanza y regulación de Internet en América Latina y el Caribe?



Fuente: Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL).

En conjunto, las partes interesadas señalaron cinco razones para esta influencia: i) la afinidad social y cultural entre los Estados Unidos, Europa y América Latina y el Caribe y las similitudes entre sus sistemas jurídicos, que hacen que los responsables de la toma de decisiones estén más dispuestos a buscar inspiración en esas fuentes; ii) el carácter mundial de Internet, que crea presión para la armonización y aumenta la importancia de considerar enfoques fuera de la región; iii) las obligaciones contraídas en virtud de los tratados internacionales, que fomentan la consideración de soluciones globales; iv) la creencia de que los países fuera de la región tienen más experiencia con las tecnologías digitales y están más familiarizados con los problemas que estas pueden acarrear; y v) el hecho de que no todos los países tengan la capacidad técnica para implementar y aplicar esos reglamentos, lo que los hace receptivos a los mecanismos de cooperación técnica internacional a través de los cuales pueden funcionar las iniciativas y los enfoques internacionales, ayudando a su implementación. En consecuencia, la tendencia general es que las iniciativas de gobernanza y regulación de Internet nacionales de América Latina y el Caribe se inspiren en enfoques extranjeros.

Como mencionó una de las partes interesadas encuestadas: “Siempre hay modas y la necesidad de seguir las tendencias. Hoy en día existe una gran conciencia sobre temas como la ciberseguridad, los datos personales y la privacidad, por ejemplo. Sin embargo, no todo se copia siempre de otra legislación. Ha habido iniciativas bilaterales: México-Unión Europea, Argentina-Unión Europea. La Ley de Neutralidad de la Red chilena fue pionera. El Marco Civil de Internet del Brasil también fue pionero. De cualquier manera, el debate es global”.

1. Aumenta el apetito por regular el ciberespacio: proliferación de iniciativas

En la actualidad existe un consenso general sobre la necesidad de regular Internet en cierta medida. Sin embargo, hay menos consenso sobre las complejidades que la regulación puede conllevar. Como se señala en el *Internet & Jurisdiction Global Status Report 2019*, la pregunta no es tanto si se debe regular Internet, sino más bien cómo y quién debe hacerlo. A nivel mundial, se observa un aumento de las formas de regulación, que pueden incluir tratados internacionales, leyes internas, reglamentos administrativos, decisiones judiciales, códigos de conducta, directrices nacionales o internacionales, declaraciones, normas técnicas, convenciones, políticas empresariales y comunitarias y obligaciones contractuales. Estas iniciativas han creado un intrincado mosaico de marcos normativos. Si bien no todos ellos tienen valor jurídico, repercuten en el panorama de políticas.

Los países de América Latina y el Caribe tienen que lidiar con esta multitud de iniciativas, no todas de su propia creación. Entre las respuestas de los interesados se pueden distinguir tres fenómenos principales.

El primero se refiere a los problemas de cumplimiento que las empresas enfrentan al tratar de comprender el marco jurídico aplicable. Por lo tanto, la primera pregunta que hay que responder es: ¿cuál es la legislación nacional aplicable a un caso concreto?

El segundo es que los reglamentos pueden crear incertidumbre jurídica por el mero hecho de ser complejos y de múltiples niveles. Incluso después de determinar la legislación nacional aplicable, una pléthora de instrumentos jurídicos, como leyes, decretos, ordenanzas, decisiones judiciales y otras fuentes jurídicas, podría dificultar la navegación del marco jurídico del país.

El tercero se refiere a las consecuencias involuntarias que las medidas regulatorias pueden tener. Esas consecuencias podrían producirse porque la tarea de equilibrar diferentes normas y derechos no necesariamente tiene un resultado predeterminado. Este es el caso de las solicitudes de pruebas electrónicas a un proveedor de servicios en la nube, pues los datos pueden estar amparados por leyes diferentes según el lugar en que se almacenen. También puede ocurrir que una aplicación infrinja algunas normas nacionales y que los efectos de la sanción a la empresa responsable de la infracción se sientan mucho más allá de las fronteras de un país. El bloqueo de la aplicación de mensajería WhatsApp en el Brasil, que afectó a los usuarios de la Argentina y Chile, es un ejemplo de ello (el bloqueo de aplicaciones se examina más a fondo en la sección V.B.4).

La profusión de reglamentos puede resolver algunos problemas, pero es en sí misma fuente de otros. La mayoría de los interesados parece opinar que debería haber más coordinación y cooperación en torno a la formulación de políticas de Internet en América Latina y el Caribe y que algunos temas están más regulados que otros.

2. **Inspiración legislativa y judicial: ¿intercambio de ideas o mera imitación?**

La abundancia de iniciativas de regulación nacionales puede ocultar la medida en que la legislación y las decisiones judiciales extranjeras suscitan debates nacionales y regionales en América Latina y el Caribe. Las iniciativas nacionales pueden imitar o directamente copiar enfoques y fundamentos elaborados en el extranjero. El examen de la literatura y las contribuciones de los interesados encuestados sugieren que la línea entre el intercambio de ideas y la imitación es muy sutil.

Esta tendencia general a la imitación se evidencia en muchos casos en diferentes esferas de la regulación de Internet en las que una iniciativa externa ha dado lugar a iniciativas nacionales o regionales.

- Este ha sido el caso de la discusión sobre la neutralidad de la red en los Estados Unidos, pues el enfoque de la Comisión Federal de Comunicaciones (FCC) proporcionó la base para el debate sobre el tema en toda América Latina y el Caribe⁴⁰.
- La sentencia del Tribunal de Justicia de la Unión Europea en el caso Costeja, que afirma el “derecho al olvido”, ha dividido a los expertos, los países y los tribunales de América Latina y el Caribe (véanse más comentarios sobre este tema en la sección IV.A.5).
- La aprobación y posterior entrada en vigor del Reglamento General de Protección de Datos de la Unión Europea ha llevado a muchos países a adoptar nuevas leyes o a reformar su régimen de protección de datos. Desde 2016 (año en que el reglamento entró en vigor) se han aprobado no menos de cuatro leyes de protección de datos, y países como la Argentina, Chile, Colombia y el Uruguay han iniciado la revisión de sus leyes en materia de protección de datos o las han reformado. Algunos países también han decidido introducir una nueva legislación general de protección de datos, entre ellos Barbados, El Salvador y Jamaica, por citar solo algunos.

La reciente aprobación de la nueva Directiva sobre los derechos de autor y derechos afines en el mercado único digital de la Unión Europea estimuló el debate sobre los regímenes de responsabilidad de las plataformas por violaciones de los derechos de autor por parte de terceros (véase la sección IV.C.2), con repercusiones que ya se están sintiendo en América Latina y el Caribe.

Esta influencia tiene consecuencias positivas y negativas en la región. Por una parte, los interesados señalaron que sirven como instrumento de armonización: al hacer que las iniciativas en los países sean similares a las de otros lugares, tienen un efecto de coordinación. Es interesante que las iniciativas de los países de América Latina y el Caribe puedan estar influyendo también en otras dentro de la región, aumentando la consonancia entre los distintos países.

No obstante, los interesados expresaron su preocupación por el hecho de que, en algunas circunstancias, las soluciones extranjeras no eran apropiadas para el contexto social, económico y cultural de la región. Uno de ellos mencionó que aunque las soluciones fueran sólidas, puede que no se apliquen a un nivel óptimo. Las instituciones encargadas pueden carecer de los recursos o la autoridad necesarios para alcanzar los objetivos de política para los que fueron diseñadas.

Una consideración final es que si el fundamento de la iniciativa extranjera es polémico o invasivo, su adopción en la región puede tener un efecto similar, lo que podría dar lugar a un conflicto.

⁴⁰ Véase O. Castro, S. Pereira da Silva y P. Viollier (coords.), *Neutralidad de red en América Latina: reglamentación, aplicación de la ley y perspectivas. Los casos de Chile, Colombia, Brasil y México, Santiago, Derechos Digitales/Intervozes, 2017 [en línea]* <https://www.derechosdigitales.org/wp-content/uploads/neutralidad-de-la-red.pdf>.

D. Preocupación por la influencia internacional y la pluralidad normativa

En muchas esferas del derecho, la legislación nacional sigue siendo la principal forma de regulación. Sin embargo, en el caso de Internet, difícilmente se puede decir que sea el único elemento que regula y orienta la conducta en línea. Otros factores, como los acuerdos internacionales, las iniciativas reguladoras extranjeras (con y sin efectos extraterritoriales), las normas técnicas y específicas de la industria, las directrices nacionales e internacionales, las condiciones de uso y servicio de las empresas, las directrices de la comunidad y las decisiones sobre arquitectura (código) también pesan significativamente en el entorno en línea.

El ciberespacio como red está influenciado y afectado por sus múltiples elementos. La circulación rápida (“viralidad”) no es solo una característica asociada a los videos, las imágenes y las piezas de información. Una pluralidad de iniciativas normativas puede causar un efecto mariposa de regulación en Internet, repercutiendo en la conducta en línea a lo largo y ancho.

Como se menciona en el *Internet & Jurisdiction Global Status Report 2019*, un modelo regulatorio piramidal con reglas estrictas emanadas del Estado no puede dar cuenta de la profusión de iniciativas normativas y su impacto relativo⁴¹. En América Latina y el Caribe, los países se sienten atraídos por las iniciativas extranjeras y, al mismo tiempo, se muestran escépticos ante ellas. Lo que no se puede negar es que una pluralidad de iniciativas, no solo de los Estados o de la propia región, influye en la conducta en línea y la rige.

1. Las normas se establecen para (y por) los grandes agentes internacionales establecidos

Los interesados entrevistados y encuestados señalaron que no todas las iniciativas tenían el mismo impacto y no todos los agentes tenían la misma posición en el proceso de toma de decisiones. Destacaron que, a menudo, los Estados y las empresas más grandes tenían más voz e influencia que los más pequeños en el establecimiento de reglas para Internet.

Las iniciativas normativas parecen sufrir una fuerza de atracción gravitatoria hacia los actores más grandes. Cuanto más grande es el agente, más se moldean las reglas a sus ambiciones. Las normas parecen haberse diseñado para satisfacer los intereses de las naciones y las empresas más grandes y se adaptan menos a las circunstancias de las pymes o de las empresas de los países más pequeños o menos desarrollados.

La mayoría de los interesados considera que esta tendencia es un obstáculo para que las pymes y las empresas de los Estados más pequeños puedan competir a nivel internacional. Algunos entrevistados mencionaron que la mayoría de las naciones y las empresas más pequeñas no tenían los recursos ni el capital humano necesarios para cumplir con complejos conjuntos de normas⁴².

Con respecto a las transacciones transfronterizas y las iniciativas internacionales, a pesar de algunos éxitos recientes, las empresas de la región todavía se ven considerablemente afectadas por la falta de armonización y coordinación de las gestiones. Las empresas de América Latina y el Caribe que actúan a nivel transnacional suelen ser financiadas por capital de riesgo extranjero o adquiridas por empresas extranjeras más capitalizadas.

Esta situación se refleja en la encuesta, en la que la mayoría de los interesados opina que los desafíos jurídicos transfronterizos que afectan Internet constituyen un obstáculo para las pymes de la región.

2. El papel cada vez mayor de las normas de la empresa: el estatus “constitucional” de las condiciones de servicio

Las empresas, en particular las plataformas, establecen sus propias reglas para regular el comportamiento en línea. Se reconoce ampliamente que la elección de la arquitectura (código) afecta y regula la conducta de los agentes en línea y puede influir en las posibilidades de la actividad en línea. Sin un botón para decir “Me gusta”, los usuarios no pueden expresar su satisfacción o falta de ella ante algún comentario, foto o video en línea⁴³. La posibilidad de reenviar un mensaje solo a 1 persona en

⁴¹ Véase F. Ost y M. van de Kerchove, “De la pyramide au réseau? Pour une théorie dialectique du droit”, Pyramides, N° 94, Bruselas, Universidad de Saint-Louis en Bruselas, 2002.

⁴² Véase S. Hubbard, “Fake news is a real antitrust problem”, CPI Antitrust Chronicle, Boston, Competition Policy International (CPI), 2017.

⁴³ Véase, por ejemplo, SPIEGEL International, “Like’ button battle: Facebook agrees to voluntary privacy code”, 8 de septiembre de 2011 [en línea] <https://www.spiegel.de/international/germany/like-button-battle-facebook-agrees-to-voluntary-privacy-code-a-785190.html>.

lugar de a 5 o 20 es un desincentivo a la difusión de información (y desinformación)⁴⁴. Estos son solo dos ejemplos de la manera en que el código puede incidir en la conducta en línea.

Sin embargo, el código es solo una de las dimensiones en las que las plataformas influyen en el comportamiento. Las condiciones de servicio y las directrices de la comunidad proporcionan una base normativa para que los proveedores de servicios de Internet actúen como reguladores y vigilen el ciberespacio. Según la plataforma de que se trate, pueden ser lo suficientemente sofisticadas para crear instituciones similares a las de un Estado⁴⁵. Recientemente, Facebook instituyó un órgano cuasijudicial paralelo denominado Junta de Supervisión que funcionará como un órgano de apelación para sus decisiones de moderación de contenido⁴⁶. Las plataformas de comercio electrónico tienen mecanismos de solución de controversias, que se extienden a la protección del derecho de autor⁴⁷. Reddit permite que las comunidades elaboren su propio conjunto de normas y les aconseja que tengan moderadores activos y procedimientos de apelación⁴⁸. La lista de plataformas y medidas que se asemejan a las de instituciones del Estado es cada vez mayor.

Las iniciativas mencionadas se han traducido en condiciones de servicio que parecen constituciones. A pesar de ser normas de la empresa, parecen ser el primer recurso. Si la conducta en línea se considera ofensiva o perjudicial, se prevén medidas de las plataformas, que se basan principalmente en sus condiciones de servicio. Al mismo tiempo, las plataformas afirman cada vez más los derechos de los usuarios, de una manera casi “constitucional”.

Estas tendencias tienen una serie de consecuencias generales. La primera (que se analiza más adelante en la sección IV.A.) es que las plataformas están llamadas a ser más responsables por lo que ocurre dentro de sus dominios. La segunda es que pueden actuar a través de las jurisdicciones, pues las normas de conducta no están limitadas por las fronteras de los Estados y una empresa puede cambiar las condiciones de todas sus plataformas en todos los países o en algunos de ellos. La tercera es que las empresas pueden acordar entre ellas normas comunes particulares y aplicarlas de manera coordinada, sin necesidad de la coordinación estatal⁴⁹.

Hay otro conjunto de implicaciones: las normas de las empresas carecen de un proceso de aprobación pública o democrática y pueden entrar en conflicto con la normativa nacional. En América Latina y el Caribe ha habido más de un conflicto de este tipo. El caso que ha llamado la atención internacional ha sido el de las “órdenes de permanencia”, decisiones judiciales que requieren que las plataformas mantengan contenido en línea, incluso aunque supuestamente viola las condiciones de servicio⁵⁰.

Un aspecto positivo es que estas normas de las empresas pueden facilitar la armonización de las normas transfronterizas. Su aplicación transnacional conduce a un debate internacional y puede dar lugar a una respuesta coordinada o armonizada. Sin embargo, los interesados encuestados señalaron la falta de transparencia y claridad en el establecimiento de esos términos. En las observaciones, un interesado señaló que tal vez el ADN mundial de esas condiciones de servicio –establecidas sobre todo por plataformas multinacionales– no esté bien preparado ni sea lo suficientemente flexible para abarcar la diversidad y las idiosincrasias presentes en las realidades locales, en particular en las naciones más pequeñas y en desarrollo como las de América Latina y el Caribe. Se podría decir que existe el riesgo de que las “constituciones” de las plataformas mundiales no sean lo suficientemente inclusivas para las realidades locales de los países más pequeños.

⁴⁴ Esta es una referencia a los cambios que la aplicación de mensajería WhatsApp ha hecho en su arquitectura para limitar la posibilidad de reenviar mensajes que ya han sido reenviados muchas veces. Véase A. Hern, “WhatsApp to impose new limit on forwarding to fight fake news”, The Guardian, Londres, 2020 [en línea] <https://www.theguardian.com/technology/2020/apr/07/whatsapp-to-impose-new-limit-on-forwarding-to-fight-fake-news>.

⁴⁵ Véase A. Chander, “Facebookistan”, North California Law Review, vol. 90, 2012. Véase también R. MacKinnon, “Facebookistan and Googledom”, Consent of the Networked: The Worldwide Struggle for Internet Freedom, Basic Books, 2012.

⁴⁶ Véase N. Clegg, “Welcoming the Oversight Board”, Menlo Park, Facebook, 2020 [en línea] <https://about.fb.com/news/2020/05/welcoming-the-oversight-board/>.

⁴⁷ Véase Mercado Libre, “Defiende tu propiedad intelectual en Mercado Libre” [en línea] <https://www.mercadolibre.com.ar/brandprotection/enforcement>.

⁴⁸ Véase Reddit, “Moderator guidelines for healthy communities”, 2017 [en línea] <https://www.redditinc.com/policies/moderatorguidelines-for-healthy-communities>.

⁴⁹ Esto se ha hecho recientemente mediante una declaración conjunta contra la difusión de información errónea con respecto a la pandemia de COVID-19. Véase C. Shu y J. Shieber, “Facebook, Reddit, Google, LinkedIn, Microsoft, Twitter and YouTube issue joint statement on misinformation”, San Francisco, TechCrunch, 2020 [en línea] <https://techcrunch.com/2020/03/16/facebookreddit-google-linkedin-microsoft-twitter-and-youtube-issue-joint-statement-on-misinformation/>.

⁵⁰ Véase HackRead, “Brazil will sue Facebook for blocking picture of indigenous woman”, 2015 [en línea] <https://www.hackread.com/facebook-blocking-brazil-indigenous-picture/>. Véase un análisis de las decisiones de permanencia en D. Keller, “Dolphins in the net: Internet content filters and the Advocate General’s Glawischnig-Piesczek v. Facebook Ireland opinion”, Stanford, Stanford Center for Internet and Society, 2019 [en línea] <https://cyberlaw.stanford.edu/files/Dolphins-in-the-Net-AG-Analysis.pdf>.

E. El papel de la territorialidad y el ejercicio de la soberanía en una red mundial

El concepto de territorialidad ha sido difícil de conciliar con algunas de las características del ciberespacio. Se supone que la territorialidad cumple la función de un principio rector tanto para proporcionar las bases para que un Estado ejerza el poder como para definir la extensión geográfica de este poder, estableciendo un límite topográfico a la soberanía del Estado.

Por otra parte, Internet se desarrolló para no tener fronteras o al menos ser neutral en ese sentido, de manera que la información pueda fluir a pesar de las barreras geográficas. Por lo tanto, la jurisdicción territorial pierde su significado preciso en un ciberespacio que supuestamente no debería reflejar las divisiones estatales políticas subyacentes del mundo físico. Sin embargo, los países no pueden ignorar que ciertas acciones en línea afectan tanto a los bienes como a las personas que se encuentran en el mundo físico y dentro de sus propios confines. La creciente interconexión de los mundos físico y virtual ha desdibujado la línea entre ambos, lo que conduce a regulaciones estatales más extensas desde el punto de vista geográfico.

Los Estados han tratado de utilizar la ubicación de personas, dispositivos o servidores como puntos de anclaje territorial para justificar el ejercicio de la jurisdicción en línea. En cierta medida, se determina la jurisdicción respecto de los actos que pueden estar jurídicamente vinculados a más de un territorio y potencialmente a más de una jurisdicción. La consecuencia es que en algunos casos los Estados se han “excedido”, atribuyendo jurisdicción cuando solo hay una conexión tenue, o “no han alcanzado”, lo que significa que algunas víctimas se quedan sin recurso.

América Latina y el Caribe tiene una relación única con el concepto jurídico de territorialidad, pues se considera que la región es la cuna del principio de no intervención en los asuntos internos de otros Estados⁵¹. No es casualidad que la definición más famosa de “Estado” provenga de una convención redactada en la región, la Convención sobre Derechos y Deberes de los Estados de 1933. En esta se define el territorio como uno de sus elementos constitutivos⁵². Este contexto tiene consecuencias para la comprensión de determinados tipos de materias como pertenecientes a la jurisdicción interna de un Estado. Es en este contexto que los Estados de la región conceptualizan la jurisdicción territorial, incluida la jurisdicción en línea.

El hecho de que América Latina y el Caribe sea la cuna del principio de no intervención influye en la comprensión de la jurisdicción en esa región. Este enfoque queda ilustrado por el trato que se da a las empresas extranjeras que parecen no seguir las leyes nacionales. La escalada para bloquear las aplicaciones o detener a los ejecutivos de las empresas parece ser una consecuencia de esta noción: dentro de su territorio, la ley de un Estado tiene que ser respetada. Del mismo modo, con las pruebas electrónicas, parece que los organismos nacionales encargados de hacer cumplir la ley se desconciertan cuando no tienen acceso a los datos sobre delitos cometidos dentro de sus fronteras.

En algunas circunstancias, la justificación de la jurisdicción es tanto dependiente como independiente del territorio. Existe un deseo de regular lo que ocurre en el territorio de América Latina y el Caribe o tiene incidencia en este pero, a partir de entonces, la jurisdicción puede extenderse más allá de la región, como por ejemplo, en el caso de la aplicación extraterritorial de las normas de protección de datos y las condiciones para las transferencias transfronterizas de datos personales. En los casos de difamación y moderación de contenidos, las órdenes de retirada a menudo se centran en la eliminación de contenidos o incluso en el cierre de cuentas, con un alcance global y no solo local.

Existe una tendencia general a que la jurisdicción se centre en la localización del comportamiento o la conducta más que en el lugar donde se almacenan los datos. Sin embargo, la ubicación y el movimiento de los datos siguen siendo a veces factores relevantes que deben tenerse en cuenta.

1. El alcance extraterritorial cada vez mayor de las leyes nacionales

Los Estados están cada vez más molestos por la manera en que la fluidez del entorno en línea, en el que no hay barreras claras a la interacción transfronteriza, se aprovecha para eludir la legislación nacional. De manera comprensible, quieren que la regulación desaliente dicho comportamiento. La razón es que las leyes deben respetarse tanto en línea como en el mundo fuera de línea. Cada Estado considera que tiene derecho

⁵¹ Véase un panorama general del desarrollo del principio en A. Tillman y J. Scarfi, *Cooperation and Hegemony in US-Latin American Relations: Revisiting the Western Hemisphere Idea*, Londres, Palgrave Macmillan, 2016. Véase una de las primeras declaraciones del principio en A. Alvarez, “Latin America and International Law”, *American Journal of International Law*, vol. 3, N° 2, Cambridge, Cambridge University Press, 1909.

⁵² Véase [en línea] <http://www.oas.org/juridico/spanish/tratados/a-40.html>.

a gobernar lo que sucede y lo que está disponible en línea. Existe la percepción de que si un comportamiento incide o tiene un efecto en el territorio de un Estado, debe estar comprendido en su jurisdicción.

A falta de instrumentos regionales o internacionales vinculantes, muchos Estados, incluidos Estados de la región, terminan por reivindicar una jurisdicción amplia, ya sea mediante nuevas leyes o mediante una interpretación extensiva de las existentes. En América Latina y el Caribe, esta tendencia general es particularmente evidente en las esferas de la protección de datos (véase la sección II.C.6) y el acceso a las pruebas electrónicas por parte de los organismos encargados de hacer cumplir la ley (véase la sección II.B.2).

A juicio de los interesados encuestados, este enfoque de la regulación (que aumenta el alcance geográfico de las leyes nacionales) puede dar lugar a una aplicación arbitraria o a la frustración. Esta última surge porque la aplicación efectiva puede ser difícil o casi imposible en algunos casos. En cuanto a la primera, las personas pueden sorprenderse de que se las procese en un país lejano por violar una ley local sin saberlo o sin darse cuenta de ello. Otro aspecto es que el alcance de la regulación puede ser tan amplio que puede resultar difícil determinar las conductas que se incluirán, en cuyo caso la aplicación puede parecer discrecional.

Una tendencia mundial paralela recogida por los países de América Latina y el Caribe es la de promulgar normas con multas excesivas en caso de incumplimiento. Las amenazas de sanciones se utilizan para fomentar el cumplimiento. La preocupación de los Estados de América Latina y el Caribe es que, con sanciones menos prohibitivas, sus leyes pasarán a un segundo plano y podrán ser ignoradas por los actores internacionales. La dificultad de este razonamiento parece ser que motiva a otros países a hacer lo mismo y a competir por imponer las multas más altas y las sanciones más duras, impidiendo la circulación de datos y negocios.

2. La extraterritorialidad plantea desafíos de ejecución

Las demandas de jurisdicción amplia pueden ser difíciles de hacer cumplir, y cuanto más amplias sean, más difícil puede ser su aplicación. Reivindicar la jurisdicción no es lo mismo que hacerla cumplir. Un Estado que aplica sus leyes basándose en un vínculo débil entre la conducta y el propio Estado puede tener dificultades para que sus acciones se consideren legítimas. Del mismo modo, afirmar la jurisdicción, sin tener la capacidad de hacerla cumplir, puede ser perjudicial para la percepción de la eficacia de la reglamentación e ir en contra del objetivo de fomentar el cumplimiento.

Sin embargo, presentar reivindicaciones de jurisdicción amplias puede ser una estrategia en sí misma. Deja claro que un asunto específico afecta un valor social importante, es decir, que el Estado se preocupa por ese tema. Esta estrategia puede ser una forma de trazar líneas jurisdiccionales y de articular un punto de vista sobre el alcance de los intereses de un Estado.

Un Estado también puede ver la necesidad de confiar en la cooperación con otro. Los activos reales y los datos pueden estar en otro país y, por lo tanto, fuera del alcance del país ejecutor o no estar de manera realista a su alcance. Esto crea el potencial de conflictos regulatorios, que constituyen tanto un reto para la cooperación interestatal como una oportunidad para encontrar soluciones aceptables para todos.

Esto se refuerza por el hecho de que una vez que se afirma la jurisdicción, el país tiene que estar dispuesto a que sea recíproca, pues otros Estados pueden reivindicar una jurisdicción igualmente amplia. América Latina y el Caribe tiene una tradición de reciprocidad internacional. Por lo tanto, es probable que las afirmaciones de jurisdicción extranjeras se correspondan con las de los países de la región.

Varios interesados señalaron que no todos los países de América Latina y el Caribe tenían la misma capacidad para extender su jurisdicción más allá de sus fronteras. Indicaron las diferencias de tamaño, peso económico y poder entre los países de la región y destacaron los posibles obstáculos a las iniciativas para igualar la acción exterior. Por consiguiente, la afirmación de una jurisdicción extraterritorial o amplia por parte de un país de América Latina o el Caribe podría resultar deficiente en lo que respecta a la aplicación de la ley.

Esto también funciona al revés. Algunas de las partes interesadas encuestadas mencionaron que las naciones más pequeñas podrían ser impotentes cuando las naciones más grandes desplegaran su poder legal. El caso de los juegos de azar en línea presentado por Antigua y Barbuda ante la Organización Mundial del Comercio (OMC) constituye un ejemplo ilustrativo⁵³. Aunque la controversia fue decidida en última instancia por el Órgano de Apelación a favor de los Estados Unidos, habría sido un reto para la nación caribeña hacer valer sus derechos y salvaguardar sus negocios contra una ley norteamericana

⁵³ Véase [en línea] https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm.

con efecto transfronterizo⁵⁴. En realidad, aunque fuera legal desde el punto de vista de la OMC, el resultado terminó siendo una medida de destrucción del mercado y el servicio ya no pudo continuar⁵⁵.

F. Nuevas funciones para los intermediarios

Los intermediarios son muy diversos: motores de búsqueda, redes de medios sociales, plataformas de comercio electrónico o de emisión en directo, mecanismos de pago digital y muchos otros agentes que facilitan las actividades más conocidas en línea. A medida que Internet alcanzó una difusión masiva, los intermediarios cobraron importancia, integrándose en la rutina de los usuarios de Internet. Se han convertido en los conductos que conectan a diferentes personas y empresas y facilitan las transacciones. El resultado ha sido un cambio en la morfología del ciberespacio, que pasó de ser un territorio salvaje en gran parte autogestionado, a una multiplicidad de jardines organizados y más o menos amurallados.

El grado de dependencia de los intermediarios de Internet es objeto de disputa. Sin embargo, es evidente que representan una parte importante del tráfico y, desde un punto de vista centrado en el usuario, simplifican el uso de Internet. Con esta nueva centralidad, ha surgido un debate sobre las funciones de estos agentes y su responsabilidad por lo que sucede en el ciberespacio. Se considera que los intermediarios deberían compartir más la carga de supervisar lo que sucede en línea.

1. Aumento de la responsabilidad de los operadores privados

Tradicionalmente, los países han considerado que los intermediarios de Internet merecen protección jurídica debido a su importante función como encrucijadas, puertas de acceso o lugares de encuentro de los usuarios de Internet. Sin embargo, una serie de situaciones relacionadas con la pornografía infantil, la violencia explícita, el terrorismo, la divulgación de imágenes íntimas (“pornografía de venganza” o “pornovenganza”), las campañas de desinformación (“noticias falsas”), las infracciones de derechos de autor a gran escala, entre otras, han puesto de manifiesto los defectos de este enfoque si se adopta sin precauciones⁵⁶.

Los países de América Latina y el Caribe han ido avanzando en la asignación a los operadores privados de un papel más importante en la gobernanza de Internet. El tema ha cobrado mayor importancia para los países de la región, en particular en los ámbitos de los discursos de odio y daños, la desinformación (principalmente en el contexto de las elecciones), las infracciones de los derechos de autor, la venta de mercancía falsificada y la protección de la privacidad y los datos.

Los intermediarios terminan desempeñando funciones cuasiestatales, por ejemplo, en su papel cuasijudicial de decidir cuándo retirar contenidos y suspender o cerrar las cuentas de infractores reincidentes de derechos de autor. Son ellos los llamados a decidir sobre la legalidad del contenido y, por ejemplo, determinar si se trata de sátira política (permitida) o discurso difamatorio (no permitido). Pueden adoptar esas medidas voluntariamente de conformidad con sus condiciones de servicio o por mandato de la reglamentación nacional y las decisiones de los tribunales.

Los regímenes jurídicos que hasta hace poco protegían a los intermediarios contra el enjuiciamiento han dado lugar a enfoques más matizados⁵⁷. En América Latina y el Caribe, las estrategias han variado de un país a otro. La República Bolivariana de Venezuela y Cuba parecen estar entre los más estrictos, pues han promulgado leyes que imponen a los proveedores de servicios de Internet la obligación de vigilar y “regular” los contenidos. También otorgan amplias facultades a los organismos públicos, que pueden incluso determinar el cierre de los intermediarios que no respetan su autoridad⁵⁸. En otros países se ha tratado de regular aspectos específicos como el discurso de odio, responsabilizando a los intermediarios si no eliminan los contenidos considerados ilegales. Otros enfoques han consistido en la publicación de códigos de conducta o la celebración de acuerdos administrativos con los intermediarios.

⁵⁴ Véase A. Chander, “Freeing trade in cyberspace”, *The Electronic Silk Road: How the Web Binds the World Together in Commerce*, Yale University Press, 2013.

⁵⁵ Véase D. Svantesson, *Private International Law and the Internet*, third edition, Alphen aan den Rijn, Wolters Kluwer, 2016.

⁵⁶ Véase G. Frois (ed.), *Oxford Handbook of Online Intermediary Liability*, Oxford University Press, 2020.

⁵⁷ Por ejemplo, el Marco Civil de Internet (Ley núm. 12965 de 2014) del Brasil consagra una cláusula de limitación de responsabilidad o disposición de salvaguardia (*safe harbour*). En Chile, la Ley núm. 20.435 de 2010 reformó la legislación de derechos de autor para establecer una cláusula de limitación de la responsabilidad civil por daños a terceros en lo que se refiere a los derechos de autor en Internet.

⁵⁸ Véanse Asamblea Nacional de la República Bolivariana de Venezuela, Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos, Caracas, 2010 [en línea] <http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-ResponsabilidadSocial-en-Radio-Televisión-y-Medios-Electrónicos.pdf>; Comisión Interamericana de Derechos Humanos (CIDH), Informe Especial sobre la Situación de la Libertad de Expresión en Cuba, Washington, D.C., 2018.

Algunas de las partes interesadas encuestadas destacaron que esta tendencia podría tener repercusiones transfronterizas. Estas son particularmente graves en los casos en que las empresas no tienen más opción que cumplir la reglamentación de un Estado (incluidas las órdenes judiciales), a riesgo de violar el régimen jurídico de otro si hay un conflicto de leyes. Las consecuencias podrían no ser fáciles de prever, especialmente para un país latinoamericano o caribeño. Las empresas pueden aplicar el enfoque del “común denominador más estricto”, que puede limitar la libertad de expresión en la región o, cuando se las presiona, pueden optar por no aplicar las leyes locales, lo que puede repercutir en la legitimidad jurídica nacional.

Los interesados señalaron que exigir a las plataformas que desempeñen la función de guardianes de Internet podría socavar la legitimidad de las instituciones del Estado, la confianza en ellas y el sentido de la justicia, mientras en situaciones electorales podría afectar el proceso democrático. Significa que las empresas quedan a cargo de establecer qué información puede circular y cómo. Sin embargo, la desinformación también puede tener un efecto perjudicial en las elecciones democráticas.

2. Se pide cada vez más a los intermediarios que proporcionen datos para apoyar investigaciones

Cuando los teléfonos se convirtieron en un importante medio de comunicación, las escuchas telefónicas se convirtieron en un valioso recurso de investigación para los agentes encargados de hacer cumplir la ley, al darles acceso a las comunicaciones reales de los presuntos delincuentes y proporcionarles una forma de saber cómo se planificaban los delitos, cuándo iban a ocurrir o cómo se habían discutido. Incluso la intención dolosa (*mens rea*) podía establecerse mejor escuchando conversaciones que habrían sido privadas si no fuera por las pistas que las conectaban con las investigaciones de delitos.

Internet ha cambiado la situación. Un sinnúmero de servicios diferentes realizan la misma función, permitiendo que se comparta información sobre conductas ilegales, ya sea en línea o fuera de línea. Las técnicas de la era telefónica no se trasladan completamente a Internet. El apoyo a las funciones de investigación ha pasado de los intermediarios que proporcionan la infraestructura a aquellos que proporcionan directamente algunas aplicaciones de Internet muy populares. Estos intermediarios de Internet son los que pueden proporcionar acceso a la información. Esto plantea al menos cuatro cuestiones principales: el acceso a los datos almacenados; el acceso a datos a granel (datos generales o tesoros de datos); el uso de la criptografía; y las categorías de servicios de datos que las empresas podrían estar obligadas a recopilar y proporcionar.

Dado que muchos intermediarios están ampliando su alcance a nivel mundial, todos esos temas suelen tener un componente transfronterizo. Diferentes normas nacionales establecen cuándo y cómo se puede dar acceso a los datos a los funcionarios encargados de hacer cumplir la ley. Si los datos están almacenados en el extranjero, los desafíos tienden a ser aún mayores. A fin de evitar las complejidades de la asistencia judicial internacional, los países de la región están estudiando la idea de imponer obligaciones a los intermediarios de Internet. Entre ellas figuran: i) la localización de los datos; ii) la presencia física en el país o el nombramiento de un representante; y iii) la obligación de proporcionar acceso a los datos, a distancia o de otro modo. Por ejemplo, los dos últimos puntos son objeto del artículo 32 del proyecto de ley de noticias falsas aprobado por el Senado brasileño⁵⁹.

También se está pidiendo a los intermediarios que den acceso no solo a datos específicos, sino a grandes volúmenes de datos. A menudo, se les pide que pongan a disposición todo un pajar en la búsqueda de una aguja mal definida. Por ejemplo, este tipo de solicitudes se ha realizado, sin éxito, en relación con los datos de localización de torres de telefonía móvil en los Estados Unidos⁶⁰. Sin embargo, en América Latina y el Caribe ha habido casos en que los tribunales superiores han accedido a solicitudes tan amplias, aunque no sea esta la respuesta habitual⁶¹. La pandemia de COVID-19 ha

⁵⁹ El proyecto de ley también contenía una obligación de localización de datos, pero esta fue eliminada antes de la votación en el Senado. Véase [en línea] <https://www.bloomberg.com/news/articles/2020-07-01/brazil-s-senate-approves-draft-bill-to-rein-in-on-fake-news>. Véanse el texto original del proyecto de ley (en portugués) y su discusión [en línea] <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944> y <https://legis.senado.leg.br/saleg-getter/documento?dm=8128670&ts=1600365729707&disposition=inline>. Véase un análisis del impacto del art. 32 en C. A. Souza y C. Perrone, “Fake news e acesso a dados armazenados no exterior”, JOTA, 2020 [en línea] <https://www.jota.info/coberturas-especiais/liberdade-de-expressao/fake-news-e-acesso-a-dados-armazenados-no-exterior-30062020>.

⁶⁰ Véase Corte Suprema de los Estados Unidos, “Carpenter v. United States” [en línea] <https://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/>.

⁶¹ Véase [en línea] <https://www.telesurenglish.net/news/Google-Must-Share-Data-Related-To-Marielle-Franco-Murder-Case-20200827-0004.html>.

ampliado el alcance de esas solicitudes del ámbito de las investigaciones de delitos a la aplicación de la política pública (por lo menos durante la pandemia)⁶².

Las obligaciones impuestas a los intermediarios para apoyar investigaciones han creado otro difícil dilema. Varios intermediarios han utilizado o se proponen utilizar técnicas de preservación de la privacidad que entrañan diferentes tipos de criptografía, incluida la criptografía de extremo a extremo. En consecuencia, podría resultar más difícil (o a veces incluso técnicamente imposible) cumplir esa función, pues la información puede no ser accesible.

En estas circunstancias, los países de América Latina y el Caribe, al igual que muchos de sus homólogos internacionales, tratan de obligar a los intermediarios a no utilizar técnicas criptográficas o a proporcionar una clave. Incluso están encontrando otras formas de acceder a la información, como el uso de un tercero no identificado. Esto es similar a lo que sucedería en una situación de escuchas telefónicas, pero con consecuencias potencialmente mucho más amplias, ya que todas las conversaciones podrían ser escuchadas (no solo conversaciones específicas) y esto podría ser realizado por cualquier persona capaz de acceder a ellas y no solo por los agentes encargados de hacer cumplir la ley.

Otra estrategia propuesta en la región ha sido que los servicios de mensajería recojan más información para que esta sea accesible para futuras investigaciones. Se han planteado dos formatos: o bien solicitar la identificación de las personas, restringiendo así el anonimato en línea, o bien exigir a los intermediarios que rastreen determinadas categorías de mensajes, en particular los de contenido ampliamente difundido⁶³.

Todas esas nuevas funciones requieren mecanismos sustanciales para equilibrar los derechos y pueden tener un efecto importante en las acciones de los intermediarios de Internet, en particular cuando prestan servicios a nivel mundial. Los expertos entrevistados señalaron la necesidad de armonizar las legítimas necesidades de aplicación de la ley con la organización de Internet, los derechos de los usuarios y el alcance mundial de los proveedores de servicios de Internet.

3. La transparencia es esencial para aumentar la confianza, pero la implementación varía

Las mayores funciones asignadas a los intermediarios de Internet también han aumentado la exigencia de mayor transparencia respecto de sus procedimientos, decisiones y acciones. La necesidad de una mayor moderación del contenido o el comportamiento por las plataformas también crea incentivos para que estas se apoyen en algoritmos automatizados de toma de decisiones a fin de satisfacer las expectativas de que se analicen los contenidos y comportamientos controvertidos. En este escenario, el debate sobre la transparencia de los procedimientos, los criterios y las justificaciones de las decisiones cobra mayor importancia.

El tema se ha abordado en cierta medida en relación con la protección de los datos y el debate sobre el derecho a una explicación cuando tiene lugar la moderación automatizada. Muchas empresas publican informes de transparencia y presentan algunos de sus procedimientos en sus condiciones de uso o en las normas de la comunidad⁶⁴.

La conveniencia de recurrir a normas vinculantes o códigos de conducta, la corregulación o la autorregulación, sigue abierta a debate. En América Latina y el Caribe, varias organizaciones de la sociedad civil opinan que una mayor transparencia es esencial. Los países han abordado esta cuestión proponiendo normas vinculantes, pero estas deben elaborarse cuidadosamente, ya que pueden tener un efecto perjudicial en el desarrollo de nuevas soluciones e imponer una carga de altos costos y burocracia a las empresas nacientes y emergentes⁶⁵.

Por consiguiente, la transparencia como principio es importante para el desarrollo de una sólida gobernanza de Internet en América Latina y el Caribe. Sin embargo, para imponerla a los intermediarios de Internet, hay que tener en cuenta las diferentes variables que actúan en la región, la capacidad de los intermediarios para implementarla y los efectos en el entorno de innovación y empresas emergentes que se está desarrollando.

⁶² Véase M. P. Canales, *La herejía tecno-optimista florece en pandemia: un repaso crítico a las tecnologías disponibles*, Derechos Digitales, 2020 [en línea] <https://www.derechosdigitales.org/wp-content/uploads/heresia-tecnooptimista.pdf>.

⁶³ Véase [en línea] <https://www.eff.org/deeplinks/2020/06/5-serious-flaws-new-brazilian-fake-news-bill-will-undermine-human-rights>. Véase también [en línea] <https://blog.mozilla.org/netpolicy/2020/06/29/brazils-fake-news-law-harms-privacy-security-and-free-expression/>.

⁶⁴ Véase [en línea] <https://rankingdigitalrights.org/>.

⁶⁵ El proyecto de ley de noticias falsas propuesto en el Brasil contiene disposiciones sobre la transparencia de las redes sociales y los servicios de mensajería. Véase el texto del proyecto de ley (en portugués) [en línea] <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>.

4. Cada vez se presta más atención al debido proceso en la moderación de contenidos

Otro aspecto importante de la evolución del papel de los intermediarios es la importancia de ofrecer oportunidades para impugnar las decisiones de moderación del contenido. La velocidad y la omnipresencia de los servicios de Internet hacen que el examen posterior por parte de la judicatura pueda ser inaccesible para los usuarios o causar dificultades o daños importantes. Hacer que agentes privados, es decir, los intermediarios de Internet, respondan de sus actos o proporcionar a los usuarios una forma de protestar, apelar o defenderse puede resultar crucial para la preservación de importantes valores sociales y derechos fundamentales (que se tratan con más detalle en la sección V.A.5).

No cabe duda de que, al igual que con la transparencia, el hecho de exigir legalmente esos procedimientos de impugnación puede dar lugar a situaciones difíciles en las que no todos los intermediarios podrán hacer frente a las exigencias que se les impongan. Sin embargo, es importante que en principio se disponga de cierto nivel de revisión, en particular desde el punto de vista de la protección de los ciudadanos de América Latina y el Caribe. Uno de los expertos encuestados señaló que la región tenía a consumir tecnologías desarrolladas fuera de ella y que estas no se adaptaban a las circunstancias de los ciudadanos latinoamericanos y caribeños. Proporcionar un espacio para que los resultados puedan ser impugnados y revisados es, por lo tanto, una forma de hacer que los servicios sean más sólidos y compatibles con las necesidades de las personas y más coherentes con sus derechos y el contexto en el que viven. Esto debe considerarse como una oportunidad para la adaptación.

Las consecuencias de esas nuevas funciones para los intermediarios, ya sean cambios en la responsabilidad, una mayor regulación o la imposición de nuevas obligaciones, plantean a su vez nuevas cuestiones transfronterizas, entre ellas las relativas a la forma de preservar mejor los derechos humanos y el carácter mundial de Internet, con las oportunidades de innovación que ofrece. Los países de América Latina y el Caribe, al igual que otros Estados de todo el mundo, tienen que equilibrar las ventajas y desventajas de las nuevas funciones de los intermediarios de Internet con los métodos utilizados para mitigar los riesgos.

CAPÍTULO ||

**PRINCIPALES
TENDENCIAS DE
ACTUALIDAD
EN AMÉRICA LATINA
Y EL CARIBE**

A. Expresión

1. Noticias falsas y desinformación

1.1. Aumento de las medidas regulatorias

Internet ha reducido las barreras para los ciudadanos que quieren informarse y expresarse. Al mismo tiempo, la desinformación, es decir, la difusión masiva de información falsa, fuera de contexto o con la intención de causar daño, también ha aumentado.

La velocidad, el volumen y el carácter viral de los flujos de información hacen que resulte difícil controlarlos. El uso de datos personales para campañas microdirigidas⁶⁶ y el efecto que tienen algunos algoritmos de crear burbujas de filtro⁶⁷ o cámaras de eco —en las que las personas ven, oyen y escuchan solo lo que quieren o esperan— aumenta la necesidad acceder a información confiable. Lo que está en juego es la capacidad de las personas de formar sus pensamientos, ideas y opiniones sin recibir ninguna influencia indebida.

Esta situación es particularmente grave durante las elecciones. Las partes interesadas encuestadas reiteraron muchas de las preocupaciones manifestadas por los actores internacionales. La desinformación puede conducir a la polarización⁶⁸, los silos de información, la supresión del voto⁶⁹ y la manipulación de la agenda política, entre otros efectos negativos⁷⁰. Una de las partes interesadas mencionó que los ataques y la manipulación proceden de actores tanto extranjeros como nacionales que utilizan la red para sembrar deliberadamente la división y la polarización.

Como afirmó una de las partes interesadas entrevistadas:

“La interferencia electoral es una gran amenaza para el derecho universal de las personas a participar en el proceso democrático. Este es un tema con el que tanto los gobiernos como las empresas tecnológicas están lidiando para hacer frente a los desafíos que representan las nuevas tácticas y tecnologías de intromisión electoral. Cabe señalar que los ataques y la manipulación coordinada ya no provienen únicamente de potencias extranjeras malignas. Cada vez más, la interferencia en los procesos electorales es utilizada por actores nacionales que tratan de sembrar la división y la polarización, tanto en contextos autoritarios como democráticos.”

Los países de América Latina y el Caribe han respondido a estas tendencias de diversas maneras. La mayoría de ellos han seguido una tendencia a elaborar reglamentos en los que se tipifica como delito la difusión de desinformación —generalmente en la sección relativa a las denominadas “noticias falsas”— o se impone a las plataformas de Internet la obligación de ser más proactivas en su vigilancia de los contenidos, trasladando a menudo la carga de la responsabilidad a los intermediarios de Internet.

⁶⁶ Véase [en línea] https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf.

⁶⁷ E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, Nueva York, Penguin, 2011.

⁶⁸ C. Sunstein, *Republic: Divided Democracy in the Age of Social Media*, Princeton University Press, Princeton, 2017.

⁶⁹ A. McStay, “Fake news and the economy of emotions: problems, causes, solutions”, *Digital Journalism*, vol. 6, N° 2, 2018 [en línea] <https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1345645>.

⁷⁰ Organización de los Estados Americanos (OEA), *Guía para garantizar la libertad de expresión frente a la desinformación deliberada en contextos electorales*, 2019 [en línea] https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf.

La amenaza de la criminalización ha sido la estrategia utilizada en el Perú, por ejemplo, donde el Ministerio de Justicia y Derechos Humanos declaró que el contenido que manipula a los ciudadanos con el fin de obtener un beneficio o alterar el orden público podría ser sancionado penalmente⁷¹. En otros países, entre ellos la Argentina, Colombia, Costa Rica, México y el Uruguay, se han realizado debates públicos sobre el tema a fin de llevar a las plataformas a integrar iniciativas de verificación de la información en su arquitectura⁷².

El Brasil ha ampliado la gama de tácticas desplegadas, y la Corte Suprema⁷³ y el Congreso Nacional⁷⁴ han iniciado, por separado, investigaciones sobre personas y redes coordinadas que supuestamente difunden discursos de odio y desinformación. Además, el 30 de junio de 2020 el Senado Federal aprobó un extenso proyecto de ley con el que se busca regular las “noticias falsas”⁷⁵. De hecho, regula una amplia variedad de asuntos, revisando sustancialmente el papel que desempeñan las plataformas de medios sociales y los servicios de mensajería. Ahora deben rastrear los mensajes de amplia difusión (“virales”), exigir una identificación adecuada en determinadas circunstancias, moderar el contenido, estableciendo un procedimiento de defensa y apelación muy detallado, y facilitar el acceso a los datos, independientemente de dónde se originen o se almacenen. El proyecto de ley también propone la creación de un órgano consultivo y establece estrictas sanciones para los casos de incumplimiento (véase más información sobre esta tendencia en la sección III.A.5).

No cabe duda de que la lucha contra la desinformación tiene repercusiones transfronterizas: las empresas que ofrecen bienes y servicios a través de las fronteras tendrán que adaptar sus políticas para hacer frente a las nuevas responsabilidades.

1.2. Los bots han automatizado las noticias falsas y la desinformación

El comportamiento orgánico y auténtico puede dar lugar a una amplia difusión de la información, pero cuando se combina con herramientas automatizadas o “bots” (cuentas creadas artificialmente que son controladas, de manera parcial o total, por programas de automatización), aumenta el potencial para llegar a un público mucho más amplio⁷⁶. Estos instrumentos también orientan el tráfico (y la atención de la gente) hacia determinados temas y tipos de información, y pueden fomentar un sentido artificial de popularidad y relevancia⁷⁷. Por lo tanto, la automatización añade más “aceleración” a la niebla de la difusión de la información viral y, para el caso, la desinformación.

Por una parte, el uso de estos instrumentos de automatización puede tener un efecto positivo al poner al frente del debate público ideas y voces que son importantes, pero se encuentran marginadas. Sin embargo, por otra parte, esta misma función puede utilizarse para manipular la información, ampliar su alcance, crear una sensación de apoyo o consenso donde puede no haberlo, y ocultar hechos importantes⁷⁸. En otras palabras, estas herramientas pueden ser amplificadores de la desinformación⁷⁹.

El uso de bots y de la automatización en las plataformas mundiales plantea otros problemas transfronterizas. Desde el punto de vista del origen, estas herramientas pueden ser extranjeras. Los bots pueden desarrollarse en países extranjeros, o pueden funcionar desde fuera del país objetivo, tal vez dentro de una red internacional coordinada.

⁷¹ Perú, Gestión, “Personas que difundan noticias falsas podrían recibir hasta 6 años de prisión”, 8 de abril de 2020 [en línea] <https://gestion.pe/peru/coronavirus-peru-personas-que-difundan-noticias-falsas-podrian-recibir-hasta-6-anos-de-prision-segun-minjus-ministerio-de-justicia-estado-de-emergencia-cuarentena-ndnc-noticia/?ref=gesr>.

⁷² La plataforma pública de investigación Confiar, de la Argentina, es un ejemplo. Véase [en línea] www.argentina.gob.ar/noticias/confiar-la-plataforma-oficial-para-combatir-la-infodemia. Además, la organización de verificación de los hechos Chequeado, también creada en la Argentina, ha coordinado la coalición LatamChequea con 35 organizaciones de América Latina. Véase [en línea] <https://chequeado.com/latamcoronavirus/>.

⁷³ Corte Suprema del Brasil, “Inquiry 4781” [en línea] <http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444198&ori=1>.

⁷⁴ Senado Federal del Brasil, “Comissão Parlamentar Mista de Inquérito - Fake News” [en línea] <https://legis.senado.leg.br/comissoes/comissao/03codcol=2292>.

⁷⁵ Véase [en línea] <https://www.bloomberg.com/news/articles/2020-07-01/brazil-s-senate-approves-draft-bill-to-rein-in-on-fake-news>. Véase el texto original del proyecto de ley (en portugués) y su discusión [en línea] <https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>.

⁷⁶ C. Shao y otros, “The spread of low-credibility content by social bots”, *Nature communications*, vol. 9, 2018 [en línea] <https://www.nature.com/articles/s41467-018-06930-7>.

⁷⁷ J. Bayer y otros, “Disinformation and propaganda – Impact on the functioning of the Rule of Law in the EU and its Member States”, *HEC Paris Research Paper*, 2019 [en línea] <http://dx.doi.org/10.2139/ssrn.3499279>.

⁷⁸ P. Howard, *How Political Campaigns Weaponize Social Media Bots*, 2018 [en línea] <https://spectrum.ieee.org/computing/software/how-political-campaigns-weaponize-social-media-bots>. Véase también P. Howard, *The Lie Machines: How to Save Democracy from Troll Armies, Deceitful Robots, Junk News Operations, and Political Operatives*, Yale University Press, 2020.

⁷⁹ S. Bradshaw y P. Howard “Troops, trolls and troublemakers: a global inventory of organized social media manipulation”, *Oxford Computational Propaganda Research Project*, 2017 [en línea] <http://comprop.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf>.

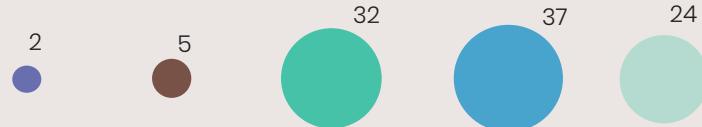
En América Latina y el Caribe⁸⁰, por ejemplo, se han notificado casos de bots que utilizaron la escritura cirílica durante las elecciones del Brasil, lo que parecería indicar un origen ruso⁸¹. En otra oportunidad, se descubrió que en una elección presidencial mexicana se usaron bots brasileños⁸². Las plataformas mundiales también han descubierto redes de cuentas automatizadas que participan en lo que se denomina “comportamiento inauténtico coordinado”. En casos significativos, el comportamiento se originó en un país pero se centró en otro⁸³.

Una segunda cuestión se refiere a las investigaciones sobre ese uso extranjero de herramientas automatizadas o bots. En muchos casos pueden violar las leyes electorales, e incluso leyes penales, sobre la difusión de desinformación. La información importante puede estar en manos de plataformas extranjeras que pueden –o no– tener un representante legal en el país en cuestión. También es posible que los datos no estén fácilmente disponibles o se almacenen en servidores en el extranjero.

Si bien en general se ha prestado atención a la forma de abordar estas técnicas a nivel nacional, los aspectos internacionales pueden tener un gran impacto en las futuras reglamentaciones para frenar las noticias falsas y la desinformación. Destacan la necesidad de cooperación y coordinación para encontrar soluciones a las campañas de desinformación en línea.

En las elecciones municipales de Río de Janeiro de 2016, se utilizó una combinación de herramientas automatizadas y un comportamiento auténtico coordinado. La campaña oficial de un candidato implementó una característica llamada “done un Me gusta” (“doe um like”). Consistía en solicitar a las personas que apoyaran al candidato donando la capacidad de dar “Me gusta” y compartir contenido durante un período de tres meses. Una vez aceptada la propuesta, una herramienta capturaría el perfil y la contraseña del usuario y los utilizaría para difundir el contenido del candidato. De este modo, cuentas reales pertenecientes a personas reales seguirían y, bajo un régimen automatizado coordinado, participarían en la campaña de un candidato⁸⁴.

La naturaleza transfronteriza de Internet, ¿facilita la interferencia extranjera en los procesos democráticos?



Está muy en desacuerdo No está de acuerdo ni en desacuerdo No está de acuerdo Está de acuerdo Está muy de acuerdo

Fuente: Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL).

2. Difamación

2.1 Los desafíos transfronterizos están aumentando

El respeto y la protección de la reputación y el honor personal se contemplan en las leyes de varios países con distintos antecedentes culturales. En tanto valor básico compartido, la difamación es ilegal, tanto en Internet como fuera de ella. Sin embargo, la aplicación, interpretación y extensión del concepto varían considerablemente. Internet ha exacerbado la importancia de estas diferencias jurídicas y ha generado más posibilidades de conflicto entre las distintas jurisdicciones.

⁸⁰ Véase un informe general del Consejo del Atlántico, *Disinformation in Democracies: Strengthening Digital Resilience in Latin America*, 2019 [en línea] <https://www.atlanticcouncil.org/wp-content/uploads/2019/09/Disinformation-in-Democracies.pdf>.

⁸¹ Véase [en línea] <http://dapp.fgv.br/en/fgv-survey-dapp-reveals-evidence-russian-robots-2014-presidential-election-campaigns/>.

⁸² Véase [en línea] https://horizontal.mx/bots-su-deteccion-y-la-participacion-en-las-campanas-electorales-en-mexico/#_ednl.

⁸³ Véase [en línea] <https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/>. Véase también [en línea] <https://www.theverge.com/2018/10/25/18021456/twitter-q3-2018-earnings-9-million-mau-decline>.

⁸⁴ D. Arnaudo, “Computational propaganda in Brazil: social bots during elections”, *Oxford Computational Propaganda Research Project*, 2017 [en línea] <https://blogs.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Brazil-1.pdf>.

Los desafíos transfronterizos surgen sobre todo cuando se presenta alguna de las siguientes situaciones: i) el contenido publicado en un país tiene repercusiones en otro; ii) el medio utilizado para la publicación se encuentra fuera del país en el cual la persona agravada tiene su residencia o trabajo habitual, ya sea porque la empresa que presta el servicio o los servidores están establecidos en otro país, o iii) el daño al honor o a la reputación de una persona ocurre en más de una jurisdicción.

En el informe *Internet & Jurisdiction Global Status Report 2019* se destacó que esto no es nuevo. Debido al potencial alcance geográfico mundial de Internet, los problemas transfronterizos de difamación han sido comunes en línea. En el caso *Dow Jones v. Gutnick*, por ejemplo, el Tribunal Supremo de Australia tuvo que decidir si la publicación se había producido en el lugar donde el artículo se había publicado en línea o donde se había descargado⁸⁵. Este tribunal fue uno de los primeros en entender que una publicación en línea puede difamar a alguien a través de las fronteras.

La cuestión de los daños y perjuicios no se podía determinar, ya que el demandante había limitado su reclamación a los daños y perjuicios sufridos en el lugar donde había entablado la demanda —Australia—, que era también donde le preocupaba principalmente proteger su reputación. Sin embargo, se dejó la puerta abierta a un debate mucho más amplio sobre si podría demandar en más de una jurisdicción, buscando los tribunales más favorables, y si podría reclamar por los daños y perjuicios que pudieran haberse producido a nivel mundial, en cualquiera de esas jurisdicciones o en todas. En cierto sentido, la cuestión es si una reputación puede ser internacional y los daños y perjuicios también deben tener en cuenta una posible dimensión extraterritorial. Las decisiones al respecto pueden interferir con las disposiciones legales de otros países y los derechos de sus ciudadanos. Si un tribunal decide conceder una indemnización por daños y perjuicios a nivel mundial, puede tomar en consideración a los países en los que el contenido no se consideraría difamatorio, limitando indirectamente la libertad de expresión.

Esto, a su vez, puede tener otras repercusiones transfronterizas. Por ejemplo, en América Latina y el Caribe, las solicitudes de indemnización por daños y perjuicios en casos de difamación con frecuencia han ido acompañadas de solicitudes de eliminación o rectificación del contenido considerado difamatorio. Los demandantes suelen perseguir a los intermediarios de Internet que se ven en la situación de tener que cumplir órdenes judiciales y decidir el alcance territorial de dichas órdenes.

Esto fue lo que ocurrió con Google y el servicio “Blogger.com”. Los tribunales colombianos⁸⁶ y mexicanos⁸⁷ instruyeron a Google para que eliminara ciertas publicaciones que aparecían en distintos blogs y se consideraban difamatorias. En el Brasil, Facebook recibió la orden de eliminar el contenido y dar de baja un perfil que se consideraba que difamaba a un candidato político⁸⁸. Cada uno de estos casos contribuye a que se entienda que ese contenido puede verse afectado en todo el mundo por fallos de tribunales nacionales.

En el caso *Glawischnig-Piesczek v. Facebook Irlanda*, el debate llegó al Tribunal de Justicia de la Unión Europea⁸⁹. La cuestión que se planteaba era si la Directiva sobre el comercio electrónico de la Unión Europea regulaba el ámbito de la jurisdicción y podía autorizar —o impedir— a los tribunales nacionales ordenar a Facebook que eliminara el contenido supuestamente difamatorio para un político austriaco con efecto mundial. La respuesta del tribunal no fue definitiva. En ella se afirmaba que la directiva de la Unión Europea no regulaba el alcance de la jurisdicción correctiva y que correspondía a los tribunales nacionales decidir al respecto, teniendo en cuenta sus propias leyes internas y el derecho internacional (véase más información sobre el alcance geográfico de la jurisdicción correctiva en la sección III.A.2).

También han surgido otros temas relacionados con la difamación. En la región se han dado casos relacionados con las técnicas de autocompletado⁹⁰ utilizadas en diferentes servicios de Internet, en

⁸⁵ Véase Tribunal Supremo de Australia “*Dow Jones and Company Inc v Gutnick* [2002] HCA 56” [en línea] <http://eresources.hcourt.gov.au/showCase/2002/HCA/56>.

⁸⁶ La Corte Constitucional de Colombia dictaminó que Google debía eliminar un blog que contenía declaraciones difamatorias. Véase I&J Retrospect Database [en línea] https://www.internetjurisdiction.net/publications/retrospect#article-6369_2017-10.

⁸⁷ Red de Políticas de Internet y Jurisdicción, diciembre de 2017. La Suprema Corte de Justicia de la Nación de México rechaza el argumento de Google de que los tribunales mexicanos no tienen jurisdicción sobre la plataforma. Véase I&J Retrospect Database [en línea] <https://www.internetjurisdiction.net/publications/retrospect#eyJ0byl6ijlwMjAtMDMifQ==>.

⁸⁸ Véase [en línea] <https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24-horas/62909>.

⁸⁹ Tribunal de Justicia de la Unión Europea, “*Case C-18/18 Glawischnig-Piesczek*”, 2019.

⁹⁰ Véase un interesante análisis de los desafíos de las técnicas de autocompletado en el trabajo de Paul Baker y Amanda Potts, “*Why do white people have thin lips? Google and the perpetuation of stereotypes via auto-complete search forms*”, *Critical Discourse Studies*, vol. 10, Nº 2, 2013, págs. 187-204.

particular en los buscadores⁹¹. Otra cuestión que ha cobrado importancia es la posible responsabilidad de las personas por el mero hecho de apoyar (por ejemplo, por poner “Me gusta”) un contenido considerado difamatorio o perjudicial⁹², o por compartir ese contenido⁹³. Por último, otra cuestión es hasta qué punto los administradores de grupos o comunidades de medios sociales, como los del servicio de mensajería WhatsApp, deben ser responsables de moderar el contenido dentro de ese grupo o comunidad⁹⁴.

2.2. La difamación sigue siendo un delito penal en algunos países de la región

En muchos países de América Latina y el Caribe, la difamación es un asunto de competencia no solo civil, sino también penal⁹⁵. La criminalización del discurso que viola la reputación de una persona sigue siendo una tradición jurídica muy arraigada en la región, pese a que el Sistema Interamericano de Derechos Humanos la ha condenado por considerarla una restricción indebida de la libertad de expresión⁹⁶. La difamación en línea también puede tener consecuencias penales, que pueden ser aún más preocupantes si el discurso se registra en época de elecciones, cuando la reparación sugerida de preferencia debe ser la rectificación o el derecho a respuesta⁹⁷.

La criminalización del discurso perjudicial para la reputación de una persona también tiene un efecto disuasorio por igual en la actividad de los periodistas profesionales, los periodistas ciudadanos y los blogueros, especialmente en las pequeñas ciudades de la región. Es fácil para las autoridades locales restringir severamente la expresión si alguien que está dando primicias o produciendo informes que podrían desagradarles arriesga su libertad al hacerlo.

3. Acoso en línea

A medida que la tecnología avanza, surgen diferentes tipos de ciberacoso⁹⁸. Tradicionalmente se reconoce que la intimidación se produce cuando hay un agresor y una víctima sometida a acoso emocional o físico. La intimidación por medio de tecnologías electrónicas, en especial Internet, incluye mensajes privados, la creación de sitios web destinados a hacer algún tipo de daño a otra persona, la publicación en línea de imágenes poco favorecedoras o inapropiadas sin permiso, y el trato hiriente o desagradable a través de teléfonos móviles o en línea⁹⁹.

El ciberacoso afecta a 1 de cada 10 niños¹⁰⁰. Según las Directrices para la protección de los niños en línea 2020 de la Unión Internacional de Telecomunicaciones (UIT), la mayoría de los niños son capaces de distinguir entre el ciberacoso y las bromas o provocaciones en línea, y reconocen que

⁹¹ En el Brasil ha habido fallos al respecto. Véase [en línea] <https://www.migalhas.com.br/arquivos/2014/9/art20140917-05.pdf>. La Corte Constitucional de Colombia también ha decidido que los buscadores no son responsables cuando entre sus resultados aparecen enlaces a contenidos considerados difamatorios. Colombia, Corte Constitucional, “Sentencia T-040/13”, 28 de enero de 2013 [en línea] <http://bit.ly/1fyIMk>; Corte Constitucional, “Sentencia T-453/13”, 15 de julio de 2013 [en línea] <http://bit.ly/1R6lHaO>; Corte Constitucional, “Sentencia T-634/13”, 13 de septiembre de 2013 [en línea] <http://bit.ly/1OyMapE>.

⁹² Sobre la situación internacional, véase [en línea]: <https://blog.oup.com/2017/09/traps-of-social-media/>. Véase también [en línea] <https://www.internationallawoffice.com/Newsletters/Litigation/Switzerland/Lenz-Staehelin/Liking-or-sharing-defamatory-Facebook-posts-can-be-unlawful>.

⁹³ Véase [en línea] <https://www.conjur.com.br/2017-nov-10/limite-penal-curtir-compartilhar-publicacoes-ofensivas-redes-sociais-crime>.

⁹⁴ Véase [en línea] <https://www.uol.com.br/tilt/noticias/redacao/2018/07/17/justica-pode-mirar-administrador-de-grupo-no-whatsapp-em-que-houve-crime.htm>.

⁹⁵ Como ejemplo, véase el estudio general realizado por el Comité para la Protección de los Periodistas sobre las leyes penales de difamación en América del Sur [en línea] <https://cpj.org/reports/2016/03/south-america.php>. Véase también el estudio del Instituto Internacional de la Prensa sobre las leyes penales de difamación en el Caribe [en línea] <https://ipi.media/pi-adds-caribbean-defamation-laws-to-online-database/>.

⁹⁶ Corte Interamericana de Derechos Humanos, “Caso Herrera Ulloa vs. Costa Rica. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 2 de julio de 2004”, Serie C, núm. 107; “Caso Ricardo Canese vs. Paraguay. Fondo, reparaciones y costas. Sentencia de 31 de agosto de 2004”, Serie C, núm. 111; “Caso Kímel vs. Argentina. Fondo, reparaciones y costas. Sentencia de 2 de mayo de 2008”, Serie C, núm. 177; “Caso Tristán Donoso vs. Panamá. Excepciones preliminares, fondo, reparaciones y costas. Sentencia de 27 de enero de 2009”, Serie C, núm. 193; “Caso González Medina y Familia vs. República Dominicana. Sentencia de 27 de febrero de 2012”; “Caso Vélez Restrepo vs. Colombia. Sentencia de 3 de septiembre de 2012”; y “Caso Fontevecchia y D’Amico vs. Argentina. Sentencia de 29 de noviembre de 2011”.

⁹⁷ Véase [en línea] https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf.

⁹⁸ Peter K. Smith, Georges Steffgen y Ruth Sittichai, “The nature of cyberbullying, and an international network”. *Cyberbullying through the New Media: Findings from an International Network*, Peter K. Smith y Georges Steffgen (eds.), Psychology Press: Taylor & Francis, 2013, pág. 5.

⁹⁹ Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), *Behind The Numbers: Ending School Violence and Bullying*, 2019, pág. 14 [en línea] <https://unesdoc.unesco.org/ark:/48223/pf0000366483?posInSet=8&queryId=a84f5b5a-3828-462f-b63c-d45eae258884>.

¹⁰⁰ Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), *Behind the Numbers: Ending School Violence and Bullying*, pág. 14 [en línea] <https://unesdoc.unesco.org/ark:/48223/pf0000366483?posInSet=8&queryId=a84f5b5a-3828-462f-b63c-d45eae258884>.

el ciberacoso tiene por objeto causar daño¹⁰¹. En las Directrices sobre la protección de la infancia en línea para los encargados de formular políticas se recomienda el establecimiento de una legislación nacional adecuada y se afirma que la armonización y la coordinación a nivel internacional es un paso fundamental para proteger a los niños en línea. Ello se debe a que contar con normas de procedimiento y leyes sobre ciberdelincuencia armonizadas en la materia permitiría establecer con mayor eficacia las sanciones penales necesarias para hacer frente a los daños que los niños pueden sufrir en línea¹⁰².

Cuando el autor del ciberacoso es anónimo o utiliza una cuenta falsa, la aplicación de normas contra este tipo de práctica resulta difícil y puede conducir a que los encargados de formular políticas adopten decisiones más firmes. Por ejemplo, la aplicación Secret se eliminó de la App Store del Brasil tras una serie de denuncias de ciberacoso que supuestamente se había producido en forma de “secretos” anónimos publicados en la aplicación¹⁰³. La misma aplicación fue muy criticada en México, también por supuestamente permitir prácticas de ciberacoso¹⁰⁴.

Global Kids Online es una importante iniciativa para proporcionar una base de pruebas internacionales sobre el uso de Internet por parte de los niños y para conectar a los interesados. Los países de la región que disponen de resultados de investigación son la Argentina, el Brasil, Chile y el Uruguay¹⁰⁵.

En abril de 2020, SaferNet Brasil y el Fondo de las Naciones Unidas para la Infancia (UNICEF) lanzaron una campaña conjunta para combatir el ciberacoso: #ÉDaMinhaConta (“Es cosa mía”). La campaña brinda instrucciones sobre cómo actuar en situaciones de intimidación (por ejemplo, cómo identificar si una persona es un objetivo o está intimidando a otra).

Una investigación realizada por la Fundación Paniamor en Costa Rica, en la que participaron 1.008 niños de entre 9 y 17 años, ha arrojado importantes conclusiones sobre el uso de Internet por parte de los niños y los riesgos relacionados con la violencia y la discriminación. De una muestra de niños de entre 9 y 12 años, el 5,9% dijo haber sido discriminado o sufrido abuso a través de Internet, y el 2,5% dijo no saberlo¹⁰⁶. Entre los de 13 a 17 años, el 3,2% dijo que sí y el 2,8% no estaba seguro¹⁰⁷.

En el Brasil, el ciberacoso y los delitos directos son los motivos más comunes para llamar al teléfono de asistencia de SaferNet, por encima de los problemas relacionados con la protección de datos, el fraude o el discurso de odio¹⁰⁸. En total, el ciberacoso es el que más notificaciones ha recibido, con 2.310 casos de un total de 25.184 desde 2007.

4. Distribución no consentida de material sexualmente explícito

La distribución no consentida de material sexualmente explícito puede ocurrir de diferentes maneras. Puede ser perpetrada por desconocidos que publican deliberadamente material sexualmente explícito en línea o por alguien que ha tenido una relación íntima con la persona y publica lo que comúnmente se conoce como pornografía de venganza (o “pornovenganza”).

Los países de América Latina y el Caribe han adoptado diferentes enfoques para abordar la cuestión. En algunos casos, la distribución no consentida de material sexualmente explícito puede tratarse como difamación, mientras que en otros se adopta un enfoque más específico, que modifica la legislación penal para tratar la práctica como un nuevo tipo de conducta delictiva.

Entre mediados de 2018 y 2020, 17 estados de México aprobaron la Ley Olimpia, que reforma la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y los códigos penales para reconocer la violencia digital como delito, con multas y penas que pueden llegar a los ocho años de prisión (en Michoacán)¹⁰⁹.

El Brasil tiene normas específicas tanto en el derecho penal como en el civil. La transmisión, publicación, distribución o puesta a disposición de pornografía, material sexualmente explícito o

¹⁰¹ Unión Internacional de Telecomunicaciones (UIT), “Guidelines on Child Online Protection”, 2020 [en línea] <https://www.itu-cop-guidelines.com/>.

¹⁰² Unión Internacional de Telecomunicaciones (UIT) *Directrices sobre la protección de la infancia en línea para los encargados de formular políticas*, 2020, págs. 28 y 29 [en línea] <https://www.itu-cop-guidelines.com/policymakers>.

¹⁰³ UOL, “Aplicativo Secret cria polêmica ao permitir postagem anônima de ‘segredos’”, 2014 [en línea] <https://www.uol.com.br/ituit/noticias/redacao/2014/08/13/secret-cria-polamica-ao-prometer-anonimato-acao-visa-proibir-o-aplicativo.htm>. Véase también GI, “Secret é retirado de loja de aplicativos da Apple no Brasil”, 2014 [en línea] <http://gi.globo.com/tecnologia/noticia/2014/08/secret-e-retirado-de-loja-de-aplicativos-da-apple-no-brasil.html>.

¹⁰⁴ Milenio, “Secret, la “app” preferida de los jóvenes para “cyberbullying””, 2014 [en línea] <https://www.milenio.com/cultura/secret-la-app-preferida-de-los-jovenes-para-ciberbullying>.

¹⁰⁵ Véase Global Kids Online [en línea] <http://globalkidsonline.net/about/>.

¹⁰⁶ Véase Informe Primera Encuesta Kids Online Costa Rica, Niñas, niños y adolescentes en la Internet, abril de 2019, figura 32 [en línea] <http://globalkidsonline.net/wp-content/uploads/2019/07/Kids-Online-Costa-Rica-1-Julio.pdf>.

¹⁰⁷ Ibíd.

¹⁰⁸ SaferNet, Helpline [en línea] <https://helpline.org.br/indicadores/>.

¹⁰⁹ México, “Ley Olimpia” [en línea] <http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf>.

imágenes de desnudos, con o sin el consentimiento de la víctima, es un delito que se castiga con una pena de entre uno y cinco años de prisión¹¹⁰. Por otra parte, en el artículo 21 del Marco Civil de Internet del Brasil se prevé un régimen específico de retiro de imágenes, videos u otros materiales que representen desnudos o actos sexuales de carácter privado: el proveedor de aplicaciones de Internet debe retirar el contenido al recibir una notificación extrajudicial, es decir, una denuncia del usuario¹¹¹.

En el Uruguay, la distribución no consentida de material sexualmente explícito es un delito y las plataformas de Internet están sujetas a sanciones si no retiran el contenido de inmediato¹¹². En otros países, como Chile¹¹³ y el Perú¹¹⁴, se están debatiendo proyectos de ley para abordar específicamente la distribución no consentida de material sexualmente explícito.

Si bien en algunos casos puede ser difícil para las tecnologías automatizadas reconocer el propósito de una publicación con contenido sexualmente explícito (tema que trata la campaña #WeTheNipple)¹¹⁵, las plataformas intermedias han ido tomando cada vez más medidas para responder a la violencia de género¹¹⁶. En primer lugar, la distribución no consentida de material sexualmente explícito viola las directrices comunitarias de todas las plataformas principales, como se describe en el *Internet & Jurisdiction Global Status Report 2019*¹¹⁷. Además, las plataformas están utilizando el aprendizaje automático y la inteligencia artificial para detectar imágenes o videos que se están compartiendo sin consentimiento, y también han puesto en marcha centros de apoyo a las víctimas¹¹⁸.

Aun así, las organizaciones de la sociedad civil piden cada vez más una respuesta más proactiva por parte de las plataformas, en lo que respecta a dar una respuesta más rápida a las notificaciones y ser más transparentes con los datos sobre violencia de género¹¹⁹.

Además de todo lo mencionado, es importante considerar que las víctimas de la distribución no consentida de material sexualmente explícito por lo general pertenecen a grupos vulnerables y a menudo discriminados. Las mujeres, por ejemplo, suelen ser las víctimas, mientras que los hombres son los perpetradores¹²⁰. Este tipo de abuso, sin embargo, no es el único que enfrentan las mujeres en línea.

Los activistas mexicanos han descrito al menos 13 posibles manifestaciones de la violencia de género en línea: acceso no autorizado y control de acceso, control y manipulación de la información, suplantación y robo de identidad, vigilancia y hostigamiento criminal, discurso discriminatorio, acoso, amenazas, intercambio no consentido de información privada, extorsión, denigración, abuso y explotación sexual relacionados con la tecnología, ataques a canales de comunicación y negligencia por parte de los agentes reguladores¹²¹.

El abuso selectivo de este tipo es particularmente frecuente en una región en la que al menos 12 mujeres mueren cada día debido a incidentes relacionados con el mero hecho de ser mujeres¹²² y donde la igualdad de género todavía está lejos de ser una realidad¹²³. En virtud de ello, la violencia

¹¹⁰ Brasil, Código penal, artículo 218-C [en línea] http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm.

¹¹¹ Chiara A. S. de Teffé "What is revenge porn and how can I protect myself?" *Brazil's Internet Bill of Rights: A Closer Look*, Carlos Affonso Souza, Mario Viola y Ronaldo Lemos (eds.), 2017, pág. 137 [en línea] https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf.

¹¹² Uruguay, "Ley nº 19580", 2018, artículo 92 [en línea] <https://www.imojo.com.uy/bases/leyes/19580-2017>.

¹¹³ Chile, Boletines, núm. 11923-25 y 12164-07 [en línea] <https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=12444&prmBoletin=11923-25>.

¹¹⁴ Véase [en línea] http://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0166920170717.pdf y <http://www.congreso.gob.pe/comisiones2016/Justicia/ProyectosLey/>.

¹¹⁵ La campaña pide a Facebook e Instagram que hagan una excepción a sus restricciones respecto de la desnudez para permitir el arte en la técnica fotográfica. Cuenta con el apoyo de representantes de distintos países del mundo, incluidos el Brasil, Chile, Colombia y la República Dominicana.

¹¹⁶ Julian Pacetta Ruiz, Mariana Girogetti Valente y Natália Neris, "Between the perpetrator and the victim: the role of Internet intermediaries on violations against women", *Sociología y Tecnociencia*, vol. 9, Nº 1, 2019, págs. 14-17. Véase [en línea] <https://revistas.uva.es/index.php/sociotecnico/article/view/2240/t779>.

¹¹⁷ Red de Políticas de Internet y Jurisdicción, *Internet & Jurisdiction Global Status Report*, 2019, pág. 86.

¹¹⁸ Facebook, "Detecting Non-Consensual Intimate Images and Supporting Victims", marzo de 2019. Véase [en línea] <https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/>.

¹¹⁹ México, "Internet es nuestra MX. Llamado a las plataformas digitales a agilizar procesos de denuncia tras agresiones que mujeres reciben en el marco de protesta #NoMeCuidanMeViolan", 2019. Véase [en línea] <https://internetesnuestra.mx/post/187169630893/llamado-a-las-plataformas-digitales-a-agilizar>.

¹²⁰ Clare McGlynn, Erika Rackley y Ruth Houghton, "Beyond 'revenge porn': the continuum of image-based sexual abuse", 2017. Véase [en línea] <https://link.springer.com/content/pdf/10.1007/s10691-017-9343-2.pdf>; Abby Whitmarsh, "Analysis of 28 days of data scraped from a revenge pornography Website", 2015. Véase [en línea] <https://everlastingstudent.wordpress.com/2015/04/13/analysis-of-28-days-of-data-scraped-from-a-revenge-pornography-website/>.

¹²¹ GenderIT.org "13 manifestations of gender-based violence online" (2018). Véase [en línea] <https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology>.

¹²² Comisión Económica para América Latina y el Caribe (CEPAL), "Feminicidio", Infografías, 24 de octubre de 2016 [en línea] <https://www.cepal.org/es/infografias/feminicidio>. En 2018, los países latinoamericanos con las tasas más altas de femicidio por cada 100.000 mujeres eran El Salvador (6,8), Honduras (5,1), Bolivia (Estado Plurinacional de) (2,3), Guatemala (2,0) y la República Dominicana (1,9). En el Caribe, Santa Lucía (4,4) y Trinidad y Tabago (3,4) registraron las tasas más elevadas. Véase CEPAL, "Feminicidio" [en línea] <https://oig.cepal.org/es/indicadores/feminicidio>.

¹²³ Véase "Indicadores" [en línea] <https://oig.cepal.org/es/indicadores> y CEPAL, "Planes de igualdad de género en América Latina y el Caribe: mapas de ruta para el desarrollo", *Observatorio de Igualdad de Género de América Latina y el Caribe. Estudios*, N°1 (LC/PUB.2017/1-P/Rev.1), Santiago, 2019.

en línea y fuera de línea deben verse como interconectadas y no deben tratarse por separado¹²⁴. No se trata de que un cierto tipo de abuso comience y termine en línea. La violencia puede tener lugar tanto fuera de línea como, en forma reiterada (y continua), en línea¹²⁵. Un ejemplo es cuando el abuso sexual se filma y se difunde en los medios sociales o cuando los activistas por los derechos de la mujer reciben amenazas en línea seguidas de ataques en la vía pública.

La dificultad de hacer cumplir esa eliminación de contenido, a veces debido a cuestiones de jurisdicción, también puede tener consecuencias que cambian la vida de las mujeres. En Colombia, por ejemplo, no se pudo identificar al remitente de las amenazas contra una mujer porque estas se enviaron desde un lugar público (un cibercafé). En otro caso, no se pudo identificar al autor porque la dirección correspondía a un lugar de los Estados Unidos¹²⁶.

Esos casos tienen un efecto que va más allá de la víctima y alcanza a todas las mujeres. Como señaló la Relatora Especial de las Naciones Unidas sobre la violencia contra la mujer: “A pesar de las ventajas y el potencial de empoderamiento de Internet y de las TIC, las mujeres y las niñas de todo el mundo han expresado en forma creciente su preocupación por el contenido y el comportamiento dañinos, sexistas, misóginos y violentos en línea. Por lo tanto, es importante reconocer que Internet se está utilizando en un entorno más amplio de discriminación y violencia por razón de género, generalizado, estructural y sistémico contra las mujeres y las niñas”¹²⁷.

En suma, los diferentes tipos de abusos que podrían perjudicar a todos también deben verse a través de la lente específica de los grupos a los que se dirigen, ya sean mujeres, minorías étnicas, pueblos indígenas, inmigrantes o personas LGBTQ. El otro lado de esta perspectiva es la forma en que Internet también ha dado voz a los grupos socialmente marginados y les ha ayudado a crear redes para luchar contra las amenazas en línea, combatir la violencia de género y prestar apoyo a las víctimas. Dos ejemplos son: Dominemos la Tecnología (en todo el mundo)¹²⁸ y Vita Activa (Méjico)¹²⁹.

5. El “derecho al olvido” se enfrenta a las características particulares de la región

Como se explica con más detalle en la sección II.C.6, varios países de la región han adoptado una ley general de protección de datos, más o menos inspirada en el Reglamento general de protección de datos de Europa. También ha incidido la decisión adoptada en 2014 por el Tribunal de Justicia Europeo en el caso de Google España, en virtud de la cual, un ciudadano español podía ejercer su “derecho al olvido” contra los buscadores en línea y se obligaba a las empresas implicadas a eliminar algunos resultados de búsqueda supuestamente perjudiciales¹³⁰.

Esta decisión desató un debate en toda la región, centrado en la situación reglamentaria de muchos países que ya han reconocido el derecho al olvido y la cuestión de si es prudente o incluso deseable instituir ese derecho. El debate se entiende más adecuadamente como un derecho a solicitar la “supresión de la lista” o la “desindexación”. En España, debido a que la sentencia no establecía tal requisito, el contenido en sí no se borra. En cambio, a los buscadores como Google, Bing y otros solo se les insta a suprimir los resultados de las consultas basadas en el nombre de la persona —y otras características personales identificables— relacionados con información que se considera irrelevante, obsoleta o sin valor real.

El caso de Google España ha motivado una serie de demandas que afirman ese derecho en el contexto de la región. Las diferencias en las normas de protección de datos (o la falta de ellas) no han impedido que algunos tribunales nacionales reconozcan la existencia de un “derecho al olvido” y ordenen a los

¹²⁴ InternetLab, *Online Gender-based Violence: Diagnosis, Solutions and Challenges. Joint Contribution to Inform the Work of the UN Special Rapporteur on Violence Against Women*, 2017, pág. 15 [en línea] https://www.internetlab.org.br/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_ONU.pdf.

¹²⁵ Agencia Sueca de Cooperación Internacional para el Desarrollo (Asdi), “Gender-based violence online”, 2019. Véase [en línea] https://www.sida.se/contentassets/97224704b4f643cba3b4fca3d931e576/brief_gender-based_violence_online_sep-2019_webb.pdf.

¹²⁶ Estudio de caso N.º 1, Colombia (Ramírez Cardona (2014), citado en Asociación para el Progreso de las Comunicaciones (APC). From Impunity to Justice: Domestic Legal Remedies for Cases of Technology-Related Violence against Women, proyecto “End violence: Women’s rights and safety online” (pág. 22) [en línea] https://www.genderit.org/sites/default/files/flow Domestic_legal remedies_0.pdf.

¹²⁷ Naciones Unidas, Informe de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos (A/HRC/38/47), 2018 [en línea] <https://undocs.org/es/A/HRC/38/47>.

¹²⁸ Véase [en línea] <https://www.takebackthetechnet.net/>.

¹²⁹ Véase [en línea] <https://vita-activa.org/>.

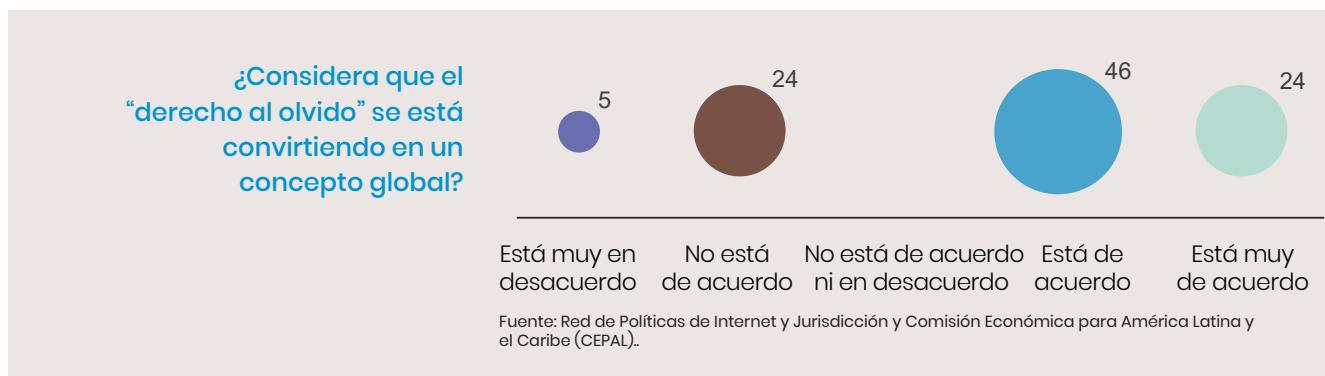
¹³⁰ Tribunal de Justicia de la Unión Europea, Case C-131/12 Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, 2014.

buscadores —y a veces a los medios de comunicación— que quiten la información de las listas¹³¹. La mayoría de las veces, los parámetros de este derecho no quedaban claros: su alcance e incluso quién debería ser responsable de la supresión de la lista y en qué condiciones se dejan abiertos¹³².

Otros tribunales han desestimado el derecho o lo han limitado¹³³. La historia de la protección de la libertad de expresión en la región tiende a servir de contrapeso a la supresión de la lista, en particular sin una orden judicial¹³⁴.

5.1. El “derecho al olvido” se percibe ampliamente como un concepto global

A los interesados encuestados se les preguntó si el derecho al olvido había alcanzado un estatus mundial o si era aplicable a América Latina y el Caribe en su conjunto. Uno de los interesados mencionó que la expresión “derecho al olvido” se había utilizado en la región como un término amplio, que incluye todos los casos en que los usuarios exigen a los proveedores de servicios de Internet que eliminen, desindexen, quiten de las listas u oculten contenido. Otros opinaron que el concepto detrás del derecho estaba cobrando impulso y que ciertos tribunales y países lo estaban reconociendo. En general, el 70,73% de las partes interesadas encuestadas y entrevistadas estaba de acuerdo o muy de acuerdo en que el derecho al olvido era, en efecto, un concepto global.



Como señaló una de las partes interesadas encuestadas: “El derecho al olvido es un nuevo derecho propuesto en el contexto de la sociedad de la información. Las reacciones a este derecho varían de un país a otro porque el concepto y el fundamento aún no están claramente definidos. La falta de consenso sobre este punto puede crear incertidumbre en una sociedad cada vez más desprovista de fronteras. Las decisiones específicas de cada país no son suficientes para el desarrollo sin problemas de este concepto, y existe una necesidad urgente de alcanzar un consenso con respecto a los puntos básicos. Dado el carácter sin fronteras del mundo actual, el conflicto entre los valores fundamentales, la protección de la dignidad de un individuo frente al derecho a saber y a garantizar la libertad de expresión, tiene resultados variables”.

5.2. Las leyes locales de amnistía y la noción compensatoria del “derecho a la memoria” inciden en la aplicación de un derecho al olvido

Ciertos elementos del ordenamiento jurídico, la historia y la cultura de la región se diferencian de sus raíces europeas originales. En los últimos tiempos, por ejemplo, muchos países de América Latina y el Caribe han debido soportar regímenes autoritarios y varios de los líderes han sido acusados de

¹³¹ Véase [en línea] https://law.stanford.edu/wp-content/uploads/2017/09/The_-Right-to-Be-Forgotten_-and-Blocking-Orders-under-the-American-Convention-Emerging-Issues-in-Intermediary-Liability-and-Human-Rights_Sep17-.pdf.

¹³² Véase [en línea] https://www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf.

¹³³ Uno de los casos más importantes se refería a la cuestión de si se podía responsabilizar a los intermediarios por contenidos que afectaran la privacidad o la reputación. El tribunal consideró que la supresión de la lista solo debe realizarse con una orden judicial o cuando se trate de información ilícita (Argentina, Corte Suprema, Caso “Rodríguez M. Belen c/Google y Otros/daños y perjuicios”, Sentencia R.522.XLIX, 28 de octubre de 2014). En el Brasil, el derecho ha sido ampliamente debatido y fue objeto de una audiencia pública en el Supremo Tribunal Federal, que hizo lugar al derecho con limitaciones. Véanse las actas del debate sobre el caso de Aida Curi [en línea] http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/AUDINCIAPBLICASOBREODIREITOAOESQUECIMENTO_Transcries.pdf.

¹³⁴ Véase [en línea] <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf>.

atroces violaciones de los derechos humanos. En la transición hacia la democracia, en la mayoría de estos Estados se han promulgado leyes de amnistía en virtud de las cuales se perdonan a los responsables de las violaciones de los derechos humanos y, en muchos casos, se impide tanto el acceso a la verdad sobre lo ocurrido como a cualquier tipo de reparación.

Bajo la orientación sustantiva del Sistema Interamericano de Derechos Humanos, en las últimas décadas se ha intentado trabajar sobre el derecho opuesto: el derecho a la memoria, el derecho de las víctimas a tener acceso a la verdad¹³⁵. En virtud de ese derecho, se plantearon oposiciones a las leyes de amnistía, se establecieron Comisiones de la Verdad e incluso se ha enjuiciado a algunos de los autores de los hechos.

En la actualidad, los expertos en protección de datos, las autoridades y las organizaciones de la sociedad civil¹³⁶ entienden que el derecho al olvido va en contra de esta tradición cultural y de derechos humanos¹³⁷. Por consiguiente, a nivel regional, la supresión como concepto debe ir acompañada de un derecho a la memoria, sobre todo en situaciones relativas a la información sobre violaciones —presuntas o reales— de los derechos humanos.

No obstante, algunos países han incluido en su legislación de protección de datos el derecho a la supresión de datos personales con una redacción similar a la del denominado “derecho al olvido” que se plantea en el caso europeo mencionado.

Las diferencias entre Europa y América Latina y el Caribe siguen radicando en que los países de la región suelen tratar la protección de los datos como algo relativo a los datos almacenados en back-end, en contraposición con el contenido que se hace público y que se entiende más claramente como algo relacionado con la libertad de expresión¹³⁸. En algunos países también ha prevalecido el principio de neutralidad de la red y se considera que la supresión de la lista o la desindexación lo socavan¹³⁹.

La forma precisa de cualquier derecho al olvido, ya sea que se trate de suprimir de la lista, de desindexar o incluso de eliminar, parece no haber sido explicada de manera coherente en la región, y la división entre las partes interesadas encuestadas parece ser un reflejo de ello.

B. Seguridad

1. Es necesario aumentar la coordinación de la ciberseguridad para hacer frente a incidentes de alcance generalizado en la región

América Latina y el Caribe siempre ha debido enfrentar problemas de seguridad a distinto nivel, ya sea personal, institucional o relacionado con la seguridad nacional. Si bien la aparición de Internet no supuso un cambio radical en este aspecto, sí cambió el panorama de la seguridad. El ciberespacio se ha convertido en otro territorio en el que es necesario brindar protección y en el que se pueden cometer delitos.

El creciente nivel de interconexión entre los mundos dentro y fuera de Internet, en particular con la llamada “Internet de las cosas”, hace que las cuestiones vinculadas a la seguridad cobren aún más relevancia. Al tiempo que en América Latina y el Caribe se registran cada vez más incidentes vinculados a la ciberseguridad, la región se convirtió en un gran refugio para quienes realizan acciones de ese tipo. A esto se suma el hecho de que muchos de los servicios de Internet más populares que se utilizan en la región suelen ser extranjeros, y enormes cantidades de datos pasan a través de la región o se almacenan

¹³⁵ Las opiniones del Sistema Interamericano de Derechos Humanos pueden encontrarse en el informe *Estándares para una Internet libre, abierta e incluyente*, 2016. Véase [en línea] http://www.oas.org/es/cidh/expresion/docs/publicaciones/INTERNET_2016_ESP.pdf.

¹³⁶ R3D, “El erróneamente llamado “derecho al olvido” no es un derecho, es una forma de censura”, 2015 [en línea] <https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura/>; Hiperderecho, “Protección de datos personales: la nueva puerta falsa de la censura”, 2016 [en línea] <http://www.hiperderecho.org/2016/07/proteccion-datos-personales-la-nueva-puerta-falsa-la-censura/>.

¹³⁷ Hay quienes lo han considerado “un insulto” a la historia de la región. Eduardo Bertoni, “The Right to Be Forgotten: An Insult to Latin American History”, 2014 [en línea] https://www.huffpost.com/entry/the-right-to-be-forgotten_b_5870664. Véase un análisis de la ex Relatora Especial para la Libertad de Expresión de la Organización de los Estados Americanos (OEA), Catalina Botero [en línea] <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf>.

¹³⁸ Esto se deduce de la manera en que los tribunales tratan estos casos. Un ejemplo es un caso brasileño que involucra a una fiscal que había sido acusada de fraude en un concurso público de admisión para el cargo de juez y posteriormente fue absuelta de todo delito. Superior Tribunal de Justicia, “Recurso especial No 1.660.168 - RJ (2014/0291777-1)”, 2018 [en línea] https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequential=1628798&num_registro=201402917771&data=20180605&formato=PDF. Otro ejemplo puede encontrarse en México [en línea] http://sise.cif.gob.mx/SVP/word1.aspx?arch=1100/1100000188593240001001.docx_0&sec=_Mercedes__Santos_Gonz%C3%A1lez&svp=1 [https://perma.cc/N8LW-9ZBZ].

¹³⁹ Colombia, Corte Constitucional, “Sentencia N° T-277 de 2015. Acción de tutela instaurada por Gloria contra la Casa Editorial El Tiempo”, 12 de mayo de 2015 [en línea] <https://perma.cc/KF4Q-VW6S>.

fuera de ella, principalmente en países de mayor desarrollo. Esto genera problemas transfronterizos que van desde dificultades para determinar la ubicación del delito cibernético hasta el acceso a las pruebas, el control de las normas de seguridad de los datos y las cuestiones relativas a la vigilancia.

Una de las partes encuestadas remarcó cómo la necesidad de acelerar el acceso a los datos y resolver los incidentes de ciberseguridad chocaba con la soberanía jurisdiccional y las identidades jurídicas nacionales. Un gran número de interesados destacó la enorme importancia de la cooperación internacional en esos problemas transfronterizos para hacer frente a este desafío.

2. Investigaciones transfronterizas y pruebas electrónicas

La corrupción no es una característica de la vida de América Latina y el Caribe por la que la región se enorgullece de ser conocida. En las dos últimas décadas, los escándalos han pasado de ser casos aislados relacionados principalmente con asuntos internos a esquemas organizados, algunos de los cuales abarcan más de una o incluso varias jurisdicciones. Un ejemplo destacado ha sido la Operación Lava Jato, que comenzó como una investigación en el Brasil y terminó dejando al descubierto sofisticados mecanismos en muchísimos países. La empresa Odebrecht, por ejemplo, ha sido objeto de investigaciones en varios países de la región, y hay expresidentes o vicepresidentes de al menos cinco países presos o que están siendo investigados. También se está investigando a varios encumbrados políticos de otros países¹⁴⁰.

Estos esquemas de corrupción que abarcan múltiples jurisdicciones dieron lugar a investigaciones que han exigido la cooperación transfronteriza de agentes encargados de hacer cumplir la ley y de otros varios agentes, con importantes debates jurisdiccionales. Tal vez el más destacado sea el acceso a pruebas digitales en distintas jurisdicciones y la necesidad de reformar los instrumentos de cooperación internacional que ofrecen mecanismos tanto de conservación como de acceso a pruebas electrónicas a través de las fronteras.

2.1. El acceso a pruebas digitales en múltiples jurisdicciones

En el curso de una investigación en varias jurisdicciones, los organismos encargados de hacer cumplir la ley deben tener acceso a información que pueda estar ubicada en otro país, quizás porque se realizan acciones en distintas jurisdicciones. Por ejemplo, una empresa podría transferir fondos a la cuenta off-shore de un funcionario corrupto o presuntos delincuentes podrían usar servicios de Internet que almacenan datos en el extranjero gestionados por servicios en la nube. Las pruebas obtenidas en una investigación pueden ser pertinentes para otra y, en algunos casos, las investigaciones de un caso de corrupción en el extranjero pueden repercutir en la seguridad de una investigación en otro país¹⁴¹.

El hecho de que algunos datos relevantes puedan tener conexión con otros países crea una serie de problemas jurisdiccionales. Sin embargo, es importante señalar que existe una distinción entre la jurisdicción sobre un delito propiamente dicho y la jurisdicción sobre las pruebas necesarias para investigar ese delito.

En cuanto a la jurisdicción sobre las pruebas, todavía hay varios puntos en discusión. En primer lugar, puede haber una controversia sobre el factor de conexión necesario para determinar la jurisdicción sobre las pruebas digitales. El elemento de conexión más común tradicionalmente ha sido la ubicación de las pruebas. Esto trae aparejadas al menos dos dificultades. Debido a su naturaleza digital y a su posible fluidez, las pruebas digitales (datos) pueden dividirse entre distintas jurisdicciones o transferirse a otro lugar sin ningún tipo de aviso o esfuerzo. Los servicios en la nube realizan ambas cosas: dividen paquetes de información y los mueven constantemente entre distintos servidores que pueden encontrarse, y por lo general se encuentran, en diferentes jurisdicciones.

La ubicación de los datos no es el único factor de conexión posible. Puede haber otros, como la nacionalidad, el domicilio o la residencia habitual de la persona a la que corresponden los datos, o el lugar de establecimiento de la empresa que posee los datos.

Además, el éxito de cualquier solicitud para poder acceder a los datos almacenados en el extranjero puede depender de la cooperación con el país en el que se encuentren dichos datos. Por lo general también ocurre que las solicitudes nacionales y extranjeras están sujetas a diferentes criterios y procedimientos, por lo que la validez y exigibilidad de una solicitud extranjera para la presentación de pruebas puede ser objeto de controversia.

¹⁴⁰ Véase un resumen del escándalo de corrupción [en línea] <https://www.bbc.com/news/world-latin-america-41109132>.

¹⁴¹ Véase un análisis de la interconexión de la corrupción, el soborno por personas extranjeras y el acceso a información y pruebas [en línea] <http://www.oecd.org/daf/anti-bribery/TypologyMLA2012.pdf>.

Por último, los países pueden imponer bloqueos que no permitan la comunicación internacional de datos, salvo en determinadas circunstancias y mediante procedimientos específicos. Algunas leyes de protección de datos, por ejemplo, bloquean las transferencias sin una orden o un consentimiento nacional.

Estas cuestiones suelen plantear una serie de retos a los agentes encargados de hacer cumplir la ley. El acceso a las pruebas de un delito cometido en el país A por ciudadanos del país A cuyas víctimas se encuentran también en el país A puede depender de un procedimiento internacional simplemente porque los datos probatorios pertinentes se almacenan fuera de ese país.

Algunos de los interesados encuestados destacaron la importancia del acceso a las pruebas almacenadas en el extranjero para las investigaciones penales y la necesidad de cooperación e intercambio de información. También señalaron que los procesos internacionales pueden ser engorrosos y no adaptarse necesariamente a la urgencia y rapidez de las investigaciones de hoy, lo que apunta a la necesidad de un cambio de paradigma en la región.

En el caso de la multinacional brasileña Odebrecht, el Departamento de Justicia de los Estados Unidos llegó a un acuerdo con la empresa para vigilar el cumplimiento de la legislación anticorrupción. El acuerdo abarcaba el intercambio de información con una organización de vigilancia y el Departamento de Justicia, incluido el requisito de transferir información (datos personales, entre otras cosas) no en el contexto de la investigación sino una vez que esta concluya, para prevenir futuras acciones ilegales¹⁴².

2.2. El sistema de asistencia judicial recíproca debe adaptarse a la era digital

La forma tradicional de solicitar pruebas extraterritoriales es a través de la cooperación internacional. Existe una red de acuerdos internacionales que prevén procedimientos jurídicos para facilitar la asistencia y la cooperación a través de las fronteras.

Los más comunes, sin duda, son los tratados de asistencia judicial recíproca. Los Estados de la región son partes en varios tratados bilaterales y multilaterales de asistencia judicial recíproca, tanto de alcance mundial como regional. La Convención Interamericana sobre Asistencia Mutua en Materia Penal (1992), por ejemplo, cuenta entre sus miembros a 26 países de América Latina y el Caribe¹⁴³. Otras convenciones específicas se refieren a la asistencia judicial recíproca y a la necesidad de cooperación internacional en esos temas. Todos los países de la región, excepto Cuba, son partes en el artículo XIV de la Convención Interamericana contra la Corrupción (1996)¹⁴⁴.

El sistema de tratados de asistencia judicial recíproca supone un adelanto respecto del uso tradicional de la cooperación diplomática y los exhortos, pero tiene sus propias dificultades. Depende de que los países sean partes en los tratados de asistencia judicial recíproca, y los procedimientos no son uniformes, ya que pueden variar de un acuerdo a otro¹⁴⁵. Además, los sistemas administrativos fueron diseñados para trabajar con solicitudes procedentes del exterior de manera excepcional; no fueron pensados para tratar con grandes volúmenes de solicitudes de este tipo. La falta de automatización y escalabilidad hace que esos procedimientos puedan no ser completarse a tiempo. Entretanto, las investigaciones pueden estancarse, puede no encontrarse a los posibles culpables, que pueden permanecer prófugos, puede haber delitos como consecuencia de otros y las pruebas pueden trasladarse (a otra jurisdicción) o destruirse.

Muchos países de la región creen que hay que reformar el sistema de asistencia judicial recíproca¹⁴⁶. La mayoría de los interesados encuestados también están de acuerdo en que es necesario incorporar procedimientos más ágiles en los acuerdos de cooperación internacional. Algunos advirtieron, sin embargo, que los procedimientos deben respetar las debidas garantías procesales, la privacidad de los datos y los derechos humanos en general. Un interesado destacó la necesidad de garantizar la autenticidad de los documentos y la credibilidad de quienes formulan la solicitud.

¹⁴² Véase [en línea] <https://globalinvestigationsreview.com/article/1139256/us-and-brazil-agree-local-odebrecht-monitors>. Véase también [en línea] <https://www.justice.gov/opa/press-release/file/919916/download>.

¹⁴³ Véase [en línea] <https://www.oas.org/juridico/spanish/tratados/a-55.html> La Convención tiene un protocolo en el que son partes muchos menos países [en línea] <http://www.oas.org/juridico/english/treaties/a-59.html>.

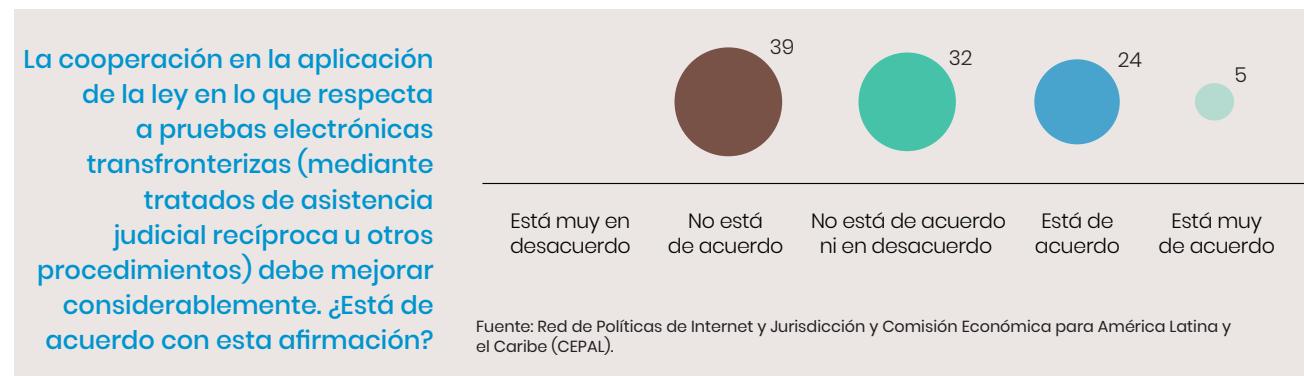
¹⁴⁴ Véase [en línea] http://www.oas.org/es-sla/dci/tratados_multilaterales_interamericanos_B-58_contra_Corrupcion.asp.

¹⁴⁵ Véase [en línea] <https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests>.

¹⁴⁶ Información presentada por los Estados de América Latina y el Caribe a la Oficina de las Naciones Unidas contra la Drogas y el Delito (UNODC). Véase [en línea] <https://undocs.org/es/A/74/130>.

En general, los interesados no abogan por la revisión general del sistema de asistencia judicial recíproca, sino que apoyan su adaptación a la era digital. Consideran que la mayoría de los problemas se deben a que las empresas de Internet se encuentran establecidas en el extranjero y tienen presencia a nivel nacional. Sus sugerencias suelen orientarse hacia un mecanismo de solicitudes directas a esas empresas (en tanto titulares de datos).

Hay poco consenso, no obstante, en torno al instrumento que se debe utilizar para la reforma. Debido a su naturaleza bilateral o multilateral, la negociación de los tratados de asistencia judicial recíproca suele llevar tiempo, y es posible que estos instrumentos no abarquen todas las necesidades de acceso a la información y su conservación. Mientras tanto, los países están buscando soluciones, ya sea de manera unilateral o en grupos con ideas afines.



2.3. La contribución del Convenio sobre la Ciberdelincuencia a las investigaciones transfronterizas

Varios Estados de América Latina y el Caribe son partes o se han sumado al Convenio sobre la Ciberdelincuencia del Consejo de Europa de 2001 que, entre otras cosas, establece mecanismos de cooperación internacional en materia de ciberdelincuencia¹⁴⁷. La Argentina, Chile, Colombia, Costa Rica, Guatemala, México, Panamá, el Paraguay, el Perú y la República Dominicana son partes del Convenio, en tanto que el Brasil fue invitado a adherir en diciembre de 2019¹⁴⁸. El Convenio prevé acciones más expeditivas para mejorar el acceso y la conservación de las pruebas.

Las partes entrevistadas y encuestadas opinaron que, si bien el Convenio sobre la Ciberdelincuencia no resolvía los problemas relativos al sistema de asistencia judicial recíproca, era un paso en la dirección correcta. Uno de los interesados señaló que participar en el Convenio sobre la Ciberdelincuencia suponía poder acceder a un importante foro de debate sobre los obstáculos a la hora de acceder a pruebas digitales.

Los miembros del Convenio se encuentran debatiendo un protocolo adicional¹⁴⁹ que proporcionará herramientas más específicas para crear un sistema más integral y expeditivo, especialmente en lo que respecta a los datos de los abonados almacenados en los servicios en la nube¹⁵⁰. Una de las principales dificultades, no obstante, es establecer una base de referencia común con respecto a la privacidad y otros derechos humanos. Algunos de los encuestados expresaron esta preocupación.

2.4. Búsqueda de alternativas al sistema de tratados de asistencia judicial recíproca fuera de la región

Debido a que los procesos internacionales aún no han alcanzado su plena madurez, varios países han puesto en marcha iniciativas unilaterales para reformar su sistema jurídico. Una de las principales soluciones ha sido proporcionar facultades jurídicas para solicitar el acceso directo a los datos a quienes los poseen, en particular los proveedores de servicios de Internet.

¹⁴⁷ Véase [en línea] <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

¹⁴⁸ Consejo de Europa, "Budapest Convention: Brazil invited to accede", 2019, available at <https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede>.

¹⁴⁹ Véase [en línea] <https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>.

¹⁵⁰ En un estudio de la UNODC, los miembros de América Latina y el Caribe mencionaron la actualización del Convenio sobre la Ciberdelincuencia como una posible solución. Véase [en línea] <https://undocs.org/es/A/74/130>.

En los Estados Unidos se aprobó la Ley CLOUD (ley aclaratoria del uso legal de datos en el extranjero), que prevé un mecanismo para que los organismos encargados de hacer cumplir la ley en los países que tienen un acuerdo bilateral específico con este país puedan pedir directamente a las empresas que proporcionen los datos. En esta Ley se aclara que la jurisdicción sobre las pruebas digitales se basa en la nacionalidad o la residencia de la persona a la que corresponden los datos (cliente del proveedor de servicios de Internet). En las directrices del Departamento de Justicia de los Estados Unidos se estipula que se puede solicitar a los proveedores nacionales de servicios de Internet que presenten los datos que posean, independientemente de su ubicación¹⁵¹.

La Unión Europea, por su parte, lanzó una iniciativa denominada e-Evidence, que consiste en un proyecto de reglamento que crearía órdenes ejecutivas para la conservación y el acceso a pruebas digitales que se envían directamente a los prestadores que brindan servicios de Internet en la Unión Europea, sin importar la ubicación de los datos. Además, se exigiría a los proveedores de servicios de Internet extranjeros que designaran un representante legal en la Unión Europea para recibir esas decisiones y órdenes¹⁵².

En ambos proyectos se reconoce que la cooperación internacional sigue siendo necesaria. Los proveedores de servicios de Internet pueden estar sujetos a leyes de terceros países que les impidan presentar las pruebas, por lo que se necesitan procedimientos especiales para garantizar el acceso a ellas. La Ley CLOUD autoriza al Presidente a negociar con los países que cumplan determinados criterios de protección de la privacidad y los derechos para llegar a acuerdos en forma simplificada que puedan facilitar la cooperación directa, permitiendo que las solicitudes se dirijan a las entidades que poseen los datos. El 5 de febrero de 2019 se dio a la Comisión Europea un mandato de doble vía para iniciar negociaciones sobre el acceso transfronterizo a las pruebas digitales con los Estados Unidos y en el contexto del mencionado protocolo adicional del Convenio sobre la Ciberdelincuencia¹⁵³.

Los entrevistados han mencionado la adhesión al Convenio sobre la Ciberdelincuencia (2001) como una forma de avanzar, aunque también destacaron que eso no resolvía todos los problemas. Los agentes encargados del cumplimiento de la ley siguen buscando formas de acceder a los datos almacenados en el extranjero. En el caso del Brasil, por ejemplo, esto se ha convertido en una discusión sobre la constitucionalidad del tratado de asistencia judicial recíproca con los Estados Unidos y se pidió al Supremo Tribunal Federal que se pronunciara sobre el asunto¹⁵⁴. El debate gira en torno a si se puede pedir a la filial nacional de un proveedor de servicios de Internet que presente pruebas que se encuentran en poder de la empresa matriz ubicada fuera del país y si el artículo 11 del Marco Civil de Internet, donde se indica que la legislación brasileña se aplica a datos recolectados en el Brasil o desde un dispositivo ubicado en ese país, proporciona una base suficiente para pasar por alto el tratado de asistencia judicial recíproca y solicitar directamente los datos almacenados en el extranjero.

3. Vigilancia

Internet puede ser un instrumento de liberación al facilitar el acceso a la información y permitir su difusión a nivel mundial. A menudo ha facilitado que las personas se comuniquen, se encuentren, intercambien ideas, unan fuerzas y obtengan acceso a diferentes tipos de bienes y servicios. Al mismo tiempo, sin embargo, Internet permite el rastreo y la localización de todas estas acciones. Valiosas colecciones de datos sobre los hábitos, gustos y movimientos de las personas se han vuelto más fáciles de obtener. El comportamiento en línea y, en cierta medida, fuera de línea también se puede trazar y hacer accesible. La vigilancia, entonces, ha resultado ser una realidad que hay que enfrentar, y no solo desde el punto de vista de sistemas de vigilancia o inteligencia muy sofisticados. Tanto el sector público como el privado son capaces de vigilar a la población (en la actualidad quizás incluso más las empresas que las administraciones estatales).

¹⁵¹ Véase [en línea] <https://www.justice.gov/opa/press-release/file/1153446/download>.

¹⁵² Véase [en línea] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en. Véase información más directa en Comisión Europea, "Propuesta de reglamento del Parlamento Europeo y del Consejo sobre las órdenes europeas de entrega y conservación de pruebas electrónicas a efectos de enjuiciamiento penal" (COM(2018) 225 final), 17 de abril de 2018 [en línea] <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52018PC0225&from=ES>; y "Propuesta de directiva del Parlamento Europeo y del Consejo por la que se establecen normas armonizadas para la designación de representantes legales a efectos de recabar pruebas para procesos penales" (COM(2018) 226 final), 17 de abril de 2018 [en línea] <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:52018PC0226&from=EN>.

¹⁵³ Véase [en línea] https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en.

¹⁵⁴ Brasil, Supremo Tribunal Federal, "Ação direta de constitucionalidade", Nº 51 [en línea] <http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>.

Estos dos lados de Internet tienden a ser difíciles de reconciliar. Iniciativas importantes pueden conducir, de manera deliberada o involuntaria, a la vigilancia. Muchos sistemas de seguridad social y de prestaciones sociales se basan en el análisis de datos y en la formulación de políticas públicas basadas en datos. Hacer más eficiente la asignación de recursos, reducir el fraude y encontrar y distribuir bienes y servicios a quienes los necesitan o merecen, y se ajustan a los criterios, son objetivos muy importantes, y todos pueden lograrse mejor con más datos y una mejor supervisión y análisis.

La otra cara de esta mayor eficiencia es que los instrumentos utilizados para lograrla también pueden utilizarse para la vigilancia. Existe un alto riesgo de que la reunión de esos datos pueda vulnerar muchos derechos fundamentales y de que esa riqueza de información se utilice de manera indebida o para discriminar, perseguir o dejar a los más vulnerables en una situación aún peor que la que tenían antes.

En América Latina y el Caribe se han registrado casos en los que se han reunido grandes cantidades de datos personales en el marco de programas sociales, acuerdos de transporte público e incluso actos populares. El impacto en línea de la pandemia ha potenciado esta tendencia¹⁵⁵. Esos datos suelen recopilarse haciendo hincapié en los sectores marginales y más vulnerables de la población. Esto puede dar lugar a exclusión, trato desigual e incluso discriminación, aparte del riesgo de que se produzcan violaciones de los datos¹⁵⁶. En la región, ciertos grupos, entre los que se encuentran periodistas y defensores de los derechos humanos, así como activistas políticos y artistas, también suelen correr un riesgo particularmente alto en relación con la vigilancia¹⁵⁷.

Otra cuestión se refiere al uso de tecnologías en áreas públicas. Muchos países de América Latina y el Caribe están considerando la posibilidad de implantar sistemas de reconocimiento facial en calles y parques, así como en actos públicos¹⁵⁸. El objetivo es frenar el crimen y mejorar la seguridad pública. Sin embargo, la tecnología puede afectar otros derechos, como la libertad de expresión y de reunión, el derecho a la protesta y la privacidad¹⁵⁹.

La vigilancia suele analizarse desde una perspectiva nacional, pero en América Latina y el Caribe las repercusiones transfronterizas son claramente visibles. En varios casos, los instrumentos que se utilizan para reunir y analizar datos o que están detrás de tecnologías como el reconocimiento facial se implementan mediante alianzas público-privadas, principalmente con empresas multinacionales. Por consiguiente, la tecnología empleada con frecuencia es extranjera, los servidores en que se almacenan los datos (por lo general, servicios en la nube) suelen estar fuera de la región y los países vecinos es habitual que reciban ofertas similares o que compitan por los mismos servicios. Con cierta frecuencia, entonces, se producirán choques jurisdiccionales transnacionales.

3.1. Cifrado

Cuanto más se pasa a ofrecer servicios en línea, más clara se vuelve la necesidad de seguridad. El cifrado es una pieza del rompecabezas de la seguridad. Una enorme cantidad de servicios de Internet dependen del cifrado para su fiabilidad¹⁶⁰. Las transacciones bancarias y financieras son las primeras que vienen a la mente, pero hay otras, como abrir una casa, acceder a las cámaras, compartir información delicada e incluso reservar un viaje. La pandemia ha puesto de manifiesto la necesidad de cifrar los intercambios con los médicos, los hospitales y la telemedicina¹⁶¹. El cifrado es una piedra angular y, en cierta medida, un requisito previo para todas esas relaciones en línea.

El uso del cifrado, sin embargo, ha tenido un impacto en otras áreas. Puede ocultar información relevante a los agentes de inteligencia y aquellos encargados de hacer cumplir la ley, y crear, de esta

¹⁵⁵ Véase [en línea] https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf.

¹⁵⁶ Véase [en línea] <https://www.derechosdigitales.org/13921/vigilancia-control-social-e-desigualdade-a-tecnologia-reforca-vulnerabilidades-estruturais-na-america-latina/>.

¹⁵⁷ Véase [en línea] http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_22_violencia_esp_web.pdf.

¹⁵⁸ Varios países tienen iniciativas de este tipo. Entre ellos se incluyen: Argentina (véase [en línea] https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf); Brasil (véase [en línea] <https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml>); Chile (véase [en línea] <https://www.infodefensa.com/latam/2020/04/08/noticia-ingresmart-implementara-chile-sistema-teleproteccion-camaras.htm>); Paraguay (véase [en línea] <https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/#sdfootnote1sym>), y El Salvador, Honduras y Nicaragua (véase [en línea] https://acceso.or.cr/assets/files/Art_Herramientas_Vigilancia_CA-mayo2020.pdf). Véase una reseña de las iniciativas en la región [en línea] <https://reconocimientofacial.info>.

¹⁵⁹ Al Sur, "New technologies and their impact on the promotion and protection of human rights in the context of assemblies and peaceful protests: The situation of Latin America", octubre de 2019 [en línea] https://adc.org.ar/wp-content/uploads/2019/10/AL-SUR_Contribution_New-technologies-in-the-context-of-assemblies-and-peaceful-protests.pdf.

¹⁶⁰ R. Polk y A. Froncek, "Your day with encryption", Internet Society, 2019 [en línea] <https://www.internetsociety.org/blog/2019/10/your-day-with-encryption/>.

¹⁶¹ Véase una reseña en D. Rozario, "Secure health care messaging in the era of COVID-19", IAPP, agosto de 2020 [en línea] <https://iapp.org/news/a/secure-health-care-messaging-in-the-era-of-covid-19/>.

forma, una tensión entre el uso del cifrado para proteger la privacidad y otros derechos fundamentales muy importantes, por una parte, y la seguridad pública, por la otra. Se argumenta que el Estado debe tener acceso a la información que se comparte, incluso cuando está cifrada, a fin de resguardar a la población de los delincuentes, los terroristas y otras fuentes de peligro. De lo contrario, el cifrado actúa como una barrera para este trabajo legítimo y protege a los culpables, a los que intentan subvertir el orden y causar daño.

Esta tensión ha dado lugar a un debate técnico, jurídico y ético que aún no se ha resuelto de manera definitiva. Ambas partes tienen puntos válidos, y encontrar el equilibrio adecuado entre mantener el cifrado para muchos propósitos diferentes y permitir el acceso a los datos pertinentes por motivos de seguridad nacional y seguridad pública no es una tarea fácil. En América Latina y el Caribe, el debate ha surgido de diferentes formas: los organismos encargados de hacer cumplir la ley exigen el acceso a los datos (en particular de aplicaciones de mensajería) a pesar del cifrado, ordenan la recopilación de más información (con posibles repercusiones en los protocolos de cifrado) y solicitan la instalación de un acceso por la puerta trasera (similar a las escuchas telefónicas).

3.2. Acceso de los organismos encargados de hacer cumplir la ley a la información y los mensajes cifrados

El acceso a información y mensajes cifrados con el propósito de aplicar la ley puede solicitarse de diferentes maneras. Los gobiernos pueden ordenar a las empresas que crean mecanismos de cifrado que proporcionen una clave maestra para que, en determinadas condiciones, puedan acceder a toda la información necesaria¹⁶². La Administración pública puede informar a las empresas con acceso a mensajes cifrados de que necesita divulgar esta información de forma no cifrada, sin considerar cómo se va a llevar a cabo el descifrado.

Desde el punto de vista de la aplicación de la ley, la situación en América Latina y el Caribe es que durante una investigación, y con la debida causa, los agentes pueden pedir a las empresas y los particulares que divulguen información. El uso —o no— del cifrado no es necesariamente una cuestión que aborde el sistema jurídico. En la inmensa mayoría de los casos, se entiende que si una empresa presta el servicio en un país, tiene que cumplir con las órdenes válidas emitidas por los organismos encargados de hacer cumplir la ley en ese país y, en particular, por las autoridades judiciales.

Debido a la forma en que se han desarrollado los protocolos de cifrado, las empresas intermedias no siempre están en condiciones de proporcionar esa información, ya sea porque ya no la poseen (su arquitectura no prevé el almacenamiento de mensajes cifrados) o porque no tienen acceso a la clave de descifrado (en el caso del cifrado de extremo a extremo, la clave privada suele estar en los dispositivos que intercambian información y no está a disposición de la empresa intermedia)¹⁶³.

Esto puede llevar a situaciones difíciles, como ha sucedido en la región. El uso del cifrado se ha vuelto polémico, y los proveedores de servicios de Internet se han visto atrapados en el fuego cruzado¹⁶⁴. Algunas aplicaciones han sido bloqueadas por orden judicial y los empleados de ciertas empresas incluso han tenido que enfrentar penas de cárcel por desobedecer las órdenes de entregar mensajes (esto se analiza con más detalle en la sección III.B.4).

3.3. Un difícil debate en torno al anonimato

La región tradicionalmente ha luchado con la idea del anonimato. Existe la idea de que está muy cerca de la impunidad, y los instrumentos que permiten el discurso anónimo tienden a ser mal vistos. El uso de máscaras o dispositivos similares durante las protestas es un ejemplo¹⁶⁵. Del mismo modo, las aplicaciones que permiten la mensajería anónima han sido impugnadas dentro y fuera de los tribunales¹⁶⁶.

¹⁶² H. Abelson y otros, *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications*, Massachusetts Institute of Technology (MIT), 2015 [en línea] <http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>.

¹⁶³ K. Ermoshina, F. Musiani y H. Halpin "End-to-end encrypted messaging protocols: an overview", *International Conference on Internet Science*, 2016 [en línea] https://link.springer.com/chapter/10.1007%2F978-3-319-45982-0_22.

¹⁶⁴ Véase [en línea] http://www2.stf.us.br/portalStf/internacional/cms/destaquesClipping.php?sigla=portalStfDestaque_en_us&idConteudo=330687.

¹⁶⁵ Véase [en línea] <https://www.derechosdigitales.org/wp-content/uploads/freedom-of-expression-encryption-and-anonymity.pdf>.

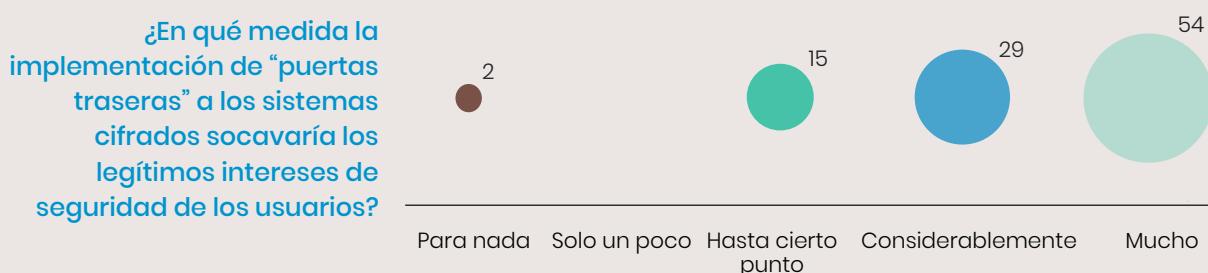
¹⁶⁶ Tech Crunch, "Brazil Court Issues Injunction Against Secret and Calls for App to Be Remotely Wiped", 2014 [en línea] <http://techcrunch.com/2014/08/20/brazil-court-issues-injunction-against-secret-and-calls-for-app-to-be-remotely-wiped/>.

La capacidad de intercambiar mensajes en una larga cadena, aunque no se trate de un discurso anónimo en sí, suele generar una situación en la que puede resultar difícil encontrar el origen o la fuente de un mensaje específico. Esto parece ser particularmente grave en el contexto de las campañas de información errónea, y potencialmente peor durante las elecciones¹⁶⁷. En el Brasil, por ejemplo, actualmente se estudia en el Congreso Nacional un proyecto de ley que ordena la recopilación de información sobre todos los mensajes que se vuelven “virales” (reenviados más de 1.000 veces)¹⁶⁸. Los servicios de mensajería estarían obligados a rastrear la fuente de esos mensajes, de modo que si su contenido causa daño o se considera delictivo, será más fácil identificar al culpable. No solo la ley exigiría la retención de datos personales no esenciales, sino que los expertos afirman que los protocolos de cifrado utilizados por los servicios podrían debilitarse si se cumplieran los requisitos del proyecto de ley¹⁶⁹.

La situación es indudablemente difícil y exige un análisis cuidadoso para determinar si se trata de una respuesta proporcional o si puede haber otras medidas disponibles que no entrañen los mismos riesgos. El Sistema Interamericano de Derechos Humanos ha subrayado la importancia de que las respuestas a los problemas relacionados con el acceso a la información con fines de aplicación de la ley y la información errónea salvaguarden y no socaven “la integridad de los sistemas informáticos sobre los que funciona Internet y de las comunicaciones que se canalizan a través de la red”, incluidos sus protocolos de cifrado¹⁷⁰.

3.4. Las “puertas traseras” se perciben como una forma de socavar la confianza en los sistemas cifrados

Las partes interesadas que participaron en la encuesta se manifestaron claramente en contra de la inserción de puertas traseras en los sistemas encriptados. Cuando se les preguntó si esa característica socavaría los intereses legítimos de seguridad de los usuarios, el 82,93% respondió que sí.



Fuente: Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL).

Esto es importante porque los agentes encargados de hacer cumplir la ley en los países de América Latina y el Caribe están presionando para que haya una manera de descifrar el contenido de los mensajes que se envían a través de aplicaciones de mensajería instantánea. A medida que aplicaciones como WhatsApp se vuelven cada vez más populares en la región, aumenta la presión para frenar el cifrado de extremo a extremo y permitir algún tipo de acceso al contenido de los mensajes para investigaciones penales.

Es importante mencionar que el cifrado es un factor clave para la confianza, no solo en las aplicaciones de mensajería, sino también en el comercio electrónico, la banca por Internet y todo tipo de actividades en línea. Romper el cifrado para un usuario puede significar romperlo también para todos los demás. Al mismo tiempo, existen otras formas de acceder al contenido de un mensaje en una investigación debidamente autorizada, incluso en el caso de aplicaciones de mensajería instantánea encriptada de extremo a extremo, sin dañar la integridad de los sistemas encriptados. Se podría, por ejemplo,

¹⁶⁷ Véase [en línea] <https://en.ejo.ch/specialist-journalism/mexicos-election-and-the-fight-against-disinformation>.

¹⁶⁸ La región no está sola, ya que se informa de que en la India se han sugerido medidas similares. Véase [en línea] <https://www.policyforum.net/encryption-and-attribution-indias-fake-news-problem/>.

¹⁶⁹ Véase [en línea] <https://www1.folha.uol.com.br/poder/2020/08/veja-dez-razoes-para-rejeitar-artigo-10-do-projeto-sobre-fake-news-que-rastreia-mensagens.shtml>. Véase también [en línea] <https://www.eff.org/deeplinks/2020/06/current-brazils-fake-news-bill-would-dismantle-crucial-rights-online-and-fast>.

¹⁷⁰ Véase [en línea] https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf.

acceder al dispositivo real utilizado para la comunicación (como puede ser un teléfono celular) o lograr que los agentes encargados de hacer cumplir la ley se infiltren en los grupos de mensajería.

Los organismos encargados de hacer cumplir la ley en la región se encuentran analizando distintas alternativas mientras el debate jurídico sobre el cifrado va madurando¹⁷¹. Los datos disponibles —metadatos o datos de otras fuentes— pueden aprovecharse para encontrar las respuestas necesarias. El uso de estrategias modernas de investigación es primordial para equilibrar el debate y preservar la seguridad nacional y la seguridad pública, al tiempo que se mantienen controladas las violaciones de la privacidad, las amenazas a la ciberseguridad y la vigilancia ilegítima, extranjera o de otro tipo.

Estas situaciones pueden parecer una cuestión interna, pero tienen repercusiones transfronterizas que incluso pueden llegar a ser internacionales. La mayoría de los servicios cifrados tienen un alcance mundial y se utilizan en múltiples jurisdicciones. Si se socava el cifrado en beneficio del cumplimiento de la ley en un país, es muy posible que esto tenga un efecto en todos los demás. Puede haber un efecto de cascada no solo para las personas que viven en países democráticos en los que se respetan los derechos humanos, sino también para los defensores de los derechos humanos en regímenes más autoritarios. Otro aspecto a considerar es que un número importante de empresas que ofrecen servicios con cifrado integrado pueden estar en realidad utilizando protocolos internacionales o interfaces de programación de aplicaciones de otras empresas, nacionales o extranjeras, de modo que el impacto puede ir más allá del proveedor directo del servicio.

Dondequiera que tenga lugar el debate, es importante tener en cuenta la complejidad de los derechos e intereses que se están equilibrando, y el hecho de que cualquier acuerdo que se alcance podría tener un impacto más allá del país que lo aplica y podría afectar a todos los grupos, incluidos los vulnerables.

La computación cuántica y el cifrado

El cifrado depende de la dificultad y el tiempo que se necesite para encontrar la combinación para descifrar cualquier mensaje. En otras palabras, el cifrado solo funciona porque forzar la cerradura es difícil y lleva mucho tiempo. Las tecnologías más nuevas, como la computación cuántica, que aumentan la velocidad de los cálculos, pueden tener un efecto doble: crear cifrados que son aún más difíciles de romper y volver inútiles a nivel global los sistemas disponibles hasta el momento¹⁷². Si bien es probable que todavía se necesiten muchos avances para poder contar con computadoras cuánticas que funcionen, el mero concepto ayuda a subrayar la importancia del cifrado y la forma en que una sola clave, o un solo cambio tecnológico, tiene el potencial de causar estragos y poner en peligro cualquier número de transacciones vitales.

4. Ciberseguridad

La importancia de asegurar el ciberespacio ha aumentado de manera exponencial en los últimos años. La pandemia ha puesto de relieve la creciente dependencia tecnológica de la infraestructura y los servicios básicos de los países, como la energía, el agua, el saneamiento, el transporte de alimentos y las cadenas de suministro, las transacciones financieras, los servicios públicos e incluso el funcionamiento de los procedimientos gubernamentales. Todos esos servicios son objetivos centrales de los ciberataques.

Varios incidentes ciberneticos de magnitud se han originado en Estados de América Latina y el Caribe o han tenido como objetivo víctimas de esos Estados¹⁷³. Esos incidentes no han hecho más que aumentar con la expansión de la conectividad y del número de personas que acceden a Internet. La ciberdelincuencia por motivos económicos, que implica el uso de programas maliciosos y fraude con tarjetas de crédito y banca en línea, suele figurar entre las principales amenazas en América Latina y el Caribe, lo que supone que la seguridad pública y nacional está estrechamente relacionada con la ciberseguridad¹⁷⁴. Sin embargo, aún son varios los países de la región que solo disponen de una gama limitada de instrumentos, capacidades e instituciones para prepararse para los ataques, identificarlos y responder¹⁷⁵.

¹⁷¹ Véase [en línea] <https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219>.

¹⁷² Véase [en línea] <https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985>.

¹⁷³ Norton, "2017 Cyber Security Insights Report. Global Results", 2017 [en línea] <https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf>.

¹⁷⁴ "ThreatMetrix Cybercrime Report: An Interview", noviembre de 2019 [en línea] <https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/>.

¹⁷⁵ Organización de los Estados Americanos (OEA)/Banco Interamericano de Desarrollo (BID), *Reporte Ciberseguridad 2020* [en línea] <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>.

Cada vez más incidentes ciberneticos han cruzado las fronteras en los últimos tiempos, lo que hace que para su resolución se necesite la cooperación y coordinación internacional. Esta capa internacional de esfuerzos ciberneticos da cuenta de la necesidad de enfoques, estándares y normas comunes, sin mencionar los recursos y la capacidad de establecer defensas y aumentar la resiliencia. Es necesario proteger no solo la infraestructura crítica, sino toda la infraestructura de información y comunicación: no solo la de un país u otro, sino la de la propia región.

Los niveles de preparación y resiliencia en la región son muy desiguales. Solo poco más de un tercio de los países cuentan con una estrategia de ciberseguridad (Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguay, República Dominicana y Trinidad y Tabago). Algunos menos (10) tienen un organismo público encargado de la gestión y coordinación de la ciberseguridad y 20 países cuentan con equipos de respuesta a incidentes de ciberseguridad, también conocidos como “equipos informáticos de respuesta de emergencia”¹⁷⁶.

Es evidente que queda mucho por hacer en lo que respecta tanto a la implementación nacional como a la cooperación internacional y regional. A nivel de los equipos informáticos de respuesta de emergencia, existe cooperación y coordinación cuando se presentan riesgos e incidentes de gran escala. CSIRTAmericas.org, una plataforma para los equipos de respuesta a incidentes de ciberseguridad dirigidos por los Gobiernos de América, sirve como herramienta de red para la alerta temprana, las alertas de ataques de denegación de servicio distribuido y la creación de capacidad¹⁷⁷. El Registro de Direcciones de Internet para América Latina y Caribe (LACNIC) también ha creado su propio equipo informático de respuesta de emergencia¹⁷⁸.

Hay mucho margen para mejorar la estructura de gobernanza de la ciberseguridad. La inclusión de los distintos interesados (no solo los gobiernos, sino también las empresas, la sociedad civil, el mundo académico y la comunidad técnica) es crucial para el sistema general, tanto para superar el “pensamiento en silos” como para garantizar un enfoque sistémico¹⁷⁹. Se trata de un proceso continuo a nivel nacional y regional. La participación de diferentes actores es una característica de los debates a nivel de la Organización de los Estados Americanos (OEA). En el marco del Comité Interamericano contra el Terrorismo (CICTE), el programa de ciberseguridad constituye un notable esfuerzo de coordinación y adopta un enfoque de múltiples interesados¹⁸⁰.

Esto también es lo que ocurre en importantes intersecciones entre los niveles regional e internacional. Por ejemplo, en las consultas regionales del Grupo de Expertos Gubernamentales sobre la Promoción del Comportamiento Responsable de los Estados en el Ciberespacio en el Contexto de la Seguridad Internacional, celebradas con la OEA, se invitó a las empresas, la sociedad civil, los círculos académicos y la comunidad técnica a formular observaciones y a participar en los debates¹⁸¹.

En el plano regional, dos instrumentos destacan la importancia de la ciberseguridad y proporcionan un marco para los compromisos comunes y la cooperación: la Declaración sobre el Fortalecimiento de la Seguridad Cibernética en las Américas (2012)¹⁸² y la Declaración sobre la Protección de Infraestructura Crítica ante las Amenazas Emergentes (2015)¹⁸³.

Las disposiciones de la legislación penal relativas a los delitos ciberneticos suelen ser otra pieza del rompecabezas. Los países de la región aún no han adaptado plenamente su legislación a las exigencias de la lucha contra la ciberdelincuencia. A nivel internacional, cinco países son partes en el Convenio sobre la Ciberdelincuencia¹⁸⁴. En este proceso de inclusión de la ciberseguridad en los programas nacionales, algunas leyes de ciberseguridad han dado lugar a restricciones de los derechos digitales. En América Latina y el Caribe se ha informado de que el proyecto de Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela reafirma amplios poderes en interés de lo que se denomina la “defensa integral” del país¹⁸⁵.

¹⁷⁶ Ibíd.

¹⁷⁷ Véase [en línea] <https://the-gfce.instantmagazine.com/magazine/global-cyber-expertise-magazine-volume-5/csirtamericasorg/overlay/strengthening-incident-response-capabilities-in-the-americas/>.

¹⁷⁸ Véase [en línea] <https://www.lacnic.net/4463/1/lacnic/lacnic-anuncia-la-constitucion-de-su-csirt>.

¹⁷⁹ Organización de los Estados Americanos (OEA)/Banco Interamericano de Desarrollo (BID). *Reporte Ciberseguridad 2020* [en línea] <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>.

¹⁸⁰ Véase [en línea] <http://www.oas.org/es/sms/cictel>.

¹⁸¹ Véase [en línea] <https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf>.

¹⁸² Véase [en línea] https://www.sites.oas.org/cyber/Documents_Declaracion%20del%20Fortalecimiento%20de%20la%20Seguridad%20en%20las%20Américas.pdf.

¹⁸³ Véase [en línea] <https://www.sites.oas.org/cyber/es/paginas/contacts.aspx>. Véase también [en línea] <https://www.oas.org/es/sms/cictel/cjreport.pdf>.

¹⁸⁴ Véase [en línea] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=XXw5lamG.

¹⁸⁵ Véase [en línea] https://freedomhouse.org/country/venezuela/freedom-net/2019#footnoteref5_7rkdmn.

Lograr el equilibrio adecuado entre promover la ciberseguridad y, al mismo tiempo, evitar las violaciones de los derechos fundamentales es una cuestión delicada y debería ser una preocupación permanente de todos los Estados de la región. Las medidas de fomento de la confianza son, por consiguiente, importantes para fortalecer la comprensión de los diferentes agentes y los desafíos que existen en los planos nacional e internacional.

4.1. Las violaciones de la seguridad han dejado al descubierto las vulnerabilidades del procesamiento de datos

Actualmente es habitual que se denuncien incidentes relacionados con la seguridad de la información y violaciones de datos. Ya se han filtrado datos sobre una gran cantidad de personas. En la mayoría de los casos, esto es consecuencia de un error humano, ya sea por no haber configurado correctamente los parámetros de seguridad, dejando espacio para que los intrusos los exploren, o por errores básicos, como el uso de contraseñas fáciles de adivinar y piratear, o incluso el acceso a programas maliciosos desde un correo electrónico o un mensaje en una computadora o dispositivo sin verificar bien su origen.

En 2019, por ejemplo, se expusieron los datos de casi todos los habitantes del Ecuador: se descubrió que en un servidor no seguro y de fácil acceso ubicado en Miami se disponía de información detallada sobre adultos y niños (incluso direcciones, relaciones de parentesco y situación financiera, así como datos sobre el empleo y la escuela)¹⁸⁶. Esto pone de relieve tanto el alcance del riesgo como su naturaleza mundial.

Los servicios digitalizados no tienen por qué respetar las fronteras. La información no necesariamente debe almacenarse y procesarse —y a menudo no se almacena ni procesa— en el país donde se recaba. Las ofertas internacionales de servicios se convierten en una destacada opción para lograr escalabilidad y eficiencia en función de los costos. Sin embargo, esos servicios pueden ser objeto de incidentes de seguridad que afectan a más de una jurisdicción.

Los casos de intrusión intencional y apropiación de información personal también se han vuelto más comunes, y van desde procedimientos simples hasta fraudes más complejos y piratería informática. El origen y la motivación de las intrusiones pueden variar mucho, desde el espionaje empresarial hasta la vigilancia de una potencia extranjera¹⁸⁷. Algunos casos pueden tener motivos en apariencia más altruistas, como la denuncia de casos de delincuencia y corrupción (en esta categoría entra el escándalo de los Papeles de Panamá)¹⁸⁸.

4.2. El desarrollo de datos biométricos e identidades digitales ha sido fuente de controversia

Los servicios están migrando al ciberespacio y se están volviendo completamente digitales. La banca es un ejemplo de un servicio en el que la mayoría de las funciones pueden funcionar en línea, sin necesidad de una presencia física. Otros servicios, incluidos los que prestan las autoridades públicas, se están estructurando de la misma manera¹⁸⁹. Esto se traduce en ganancias en escala y eficiencia. Por ejemplo, una persona de edad que recibe una pensión del Estado no tiene que presentarse necesariamente ante un funcionario para aportar una prueba de vida: hay métodos digitales que suponen un menor esfuerzo para la persona y costos más bajos para la Administración.

Este cambio, sin embargo, conlleva el desafío de autenticar la identidad de una persona: confirmar que alguien es realmente quien dice ser. Un sistema de identificación digital parece ser una forma de resolver estas dificultades y de autenticar inequívocamente a una persona. La identificación digital puede servir de llave para desbloquear el acceso a los servicios digitales, reduciendo los costos de transacción y aumentando la eficiencia¹⁹⁰.

Varios Estados de América Latina y el Caribe se encuentran estudiando la manera de instaurar formas de identidad digital. A diferencia de otras regiones del mundo, no obstante, estos países por lo general ya tienen un sistema de identidad nacional establecido¹⁹¹, lo que facilita —y a la vez complica— el

¹⁸⁶ Véase [en línea] <https://www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html>.

¹⁸⁷ Véase [en línea] <https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillance>.

¹⁸⁸ Véase [en línea] <https://www.icij.org/investigations/panama-papers/pages/panama-papers-about-the-investigation/>.

¹⁸⁹ América Latina en *United Nations E-Government Survey, 2018* [en línea] <https://www.un.org/development/desa/publications/2018-un-e-government-survey.html>.

¹⁹⁰ Banco Mundial, *Principios sobre la identificación para el desarrollo sostenible: hacia la era digital* [en línea] <http://pubdocs.worldbank.org/en/168561509656716894/web-Spanish-ID4D-IdentificationPrinciples.pdf>.

¹⁹¹ Banco Interamericano de Desarrollo (BID), "Registros civiles y oficinas de identificación: análisis y fichas de país", 2019 [en línea] <http://dx.doi.org/10.18235/0001865>.

proceso¹⁹². Los protocolos y mecanismos de seguridad disponibles no necesariamente se extienden o se ajustan bien a los requisitos de la identificación digital. Los riesgos y las preocupaciones no se alinean a la perfección. Los principales son el acceso no autorizado a los datos personales y el control de dichos datos, y las cuestiones relacionadas con la inclusión digital y la ciberseguridad¹⁹³.

Muchos de los esfuerzos que se están realizando para crear identificaciones digitales están planteando una variedad de posibles problemas transfronterizos relacionados con la forma en que estas identificaciones podrían utilizarse en línea y sus repercusiones más allá de las fronteras del país en cuestión. Se plantean inquietudes respecto de los lugares donde se almacenan los datos, los orígenes de las posibles amenazas a la ciberseguridad y la mejor manera de gestionar los mecanismos de registro, certificación y autorización¹⁹⁴. La dependencia de un proveedor, el uso de tecnología patentada, los sistemas no interoperables y los servicios en la nube (almacenamiento y procesamiento de datos a nivel internacional) también son factores importantes¹⁹⁵. Dependiendo de cómo se responda a estos desafíos, las cuestiones de eficiencia, inclusión, transparencia, seguridad, resiliencia y privacidad entrarán en juego de distinta manera¹⁹⁶.

En el caso de los acuerdos basados en la nube, por ejemplo, los datos pueden almacenarse en el extranjero y en varios lugares. El tratamiento del acceso, las transferencias de datos y los incidentes de seguridad puede tener importantes repercusiones jurisdiccionales transfronterizas que vayan más allá de las cuestiones más comunes del almacenamiento de datos del gobierno electrónico. Un ejemplo es la investigación de infracciones o delitos relacionados con esos servicios, que depende, en gran medida, de la cooperación internacional.

El hecho de que estas identidades digitales suelan ir acompañadas de atributos biométricos personales capturados electrónicamente (huellas dactilares, iris, imágenes faciales, etc.) hace que estas decisiones sean aún más significativas¹⁹⁷. Una persona no puede cancelar y volver a emitir su rostro o sus huellas dactilares si se filtran datos biométricos, como ocurriría, por ejemplo, con una tarjeta de crédito robada. Esto hace que la estructuración de esas soluciones sea una prioridad y significa que se requieren especificaciones de ciberseguridad de alto nivel por diseño.

Una última cuestión es que el reconocimiento mutuo de las identificaciones puede ser un motor de la integración regional y económica, lo que incluye un mercado único digital. Los países del Mercado Común del Sur (MERCOSUR) reconocen mutuamente sus identificaciones a los efectos migratorios, lo que constituye un primer paso. Varias iniciativas de firma electrónica han prosperado tanto en el MERCOSUR como en otros acuerdos regionales¹⁹⁸. Sin embargo, el reconocimiento de las identificaciones digitales es lo que puede liberar el mayor potencial de circulación de bienes, servicios y empresas en toda la región e impulsar la economía digital¹⁹⁹.

Varios países de la región están avanzando hacia la digitalización de sus documentos de identificación. La Argentina, por ejemplo, ha integrado su proceso en el Sistema de Identidad Digital (SID). De igual modo, el Uruguay se ha convertido en líder en materia de gobierno electrónico y ha puesto en marcha un programa de identidad digital que abarca toda la población. El Perú implementó recientemente un sistema electrónico de identidad nacional (DNI Electrónico o DNIE), que da acceso a varios servicios gubernamentales²⁰⁰. En cuanto a las aplicaciones, se informa de que, gracias al uso generalizado de las identidades digitales, las prestaciones de socorro de emergencia aprobadas por el Gobierno de Chile al principio de la pandemia se pusieron rápidamente a disposición de la población más necesitada, aunque se aplicó un fuerte mecanismo de comprobación²⁰¹.

¹⁹² Es importante señalar que los países de América Latina y el Caribe no han logrado establecer un registro universal de los nacimientos, lo que también puede representar un problema en lo que respecta a la inclusión general. Fondo de las Naciones Unidas para la Infancia (UNICEF), "Birth Registration in Latin America and the Caribbean: Closing the Gaps", 2016 [en línea] <https://data.unicef.org/resources/birth-registration-latin-america-caribbean-closing-gaps/>.

¹⁹³ McKinsey, *Digital Identification: A Key to Inclusive Growth*, 2019 [en línea] <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>.

¹⁹⁴ Véase [en línea] <https://id4d.worldbank.org/guide/hosting-options>.

¹⁹⁵ Esto ha ocurrido en otras regiones. Véase una comparación [en línea] <http://documents.worldbank.org/curated/en/15611493234231522/pdf/114628-WP-68p-TheStateofIdentificationSystemsinAfricaASynthesisofIDAssessments-PUBLIC.pdf>.

¹⁹⁶ S. Bhadra, *Five Surprisingly Consequential Decisions Governments Make About Digital Identity*, 2019 [en línea] <https://www.omidyar.com/blog/five-surprisingly-consequential-decisions-governments-make-about-digital-identity>.

¹⁹⁷ A. Gelb y J. Clark, "Identification for development: the biometrics revolution", CGD Working Paper, N° 315, Washington, D.C., Center for Global Development, 2013 [en línea] <https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315>.

¹⁹⁸ Comisión Económica para América Latina y el Caribe (CEPAL), "Mercado regional digital: aspectos estratégicos" [en línea] https://repositorio.cepal.org/bitstream/handle/11362/43476/1/S1800295_es.pdf.

¹⁹⁹ Véase [en línea] <https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0>.

²⁰⁰ Banco Interamericano de Desarrollo (BID), "Registros civiles y oficinas de identificación: análisis y fichas de país", 2019 [en línea] <http://dx.doi.org/10.18235/0001865>.

²⁰¹ Banco Mundial, "El poder de la identidad digital", 20 de agosto de 2020 [en línea] <https://blogs.worldbank.org/es/voices/el-poder-de-la-identidad-digital>.

C. Economía

1. Comercio electrónico: la aspiración de un mercado único digital

No es sorprendente que Internet haya generado un cambio de paradigma en el comercio internacional. La infraestructura comercial desarrollada a lo largo de milenios para el intercambio de bienes mediante transacciones comerciales internacionales se enfrenta a grandes retos en el esfuerzo por ajustarse a la velocidad y la variedad de transacciones que presentan las oportunidades en línea. El acceso a los mercados de bienes e incluso de servicios es cualitativa y cuantitativamente diferente en línea. Las nuevas tecnologías basadas en Internet han reducido los costos del comercio transfronterizo. Tanto los servicios como los bienes cruzan las fronteras independientemente de su volumen o valor. Con costos más bajos, las empresas de todos los tamaños pueden integrarse en la cadena de valor internacional y participar en el comercio mundial.

El hecho de que Internet no tenga sede en un país u otro significa que una persona del país A puede suministrar servicios o bienes a alguien del país B a través de una plataforma (un servicio de intermediación) que no se encuentra en ninguno de los dos países. Esto es lo que claramente ocurre en la emisión en directo de video y música, con los bienes (el comercio electrónico propiamente dicho), en los medios de información y con los servicios de finanzas, salud y otros. Este tipo de comercio internacional puede adoptar distintas formas: entre empresas (B2B), de la empresa al consumidor, de consumidor a consumidor y relaciones de los individuos y las empresas con el gobierno. El denominador común de esas transacciones es que Internet ha facilitado el acceso a los mercados más allá de las fronteras nacionales²⁰². Se está forjando un mercado diferente y completamente digital.

Sin embargo, las operaciones transfronterizas no pueden estar necesariamente sujetas a una sola jurisdicción. En otras palabras, los mercados pueden parecer globales, pero las leyes que se aplican a ellos tienden a ser locales. Los interesados que fueron encuestados señalaron que esto se aplicaba a las transacciones contractuales, los mecanismos de solución de controversias (acceso a los tribunales), la protección de los consumidores, los pagos transfronterizos (que se examinan con más detalle en la sección II.C.4), las corrientes internacionales de datos (sección II.C.6) y la legislación antimonopolio.

Con el fin de encontrar soluciones a estos problemas, algunas regiones han propuesto estrategias para armonizar las reglas y normas²⁰³. Una de las iniciativas más conocidas es el mercado único digital europeo²⁰⁴.

En América Latina y el Caribe también hay iniciativas encaminadas a facilitar el comercio digital con miras a conformar un mercado único digital regional²⁰⁵. En esta sección se examinarán las oportunidades y los retos transfronterizos de esas iniciativas y algunas de las peculiaridades de la región.

1.1. Oportunidades y desafíos para un mercado único digital regional

La digitalización ha tomado la forma de servicios públicos prestados en línea, de aplicaciones que hacen realidad lo que se denomina “Internet de las cosas” en casas, fábricas y granjas, de la automatización de procesos, y del uso a gran escala de macrodatos e inteligencia artificial para mejorar una gran variedad de actividades. La economía digital ha repercutido en los bienes y servicios más importantes para el comercio transfronterizo. Los bienes y servicios digitales ya son parte de la vida, y el acceso en línea a servicios y bienes físicos se ha convertido en cosa de todos los días. Por consiguiente, la importancia económica y social de los mercados digitales se hace sentir a todos los niveles.

Para beneficiarse plenamente de estos avances es necesario el acceso a los mercados, así como su integración o interoperabilidad. La promoción de un mercado único digital es una estrategia importante. Está ligado a la naturaleza sin fronteras de Internet, a pesar de las divisiones geográficas y jurisdiccionales, extendiendo los beneficios de un mercado digital entre los participantes. Las personas y organizaciones que residen en cualquier lugar de la región pueden ofrecer servicios y bienes a toda la región, de la misma manera que pueden buscar los servicios y bienes que deseen, independientemente de su origen.

²⁰² Véanse estimaciones sobre la posición relativa de cada tipo de comercio en el estudio de la Conferencia de las Naciones Unidas sobre Comercio y Desarrollo (UNCTAD) [en línea] [https://unctad.org/en/PublicationsLibrary/tn_uctad_ict4d06_en.pdf](https://unctad.org/en/PublicationsLibrary/tn_unctad_ict4d06_en.pdf).

²⁰³ Algunos académicos, en vez del de “armonización”, promueven el concepto de “glocalización”, combinando aspectos de distribución y acceso global de conformidad personalizada con las leyes locales. Véase A. Chander, “Glocalization and harmonization”, The Electronic Silk Road, Yale Press, 2013.

²⁰⁴ Iniciativa de la Comisión Europea, Mercado único digital europeo, véase [en línea] <https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market>.

²⁰⁵ Véase [en línea] https://repositorio.cepal.org/bitstream/handle/11362/43476/1/SI800295_es.pdf.

Esta estrategia debe incluir la integración y armonización de las normas jurídicas. La mayoría de los Estados de América Latina y el Caribe pertenecen a una o más organizaciones y acuerdos regionales relacionados con el comercio digital transnacional, como la OEA, la Comisión Económica para América Latina y el Caribe (CEPAL), la Comunidad Andina (CAN), la Comunidad del Caribe (CARICOM), la Asociación Latinoamericana de Integración (ALADI), la Cooperación Económica de Asia y el Pacífico (APEC), el Sistema de la Integración Centroamericana (SICA), el MERCOSUR, el Tratado de Libre Comercio de América del Norte (TLCAN), el Proyecto Mesoamérica, la Alianza del Pacífico y el Acuerdo de Asociación Transpacífico (TPP)²⁰⁶. Una iniciativa digna de mención es el Espacio Único de TIC de la CARICOM, que tiene por objeto facilitar la creación de un espacio digital unificado para la circulación de bienes, personas, servicios y capital²⁰⁷.

En la región, sin embargo, todavía queda mucho por hacer en lo que respecta a infraestructura común y marcos jurídicos armonizados. No existe una entidad central unificadora con capacidad para vincular a los países en distintas iniciativas. También se deja que cada jurisdicción lleve a delante, por separado, los esfuerzos vinculados a la aplicación de la ley. Esto se refleja en las opiniones de los interesados entrevistados, que indicaron que la dificultad para establecer un mercado único digital en América Latina y el Caribe radicaba en el hecho de que ninguno de los esfuerzos de integración propuestos se había llevado a cabo con éxito. Por consiguiente, las diferencias jurisdiccionales inciden en el acceso a los mercados y las oportunidades de crecimiento en la región. Un experto mencionó como los obstáculos más importantes la disparidad jurídica y económica, y la falta de normas reglamentarias comunes mínimas.

No obstante, hay algunas tendencias comunes entre los países de la región. El comercio electrónico se expande constantemente. Además, el entorno de empresas emergentes está creciendo exponencialmente en campos como la logística, el transporte, los pagos digitales y la tecnología agrícola²⁰⁸. Sin embargo, aún queda un largo camino por recorrer, en particular en lo que respecta a los acuerdos intrarregionales²⁰⁹.

Varios de los encuestados dijeron ver en la digitalización de la economía una oportunidad, pero subrayaron la necesidad de armonizar las regulaciones. Se considera que la armonización es especialmente crucial en esferas como la protección de los consumidores, la protección de los datos personales, la identidad digital, los pagos digitales, los valores negociables digitales, las normas de transporte y logística, y los régimen fiscales.

Esa percepción parece estar en sintonía con las recomendaciones de las organizaciones internacionales²¹⁰. Aún son pocas las iniciativas legislativas o reglamentarias en la región que tienen en cuenta los desafíos transfronterizos que implica la creación de un mercado digital más integrado²¹¹. Las que existen todavía tienden a organizarse desde una perspectiva nacional, lo que da lugar a una situación de considerable fragmentación, con una multiplicidad de normas.

1.2. La región cuenta con una sólida cultura de derechos del consumidor, pero con diferentes normas locales

Prácticamente todos los países de América Latina y el Caribe tienen en vigor una legislación de protección del consumidor, la mayoría en forma de una legislación específica²¹². Algunos tienen leyes específicas sobre las transacciones de consumo en línea, pero en la mayoría, el régimen estatal de protección del consumidor se ocupa principalmente de las relaciones por fuera de Internet. Esta situación crea una oportunidad para desarrollar un mercado único digital para las plataformas de Internet y el comercio electrónico en general.

²⁰⁶ Comisión Económica para América Latina y el Caribe (CEPAL), "Mercado digital regional", 2018 [en línea] https://repositorio.cepal.org/bitstream/handle/11362/43476/1/S1800295_es.pdf.

²⁰⁷ Véase [en línea] https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC_Unleashing_Internet_in_Caribbean_20170221.pdf.

²⁰⁸ Comisión Económica para América Latina y el Caribe (CEPAL), "Mercado digital regional", 2018 [en línea] https://repositorio.cepal.org/bitstream/handle/11362/43476/1/S1800295_es.pdf.

²⁰⁹ Los datos del Banco Mundial indican que aún hay mucho por mejorar en el mercado digital de América Latina y el Caribe. Véase [en línea] www.doingbusiness.org.

²¹⁰ Véase, por ejemplo, el estudio de la Organización de Cooperación y Desarrollo Económicos (OCDE) [en línea] https://www.oecd-ilibrary.org/science-and-technology/politicas-de-banda-ancha-para-america-latina-y-el-caribe_9789264259027-es.

²¹¹ Corporación Andina de Fomento (CAF), "Building a Digital Single Market Strategy for Latin America" [en línea] <https://scioteca.caf.com/handle/123456789/980?show=full>.

²¹² Comisión Económica para América Latina y el Caribe (CEPAL), "Mercado digital regional", 2018 [en línea] https://repositorio.cepal.org/bitstream/handle/11362/43476/1/S1800295_es.pdf. Véase también "World Consumer Protection Map" [en línea] <https://unctadwcpm.org>. Véase una reseña de distintos regímenes nacionales y su desempeño en comparación con otros países del mundo en Hans-W. Micklitz y Genevieve Saumie, *Enforcement and Effectiveness of Consumer Law*, Springer, 2018.

La internacionalización del mercado plantea problemas jurisdiccionales a las empresas que operan a través de las fronteras. Estas empresas, que operan en las áreas de comercio electrónico, mercados o medios sociales, deben estar preparadas para cumplir con las leyes de protección del consumidor de todas las jurisdicciones en las que realizan actividades comerciales. Las leyes nacionales de protección del consumidor son aplicables independientemente del lugar donde se encuentre establecida la oficina central de una empresa de Internet. El mero hecho de que ofrezcan servicios y bienes a los consumidores locales ya da lugar a protecciones nacionales²¹³.

La presencia de una cultura común de protección del consumidor en América Latina y el Caribe ha coexistido hasta ahora con la falta de un marco armonizado adecuado o de un mercado único digital, lo que expone a las empresas a diversas normas de protección nacionales. Además, los consumidores pueden tratar de resolver sus controversias en su país, por lo que las empresas son llamadas a comparecer ante los tribunales de distintas jurisdicciones o a participar en diferentes procedimientos de solución de diferencias fuera del país donde se encuentran establecidas.

En otro nivel de complejidad, muchas de las leyes en cuestión se entienden como normas imperativas (*lois de police*), lo que significa que en la mayoría de los casos las estipulaciones contractuales no deben contradecirlas. En otras palabras, esas leyes se aplican independientemente de las condiciones y estipulaciones contractuales presentes en las transacciones por Internet²¹⁴.

Durante las negociaciones de la Séptima Conferencia Especializada Interamericana sobre Derecho Internacional Privado (CIDIP-VII) relativa a la protección internacional de los consumidores, varios países sostuvieron que las transacciones internacionales de los consumidores deberían estar sujetas al “principio de protección más favorable”. La ley aplicable al contrato sería la más favorable para el consumidor, ya sea la ley que se aplique en el lugar de jurisdicción, de residencia habitual del consumidor o del contrato²¹⁵.

La falta de normas comunes de protección del consumidor repercute en la forma en que los proveedores de servicios de Internet pueden interactuar con los consumidores de la región. La existencia de distintas leyes de protección del consumidor puede traducirse en diferentes normas relacionadas con la publicidad, las prácticas de facturación injustas, la terminación de contratos y el cambio de empresas (así como portabilidad e interoperabilidad)²¹⁶. Esta situación podría suponer una barrera al comercio²¹⁷.

El otro lado de la ecuación es que, a diferencia del mercado digital en Europa, por ejemplo, las leyes de protección del consumidor en América Latina y el Caribe por lo general se aplican solo dentro de los límites de cada jurisdicción nacional. Por consiguiente, es común que las empresas utilicen tecnologías de geolocalización para restringir el acceso a bienes y servicios en determinados lugares²¹⁸.

En el MERCOSUR se han puesto en marcha diversas iniciativas orientadas a armonizar las normas de protección del consumidor. Recientemente, los miembros propusieron estructurar y utilizar una plataforma digital para la solución de controversias en materia de consumo²¹⁹. Esto podría contribuir a promover los servicios de Internet transfronterizos y el comercio electrónico en la región mediante la disminución de los costos de los litigios y las controversias de los consumidores.

1.3. Las cláusulas de elección de la ley y la jurisdicción aplicables tienden a ser mal vistas en el comercio electrónico debido a la protección del consumidor a nivel nacional

La falta de normas armonizadas y de un mercado único digital, sumada a la naturaleza laxa de Internet, hace que resulte particularmente difícil determinar la jurisdicción sobre las transacciones transfronterizas. Para ofrecer más previsibilidad, la mayoría de las empresas de Internet optan por incluir en sus contratos una cláusula de jurisdicción o un método de solución de controversias (arbitraje, mediación o conciliación), así como cláusulas de elección de la ley aplicable. Con estas estipulaciones limitan su exposición y reducen las posibles complicaciones jurisdiccionales.

Los regímenes jurídicos de todo el mundo por lo general permiten esas opciones en el marco de lo que se denomina “autonomía de las partes”. Los países de América Latina y el Caribe han luchado con el

²¹³ Corporación Andina de Fomento (CAF), “Building a Digital Single Market Strategy for Latin America” [en línea] <https://scioteca.caf.com/handle/123456789/980?show=full>.

²¹⁴ C. Marques, “A proteção da parte mais fraca em direito internacional privado e os esforços da CIDIP VII de proteção dos consumidores”, Curso de Derecho Internacional de la OEA [en línea] http://www.oas.org/es/sia/ddi/docs/publicaciones_digital_XXXIV_curso_derecho_internacional_2007_Claudia_Lima_Marques.pdf.

²¹⁵ Las negociaciones no prosperaron, pero el concepto se mantuvo como una importante propuesta en los foros internacionales y sentó las bases para el debate intrarregional [en línea] <http://aebm.mo/en/2018Vol1Issue1/8>.

²¹⁶ Véase [en línea] <https://www.oecd-ilibrary.org/docserver/9789264251823-16-en.pdf?expires=1588103565&id=id&accname=guest&checksum=233F2DB69A0B854F1BC076348793B73 6>.

²¹⁷ M. Durovic, “International consumer law: what is it all about?”, *Journal of Consumer Policy*, vol. 43, 2020 [en línea] <https://doi.org/10.1007/s10603-019-09438-9>.

²¹⁸ Corporación Andina de Fomento (CAF), “Building a Digital Single Market Strategy for Latin America” [en línea] <https://scioteca.caf.com/handle/123456789/980?show=full>.

²¹⁹ Véase [en línea] <https://www.cancilleria.gob.ar/es/actualidad/noticias/comunicado-conjunto-de-los-presidentes-de-los-estados-parten-del-mercrosur>.

concepto durante la mayor parte del siglo XX²²⁰ y ello ha culminado en la aprobación de la Convención Interamericana sobre Derecho Aplicable a los Contratos Internacionales de 1994. No obstante, y debido, en parte, a la consagración del principio de autonomía de las partes, la Convención no ha recibido una amplia aceptación: solo México y la República Bolivariana de Venezuela la ratificaron²²¹. En las últimas dos décadas, sin embargo, el principio ha cobrado fuerza y muchos países han adoptado una postura más flexible y han acogido la autonomía de las partes en determinadas categorías de contratos²²².

Además, varios Estados son partes en la Convención de las Naciones Unidas sobre los Contratos de Compraventa Internacional de Mercaderías (CIM) de 1980. Las ventas transfronterizas de mercancías por Internet podrían quedar, por consiguiente, abarcadas por sus disposiciones, que prevén la autonomía de las partes. Sin embargo, la Convención no necesariamente sustituye a otras consideraciones, en particular la protección del consumidor²²³.

La cuestión de la jurisdicción y la ley aplicable se ha convertido, entonces, en una de tres partes: i) si un país permite la elección de la ley y la jurisdicción aplicables; ii) si se acepta la autonomía de las partes en lo que respecta a la elección de medios no judiciales de solución de controversias (por ejemplo, el arbitraje y la mediación) y en qué condiciones, y iii) si ciertas categorías de transacciones, como las de consumo, reciben un nivel de protección diferente.

La fuerte cultura de protección del consumidor ha dejado huella en la forma en que se interpretan los contratos en la región. Muchos países de América Latina y el Caribe entienden que los contratos en los que existe un desequilibrio inherente entre las partes —donde la parte más fuerte impone obligaciones contractuales— deben ser objeto de un mayor escrutinio²²⁴. La consecuencia es que las cláusulas de la ley y la jurisdicción aplicables suelen ser mal vistas cuando pueden resultar desventajosas para la parte más débil²²⁵. En algunas circunstancias, se consideran abusivas, en particular si limitan las opciones de solución de controversias o el acceso al poder judicial. Este es el caso, en particular, de las transacciones en las que participa un consumidor²²⁶.

La mayoría de las transacciones que se realizan por Internet (por ejemplo, comercio electrónico y servicios de Internet) se rigen por los denominados “acuerdos de pulsar y comprar” (click-wrap) o “acuerdos de aceptación mediante la navegación por sitios web” (browse-wrap), cuyas cláusulas sustantivas se encuentran en los términos y condiciones disponibles en línea. Estos contratos dejan poco espacio para la negociación. Por lo general, la parte más débil (un consumidor) no tiene otra opción que aceptar todas las cláusulas tal como están o renunciar al acceso a ese servicio o bien. Esos acuerdos se consideran contratos de adhesión y tienden a interpretarse a favor de la parte más débil. De este modo pueden aplicarse leyes de protección del consumidor y además también puede considerarse que las cláusulas de la ley y la jurisdicción aplicable no son válidas, en especial si los consumidores las cuestionan en los tribunales²²⁷.

Del mismo modo, una cláusula del mecanismo de solución de diferencias puede correr la misma suerte. Si la cláusula impide que un consumidor tenga acceso al poder judicial, esto puede interpretarse como un abuso y los tribunales pueden no hacerla cumplir. Las empresas de Internet que quieren limitar su exposición a diferentes tribunales y leyes pueden terminar recurriendo a técnicas de geolocalización para limitar su alcance geográfico (véase más información sobre estas técnicas en la sección III.B.1).

²²⁰ Véase [en línea] http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.

²²¹ Véase [en línea] <http://www.oas.org/juridico/spanish/firmas/b-56.html>.

²²² En la región, solo el Uruguay rechaza expresamente la autonomía de las partes, aunque ha habido cierta aceptación en la doctrina y la jurisprudencia. En el Brasil se sigue debatiendo sobre su plena aplicabilidad y la jurisprudencia no es consecuente al respecto. Véase una reseña en Comité Jurídico Interamericano, “Guide on the Law Applicable to International Commercial Contracts”, febrero de 2019 [en línea] https://www.oas.org/en/sla/ajc/docs/Guide_Law_Applicable_to_International_Commercial_Contracts_in_the_Americas.pdf.

²²³ Véase una lista de países partes [en línea] https://uncitralun.org/es/texts/saleofgoods/conventions/sale_of_goods/cisg.

²²⁴ Véase [en línea] http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.

²²⁵ La Asociación de Derecho Internacional ha reconocido que los consumidores suelen ser las partes más débiles en los contratos transfronterizos. Véase Asociación de Derecho Internacional, “Resolution No.1/2016. Committee on the International Protection of Consumers”, [en línea] https://www.ila-hq.org/images/ILA/docs/No.1_Resolution_2016_ProtectionOfConsumers_4Models.pdf. Un claro ejemplo es el artículo 2651 del Código Civil de la República Argentina, que permite la autonomía de las partes en todos los contratos, excepto en los que intervienen consumidores. Otro ejemplo es el artículo 89 y siguientes del Código de Derecho Internacional Privado de la República de Panamá, donde se establece un régimen especial para los contratos en los que las partes no están en igualdad de condiciones (“contratos desiguales o de adhesión”).

²²⁶ Se han registrado esfuerzos intrarregionales —de los cuales la Séptima Conferencia Especializada Interamericana sobre Derecho Internacional Privado es un ejemplo— orientados a establecer convenciones internacionales para hacer frente a distintos problemas jurisdiccionales transfronterizos internacionales en los que intervienen consumidores. La Séptima Conferencia Especializada Interamericana sobre Derecho Internacional Privado no prosperó, entre otras razones, porque no se llegó a un acuerdo sobre el papel de la autonomía de las partes o la opción de poder elegir el arbitraje como medio para resolver las controversias. Véase una reseña de esta iniciativa en D. Fernández Arroyo y J. A. Moreno Rodríguez, *Protección de los consumidores en América: trabajos de la CIDIP VII (OEA)*, Asunción, La Ley-CEDEP, 2007. Véase también [en línea] http://www.oas.org/es/sla/ddi/docs/publicaciones_digital_XXXIV_curso_derecho_internacional_2007_Claudia_Lima_Marques.pdf y <https://docplayer.es/80967826-The-inter-american-convention-on-the-law-applicable-to-international-contracts-and-the-furtherance-of-its-principles-in-the-americas.html>.

²²⁷ Véase [en línea] http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf.

1.4. Los Gobiernos de la región están imponiendo normas más estrictas para la moderación y eliminación de contenidos en las plataformas en línea

En el informe Internet & Jurisdiction Global Status Report 2019 se identificó que existe una tendencia mundial a que los Estados tengan una actitud más dura hacia las plataformas de Internet, y los países de América Latina y el Caribe no son la excepción.

Las peculiaridades de las empresas de Internet y de los servicios que prestan inicialmente dieron lugar a la adopción generalizada de normas y garantías que las protegerían de litigios importantes relacionados con contenidos creados por terceros, principalmente sus propios usuarios. Esta tendencia surgió a finales de la década de 1990, cuando el artículo 230 de la Ley de Decencia en las Comunicaciones y la Ley de derechos de autor del milenio digital crearon una especie de refugio seguro para los proveedores de Internet en los Estados Unidos. La Unión Europea siguió el ejemplo con la Directiva sobre el comercio electrónico (2000/31/EC).

Muchas cosas han cambiado desde fines de los años noventa, ya que las plataformas de comercio electrónico se han vuelto omnipresentes y las empresas de medios sociales pueden tener como usuarios a la mayoría de la población de un país sin tener ninguna oficina allí. Al mismo tiempo, la asombrosa velocidad con que se produce el contenido en línea sigue reforzando la necesidad de diseñar un régimen especial de moderación del contenido y responsabilidad. No cabe duda de que los 6.000 tuits enviados por segundo y las 400 horas de video de YouTube subidas cada minuto son cifras que suponen todo un desafío.

Algunos países de la región recogen en sus legislaciones cláusulas de limitación de responsabilidad para los intermediarios de Internet, creando una excepción específica para la aplicación de las normas de responsabilidad civil general o los regímenes generales de protección del consumidor en caso de mal funcionamiento de los productos o servicios²²⁸.

Aunque la situación está cambiando rápidamente y todo el tiempo surgen grandes cantidades de empresas locales de Internet, los países de América Latina y el Caribe siguen recibiendo servicios principalmente de empresas y plataformas de Internet establecidas fuera de la región. En consecuencia, toda interacción tiende a ser transnacional, lo que puede plantear conflictos jurisdiccionales.

El enfoque de las plataformas de Internet ha cambiado por lo menos en dos esferas: el contenido de terceros (moderación del contenido) y la protección de la propiedad intelectual (piratería y falsificación). Como ya se ha mencionado, esferas como la aplicación de la ley (sección III.B.2), el ciberacoso (sección III.A.3) y la exposición no autorizada de imágenes íntimas (sección II.A.4) también han ejercido presión sobre los intermediarios de Internet para que asuman un papel más activo y cooperen con los organismos encargados de hacer cumplir la ley.

En el Brasil, se pidió al Supremo Tribunal Federal que se pronuncie sobre si la cláusula de limitación de responsabilidad incluida en el Marco Civil de Internet del Brasil —una cláusula que limita la responsabilidad de los intermediarios de Internet por el alojamiento o la transferencia de contenidos de terceros— está en consonancia con la Constitución de la República Federativa del Brasil.

En la Argentina, un proyecto de ley para regular la responsabilidad de los intermediarios no recibió el apoyo necesario²²⁹. Del mismo modo, México ha luchado por encontrar apoyo para establecer un régimen de responsabilidad de conformidad con el Tratado entre México, los Estados Unidos y el Canadá, que garantice la seguridad para el comercio digital transfronterizo entre las partes²³⁰.

En el Ecuador se propuso un proyecto de ley para regular el contenido en línea que incluía disposiciones que hacían a los intermediarios de Internet directamente responsables de eliminar los contenidos considerados ilegales²³¹. En Honduras se propuso un proyecto de ley similar, en el que se proporcionaban definiciones muy amplias de los tipos de contenido ilegal que los intermediarios de Internet deben vigilar²³².

En el mismo sentido, una ley aprobada en la República Bolivariana de Venezuela hace hincapié en la responsabilidad de los intermediarios y prevé sanciones si no retiran el contenido ilegal. Las entidades estatales también pueden solicitar directamente que se retire el contenido²³³. Un proyecto de ley presentado en el Paraguay buscaba imponer a los proveedores de servicios de Internet la obligación de eliminar el contenido considerado “ofensivo”²³⁴.

²²⁸ Solo el Brasil y Chile tienen cláusulas de limitación de responsabilidad de los intermediarios de Internet para alojar o transferir contenidos de terceros, promulgadas como parte de su legislación. Véase Banco Interamericano de Desarrollo (BID), “Accelerating Digital Trade in Latin America and the Caribbean” [en línea] <https://publications.iadb.org/publications/english/document/Accelerating-Digital-Trade-in-Latin-America-and-the-Caribbean.pdf>.

²²⁹ Véase [en línea] <https://www.lanacion.com.ar/tecnologia/los-intermediarios-internet-debate-seguira-pendiente-nid2192063>.

²³⁰ Véase [en línea] <https://www.derechosdigitales.org/12564/usmca-y-el-futuro-de-internet/>.

²³¹ Véase [en línea] <https://www.eluniverso.com/opinion/2017/06/13/nota/6229435/redes-sociales-censura>.

²³² Véase [en línea] <https://www.accessnow.org/comunicado-ley-que-regula-los-actos-de-odio-y-discriminacion-en-internet-de-honduras/> y <https://www.hrw.org/es/news/2018/04/09/honduras-proyecto-de-ley-sobre-ciberseguridad-amenaza-la-libertad-de-expresion>.

²³³ Véase [en línea] <http://espaciopublico.org/ley-odio-venezuela-amenaza-la-libre-expresion-america-latina/>.

²³⁴ TEDIC, “Un proyecto de censura política”, 11 de octubre de 2017 [en línea] <https://www.tedic.org/un-proyecto-de-censura-politica/>.

Las organizaciones de la sociedad civil han expresado su preocupación con respecto a las iniciativas para fortalecer la responsabilidad de los intermediarios²³⁵. El Relator Especial para la Libertad de Expresión se ha hecho eco de los posibles riesgos que estas iniciativas legislativas pueden suponer para los derechos humanos²³⁶.

Si bien gran parte de la atención se ha centrado en las plataformas de medios sociales, no se han ignorado los sitios web de comercio electrónico ni los mercados. Los Gobiernos de la región han endurecido las medidas contra la piratería y los productos falsificados, restringiendo los contenidos considerados ilegales y reforzando las protecciones de los derechos de propiedad intelectual.

La reforma de los derechos de propiedad intelectual, incluidos los derechos de autor, también puede brindar a los países la oportunidad de armonizar sus opiniones y facilitar los enfoques a nivel regional, facilitando la circulación de los bienes y servicios protegidos por derechos de autor y de otras clases de propiedad intelectual.

2. Propiedad intelectual

En el informe *Internet & Jurisdiction Global Status Report 2019* ya se destacaron varias intersecciones entre Internet y los derechos de propiedad intelectual. Los derechos de propiedad intelectual sobre patentes, marcas y diseños en el entorno digital no tienen por qué estar restringidos a un territorio en particular. Su materialización en una forma física puede parecer una limitación, como por ejemplo cuando una película tenía que estar en formato de filme, cinta o videodisco digital (DVD) para poder circular. Pero cuanto más se convierte la carne en palabra, parafraseando a Barlow, menos actúan como restricción las barreras físicas que obstaculizan la circulación de la propiedad intelectual²³⁷. El material protegido por derechos de autor puede descargarse o emitirse en directo sin tener en cuenta las fronteras.

La reglamentación de la propiedad intelectual, no obstante, sigue siendo en muchos aspectos un asunto interno de cada país, sobre todo en lo que respecta a las excepciones. Por consiguiente, las diferencias reglamentarias, que van desde las interpretaciones de los tratados internacionales hasta los mecanismos de aplicación efectiva, tienden a crear dificultades transfronterizas. Esto resulta particularmente difícil cuando los particulares y las empresas utilizan la naturaleza sin fronteras de Internet para eludir la legislación o incluso las decisiones judiciales orientadas a proteger eficazmente la propiedad intelectual.

2.1. Protección de la propiedad intelectual: repercusiones en la economía y los derechos humanos

Los mecanismos de observancia del derecho de autor varían de un Estado a otro. La forma en que están estructurados es un aspecto importante de un equilibrio muy intrincado entre la provisión de incentivos a los autores, la protección de los intereses económicos de la industria y la salvaguarda del derecho y el interés de la sociedad en acceder a los frutos de la creación. En otras palabras, el derecho de autor es una institución clave que fomenta y protege la cultura. Sin embargo, si se aplica el derecho de autor de manera demasiado estricta, puede que se restrinja el acceso al conocimiento y el avance de la cultura.

En un entorno en el que los memes son una importante tendencia social, las nuevas obras suelen producirse sobre la base de material anterior, generalmente protegido por derechos de autor. La restricción del acceso y el uso de contenidos protegidos por derechos de autor limita tanto el acceso al conocimiento (ideas y material) como la innovación²³⁸.

En América Latina y el Caribe es fundamental que el equilibrio entre la protección de los derechos de autor y la salvaguardia del acceso se refleje bien en las reglamentaciones. Las partes interesadas encuestadas señalaron la relación entre el derecho de autor y el desarrollo, pero también destacaron que en muchas circunstancias el derecho de autor podía utilizarse para restringir el acceso de las sociedades a la información. El derecho de autor se ha utilizado incluso como herramienta para restringir la libertad de expresión. Se ha informado de que eso fue lo que ocurrió con material crítico del Presidente Correa durante las elecciones ecuatorianas²³⁹.

²³⁵ Véase [en línea] <https://www.derechosdigitales.org/internetesnuestra/desafios-gobernanza.pdf>.

²³⁶ Organización para la Seguridad y Cooperación en Europa (OSCE), "Joint Declaration on Freedom of Expression and "Fake News", Disinformation and Propaganda" [en línea] <https://www.osce.org/fom/302796>. La Comisión Interamericana de Derechos Humanos también ha mostrado su preocupación con una iniciativa similar en el contexto electoral. Véase [en línea] https://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf <https://www.osce.org/fom/302796>.

²³⁷ John Perry Barlow, "Selling wine without bottles: the economy of mind on the global net", *Duke Law and Technology Review*, vol. 18, 2019.

²³⁸ A. Chander y M. Sunder, "Dancing on the grave of copyright?", *Duke Law & Technology Review*, vol. 18, 2019 [en línea] <https://ssrn.com/abstract=3436972>.

²³⁹ Véase [en línea] <https://www.hrw.org/world-report/2018>. Véase [en línea] <https://www.hrw.org/es/world-report/2018/country-chapters/313046>. Se ha informado de que esto también ha ocurrido en otras circunstancias. Véase A. Ellerbeck, "Cómo la ley sobre el derecho de autor se usa para silenciar a críticos del presidente Correa", Comité para la Protección de los Periodistas, 21 de enero de 2016 [en línea] <https://cpj.org/es/2016/01/como-la-ley-sobre-el-derecho-de-autor-se-usa-para/>.

Otro aspecto que hay que tener en cuenta es que en muchas circunstancias la información inexacta (incluida la desinformación) está disponible gratuitamente y circula sin barreras, pero los conocimientos reales y la información necesaria están restringidos, “protegidos” por barreras de pago y bases de datos de difícil acceso²⁴⁰.

En este contexto, se ha debatido cómo equilibrar mejor la protección de la propiedad intelectual, en particular el derecho de autor, con los derechos a la educación, el acceso a la información y el autodesarrollo y otros derechos humanos. La cuestión, en algunos casos, ha sido si los procedimientos de aplicación estrictos contra la piratería y, en ciertas circunstancias, la reproducción no autorizada son la mejor manera de lograr los objetivos de política en relación con el derecho de autor.

Un buen ejemplo es la protección de los conocimientos tradicionales. La salvaguardia adecuada de los conocimientos, las tradiciones, los procedimientos y las manifestaciones culturales de los grupos tradicionales y las poblaciones indígenas de la región es fundamental para la protección de su modo de vida y, por extensión, de sus derechos humanos. Muchos países de la región han tomado conciencia de la necesidad de establecer normas mejores y más específicas que reconozcan los conocimientos tradicionales. El Brasil, Costa Rica, el Perú y la República Bolivariana de Venezuela son claros ejemplos de esta tendencia. Se han dado casos de países que han presentado denuncias a empresas internacionales por su explotación de los conocimientos tradicionales, y las relaciones se han transferido, en algunos casos, a intermediarios de Internet que venden productos con la debida protección²⁴¹.

2.2. Los efectos transfronterizos del filtrado que se usa para hacer cumplir los derechos de propiedad intelectual

La dinámica de la protección de los derechos de autor en línea tiene muchas facetas diferentes. El sector privado, y los intermediarios de Internet en particular, han sido llamados a desempeñar un papel más importante últimamente. De forma voluntaria o mediante acuerdos con el sector público, varias empresas, sobre todo de mercados y redes sociales, han desarrollado mecanismos de protección de los derechos de autor.

Amazon, por ejemplo, ha ampliado su Proyecto Cero de lucha contra la falsificación a un total de 17 países (incluidos el Brasil y México en la región de América Latina y el Caribe), como parte de su iniciativa de protección de la propiedad intelectual y las marcas²⁴². La plataforma de comercio electrónico Mercado Libre, que opera en 18 países de América Latina, también tiene un programa de protección de los derechos de autor que funciona de manera similar. Estos programas incluyen instrumentos para los titulares de derechos y prevén sanciones por posibles violaciones, que pueden ir hasta la suspensión o cancelación de la cuenta para los reincidentes²⁴³.

Estos mecanismos voluntarios no necesariamente son suficientes, y algunas jurisdicciones han pedido que se revise la reglamentación vigente en la materia. La Unión Europea emitió recientemente la Directiva 2019/790, que ha causado una gran controversia tanto en Europa como en la región²⁴⁴. La directiva tiene por objeto aumentar la responsabilidad de los intermediarios de Internet por el contenido de terceros en sus entornos en línea (véase más información sobre la nueva función de los intermediarios de Internet en la sección I.F).

Esas reglamentaciones han repercutido de dos maneras en la región. En primer lugar, han incitado a los países a revisar su legislación de derechos de autor para incluir obligaciones similares. En segundo término, como efecto transfronterizo directo, el material propiedad de varios artistas o titulares de derechos de autor puede ser retirado por esas plataformas y el proceso deberá impugnarse en otros países (véase más información sobre los mecanismos en línea para impugnar esas decisiones en la sección III.A.5)²⁴⁵.

²⁴⁰ A. J. Robinson, “The truth is paywalled but the lies are free”, *Current Affairs*, 20 de agosto de 2020 [en línea] <https://www.currentaffairs.org/2020/08/the-truth-is-paywalled-but-the-lies-are-free>.

²⁴¹ Véase [en línea] <https://yourlatamflagship.com/2020/01/16/how-latin-america-countries-protect-their-traditional-knowledge-through-ip/>. Véase más información sobre esta tendencia desde una perspectiva latinoamericana en L. Lixinski, *International Heritage Law for Communities Exclusion and Re-Imagination*, Oxford University Press (OUP), 2019.

²⁴² Co comunicado de prensa “Amazon Project Zero launches in seven new countries”, agosto de 2020 [en línea] <https://press.aboutamazon.com/news-releases/news-release-details/amazon-project-zero-launches-seven-new-countries/>.

²⁴³ Mercado Libre, “Brand Protection Program qué es y cómo usarlo” [en línea] <https://vendedores.mercadolibre.com.ar/blog/notas/brand-protection-program-que-es-y-como-usarlo/>.

²⁴⁴ Véase [en línea] <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790>.

²⁴⁵ Véase [en línea] <https://br.creativecommons.org/a-diretiva-da-uniao-europeia-sobre-direito-de-autor-e-seu-impacto-sobre-os-usuarios-na-america-latina-e-no-caribe/>.

Las organizaciones de la sociedad civil han expresado su preocupación por el hecho de que la nueva directiva de la Unión Europea sobre derechos de autor pueda convertirse en un modelo para la reforma de los derechos de autor en la región y pueda tener un efecto disuasorio en el discurso y obstaculizar el comercio en línea. A su juicio, los requisitos de esta legislación pueden dar lugar a un filtrado automático y dejar muy poco espacio y tiempo para el análisis contextual²⁴⁶.

En el Brasil, el proyecto de ley contra las noticias falsas (véase la sección II.A.1) ha alentado a las asociaciones de la industria de la radio y la televisión a proponer una indemnización para los editores de material de prensa como forma de compensación por derechos de autor cuando dicho material es utilizado por los proveedores de servicios de Internet. En su opinión, esta medida sería eficaz para impulsar el periodismo profesional, y podría ayudar a combatir la desinformación y las noticias falsas²⁴⁷. Un mecanismo similar (el impuesto a los enlaces), previsto en el artículo 15 de la Directiva de la Unión Europea sobre el derecho de autor²⁴⁸, ha sido ampliamente criticado por considerar que podría poner en peligro el acceso a la información y por los inconvenientes que podría acarrear para los servicios pequeños y no comerciales²⁴⁹.

Los filtros, que son herramientas automatizadas para detectar y eliminar el contenido protegido por derechos de autor, exacerbán aún más este fenómeno. Las técnicas que utilizan suelen generar falsos positivos, marcando y restringiendo contenido que es legal o que entra dentro de alguna de las excepciones a las restricciones del derecho de autor (parodia, uso justo, uso educativo, etc.). Por lo tanto, las empresas deben adaptar sus filtros a la diversidad de leyes y contextos locales, o tendrán que optar por un filtro general que puede crear más restricciones de las necesarias.

Es probable que América Latina y el Caribe acuse el impacto de los filtros y controles de derechos de autor. La circulación de materiales con derechos de autor puede verse afectada. Los sectores de la cultura y el entretenimiento son claros ejemplos. Los países se benefician de la polinización cruzada cultural entre los artistas de la región. El intercambio en línea suele ser sinónimo de mercados y públicos mucho más grandes para los artistas locales. Los filtros pueden proteger los derechos de autor, pero también pueden limitar la exposición y dificultar la apelación de las decisiones adoptadas por las plataformas (véase información sobre las apelaciones en la sección III.A.5).

3. Internet de las cosas

En todo el mundo se ha producido un fenómeno doble: la digitalización del espacio físico y la fusión del mundo físico con el digital. Al tiempo que reduce los costos de producción, transacción y distribución, esta superposición de lo físico y lo digital también crea nuevas oportunidades. El concepto de Internet de las cosas cubre una parte importante de este proceso. La conexión de dispositivos que tradicionalmente no estaban conectados (desde refrigeradores hasta tractores y desde redes de abastecimiento de agua hasta redes de suministro eléctrico) permite disponer de más datos y funciones. Por consiguiente, se pueden suministrar bienes y servicios más especializados, se puede optimizar la adopción de decisiones basadas en hechos (basadas en datos) y se pueden mejorar las experiencias generales, incluida la oportunidad.

La Internet de las cosas es más que proporcionar una conexión a Internet: crea ecosistemas basados en la tecnología cuyo valor proviene de la captura, el registro y el análisis de datos. El valor de estas funciones se ve potenciado por la combinación con la computación en la nube, la tecnología de cadenas de bloques, la robótica y la inteligencia artificial²⁵⁰. Un fabricante de equipos agrícolas puede tener acceso, por ejemplo, a datos sobre el clima, los hábitos de conducción y el rendimiento de los cultivos. Alguien que se dedica a crear relojes inteligentes puede utilizar las funciones de monitoreo del producto para proporcionar una serie de bienes y servicios que pueden ayudar a las personas a administrar mejor el ejercicio que realiza y los hábitos de consumo de bebidas y alimentos: en una palabra, su salud. Una ciudad puede tomar mejores decisiones sobre cómo se asignan los recursos del sistema de transporte.

²⁴⁶ Véase [en línea] <https://web.karisma.org.co/la-directiva-europea-de-derecho-de-autor-y-su-impacto-en-los-usuarios-de-america-latina-y-el-caribe-una-perspectiva-desde-las-organizaciones-de-la-sociedad-civil/>.

²⁴⁷ O Globo, "Entidades pedem transparéncia e valorização do jornalismo profissional no projeto contra fake news" 18 de agosto de 2020 [en línea] <https://oglobo.globo.com/brasil/entidades-pedem-transparencia-e-valorizacao-do-jornalismo-profissional-no-projeto-contra-fake-news-24593224>.

²⁴⁸ Unión Europea, "Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo de 17 de abril de 2019 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE.

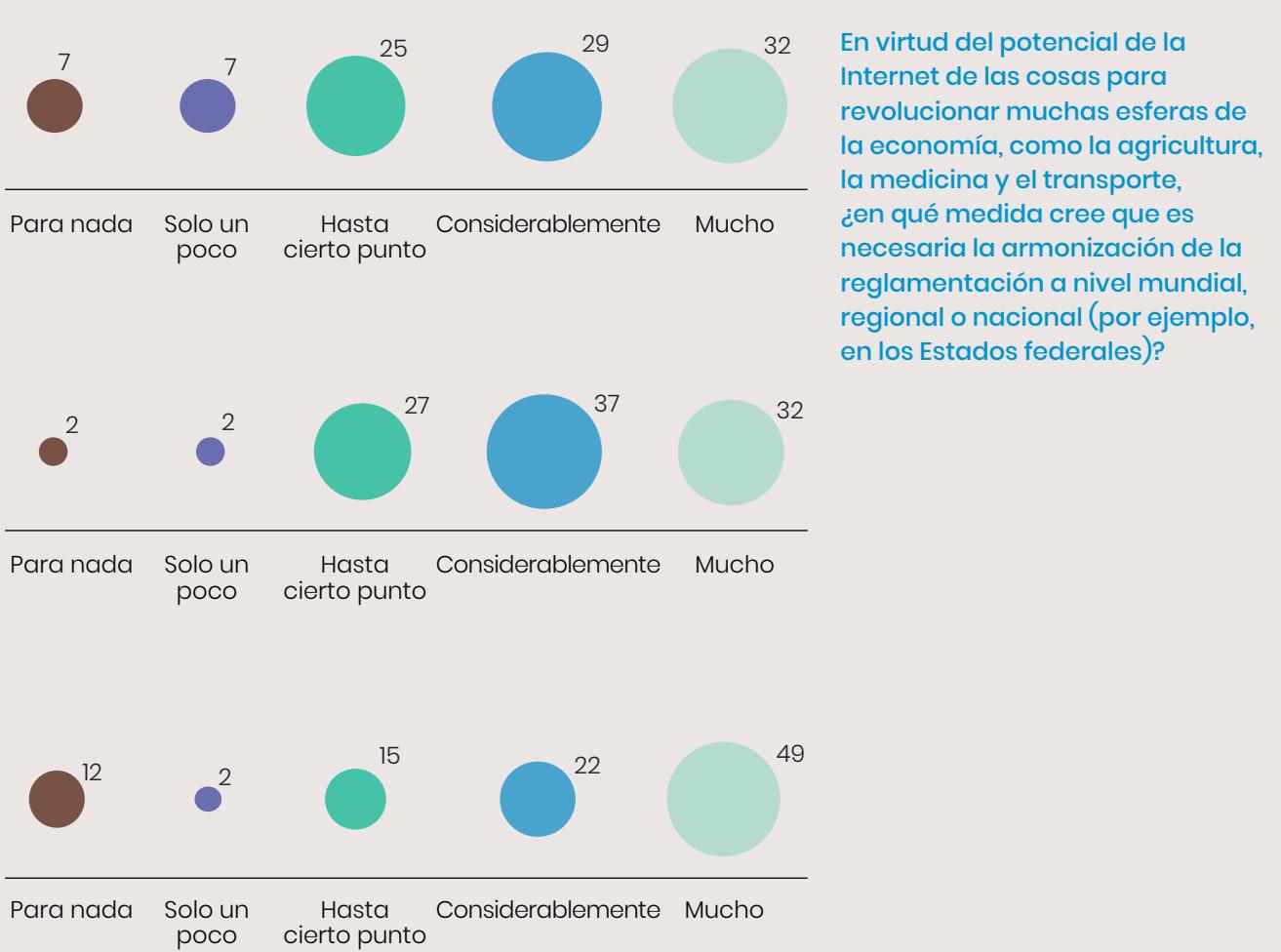
²⁴⁹ Cory Doctorow, "The European Copyright Directive: what it is, and why has it drawn more controversy than any other directive in EU history?", Electronic Frontier Foundation, 19 de marzo de 2019 [en línea] <https://www.eff.org/pt-br/deeplinks/2019/03/european-copyright-directive-what-it-and-why-has-it-drawn-more-controversy-any>.

²⁵⁰ Comisión Económica para América Latina y el Caribe (CEPAL), *Datos, algoritmos y políticas: la redefinición del mundo digital* (LC/CMSI.6/4), Santiago, 2018.

Los modelos comerciales que giran en torno a la Internet de las cosas no tienen por qué respetar los mercados verticales ni tienen que estar restringidos por las fronteras nacionales. Se benefician de la naturaleza sin fronteras de la red a la que están conectados y, en cierta medida, de la desmaterialización que conlleva la digitalización. Esto significa una sociedad “sensorial”, donde todo lo que pueda vincularse a Internet se vinculará y los datos que puedan compartirse también se compartirán. El comercio transfronterizo y los flujos de datos a través de las fronteras son una consecuencia probable de la implantación de la Internet de las cosas. Para aprovechar al máximo la Internet de las cosas, es necesario que haya escala, convergencia, armonización y un entorno interoperable con un mercado interconectado.

Las partes interesadas encuestadas señalaron que los principales desafíos se referían al establecimiento de protocolos, normas comunes, patrones de la industria y la armonización de reglas y reglamentos. En general, sus preocupaciones por la región coincidían con las recogidas en el informe *Internet & Jurisdiction Global Status Report 2019*: seguridad y privacidad, normas técnicas comunes, seguridad de los productos, disponibilidad de ancho de banda y conectividad, normas de responsabilidad e interoperabilidad regional.

Uno de los interesados señaló que la plena armonización de las reglamentaciones y normas en la región podía ser un objetivo difícil de alcanzar, pero que era posible llegar a un acuerdo sobre reglas o directrices respecto de la forma en que las empresas y los Estados podían sortear las diferencias que se registraban en la región en materia de regulación. Algunos de los interesados destacaron que debía darse prioridad a la estructuración del sistema en torno a incentivos a la inversión privada para que la industria pueda operar en todos los países. Todas estas inquietudes y sugerencias ponen de manifiesto la necesidad de coordinación y cooperación, tanto a nivel intrarregional como mundial.



Fuente: Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL).

3.1. De lo privado a lo público: casas conectadas inteligentes en ciudades conectadas inteligentes

Las oportunidades que ofrece la Internet de las cosas abarcan todas las cosas que pueden tener un sensor integrado y conectarse a Internet, desde las más íntimas (cuerpo humano) hasta las más públicas (ciudades), pasando por casas, industrias y campos²⁵¹. La naturaleza transversal de la Internet de las cosas hace que se planteen oportunidades y desafíos en una amplia gama de temas y sectores.

La aplicación más cercana a la experiencia humana está en las tecnologías ponibles: dispositivos inteligentes que las personas llevan encima, en contacto con el cuerpo, y que les ayudan en las actividades diarias. Estos van desde los dispositivos más utilizados, como los relojes inteligentes, hasta los más sofisticados, que miden las ondas cerebrales o la frecuencia cardíaca. La conveniencia y el valor se deben a su capacidad de proporcionar fácilmente información sobre la situación de una persona, lo que permite una mejor toma de decisiones.

La situación es similar en el caso de los dispositivos para el hogar y la Internet de las cosas. No hay duda de que estos dispositivos ofrecen muchos beneficios, por ejemplo, al aumentar la facilidad y la eficiencia de la utilización de bienes y servicios que pueden reducir el consumo doméstico (electricidad, agua y gas), o al proporcionar seguridad, en el caso de las cámaras que vigilan el terreno de una vivienda o los aparatos que detectan un incendio o cierran la propiedad cuando hay peligro. Pueden servir para establecer una mejor conexión con el mundo exterior, facilitando la compra de alimentos o la solicitud de servicios.

Sin embargo, también pueden conllevar algunos riesgos. La Internet de las cosas trabaja con datos que aportan los conocimientos necesarios para que se puedan proporcionar bienes y servicios innovadores. La ubicuidad²⁵² e intimidad de muchos de esos dispositivos socavan la separación entre las esferas pública y privada, y podrían alterar la presunción de privacidad que las personas asocian con su hogar y su cuerpo²⁵³. Para las personas es difícil controlar y comprender las clases de datos recopilados y procesados. Por consiguiente, es necesario abordar las cuestiones de transparencia, control, consentimiento y responsabilidad.

Teniendo en cuenta que los proveedores pueden tener un alcance mundial, la cooperación y la coordinación parecen ser primordiales²⁵⁴. La mayoría de las iniciativas han adoptado la forma de planes, estrategias y políticas nacionales, y solo han incorporado marginalmente una dimensión mundial o regional, sin establecer un vínculo entre estas dimensiones y el tema de la Internet de las cosas propiamente dicho. Las partes interesadas que fueron encuestadas coincidieron en la necesidad de armonización, pero parecen estar divididas en cuanto a la necesidad de establecer normas específicas para la Internet de las cosas. Por ejemplo, algunos cuestionaron si una regulación más básica, que aborde temas como la protección de los consumidores y de los datos personales y la ciberseguridad, debería interpretarse ampliamente para abarcar los desafíos que plantea esta tecnología.

Planes, estrategias y acciones en relación con la Internet de las cosas:

El Brasil cuenta con un Plan Nacional de Internet de las Cosas, que se centra en cuatro sectores principales: ciudades, salud, agronegocio y manufactura inteligentes. También hace hincapié en cuatro esferas estratégicas para el desarrollo: innovación e internacionalización, capital humano, privacidad y seguridad normativa, e infraestructura para la conectividad y la interoperabilidad²⁵⁵.

México ha establecido como prioridad de política centrarse en la Internet de las cosas en la industria y uno de los puntos focales es la fabricación de automóviles²⁵⁶.

Tanto la Argentina como Colombia han diseñado políticas relativas a la Internet de las cosas en colaboración con el sector privado. El objetivo de ambos países es incentivar las alianzas estratégicas, la cooperación y los acuerdos comerciales para promover un entorno favorable al desarrollo de la Internet de las cosas²⁵⁷.

²⁵¹ Véase [en línea] <https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/>.

²⁵² Algunos dispositivos están siempre encendidos, recabando datos personales. Véase [en línea] https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf.

²⁵³ Internet Society, "Policy Brief: IoT P for Policymakers", 19 de septiembre de 2019 [en línea] www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/.

²⁵⁴ En un estudio de McKinsey se ha abordado el tema del alcance mundial de ciertos proveedores de servicios. Véase [en línea] <https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/unlocking-value-from-iot-connectivity-six-considerations--for-choosing-a-provider>.

²⁵⁵ En 2019, el plan se institucionalizó mediante el Decreto Presidencial núm. 2984/2019 [en línea] http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm. El plan original se lanzó en 2017 mediante una iniciativa de múltiples interesados en asociación con el Banco Nacional de Desarrollo Económico y Social (BNDES) [en línea] <https://www.bnDES.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil>.

²⁵⁶ Véase [en línea] <https://www.gob.mx/promexico/acciones-y-programas/mapas-de-ruta-22850>.

²⁵⁷ En Colombia se estableció a través del Centro de Excelencia y Apropriación en Internet de las Cosas (CEA-IoT). Véase [en línea] <http://www.ceaiot.org>. En la Argentina, esta función está a cargo de la Cámara Argentina de Internet (CABASE). Véase [en línea] <http://cabaseiot.com.ar>.

Las ciudades inteligentes son otra área donde la Internet de las cosas juega un papel transformador. Esta tecnología puede integrarse en el paisaje de la ciudad para captar y analizar datos que, ya sea por medios tradicionales o tecnológicos, permitan a las autoridades resolver mejor los problemas de los municipios²⁵⁸. La Internet de las cosas ayuda a organizar el entorno urbano, sentando las bases para lograr respuestas más rápidas y basadas en la evidencia empírica. Ya se está trabajando en su implementación en áreas como el tráfico, el estacionamiento, la seguridad, la contaminación y la higiene²⁵⁹.

Los proyectos de ciudades inteligentes por lo general se ejecutan mediante asociaciones público-privadas en las que participan varios agentes, no todos pertenecientes al país en cuestión. Cada capa implica una compleja serie de decisiones sobre, por ejemplo, qué instituciones y empresas deben participar, de dónde deben provenir los suministros, cuál debe ser la configuración, quién debe administrar el proyecto y cómo debe administrarlo. Las respuestas pueden exigir una coordinación regional e internacional.

Se observa, entonces, que en muchos puntos de contacto internacionales surgen posibles complejidades en materia jurisdiccional. Cada capa, comenzando por la infraestructura de conectividad (por ejemplo, 5G), depende de alianzas estratégicas y de la cooperación entre una serie de prestadores y proveedores que pueden estar ubicados en cualquier lugar del mundo. En la medida en que el ecosistema de la Internet de las cosas en la región se vuelve más complejo y los bienes y servicios se suministran cada vez más a través de una cadena de proveedores que pueden no estar establecidos en el mismo país que el usuario, es posible que haya que revisar las soluciones jurisdiccionales.

América Latina y el Caribe presenta uno de los niveles de urbanización más altos del mundo, por lo que los desafíos son considerables. La Internet de las cosas para los servicios públicos podría tener un gran impacto y alterar todo el panorama de las ciudades, así como la forma en que se diseñan las políticas públicas para esas urbes. Las ciudades y los países de la región por sí solos no pueden proporcionar todas las soluciones necesarias²⁶⁰. La necesidad de coordinación se vuelve aún más fuerte ante la tendencia a buscar asociaciones y alianzas con proveedores extranjeros.

Otros dos aspectos adquieren un carácter particular en América Latina y el Caribe: los datos municipales abiertos y la participación ciudadana. Las ciudades de la región han adoptado los datos abiertos con rapidez en comparación con las de otros lugares. Esto permite que los datos disponibles se vuelvan a utilizar para servicios innovadores. A partir de una iniciativa brasileña de los años noventa, la participación ciudadana en la asignación de los fondos municipales ha pasado a formar parte de la dinámica administrativa de muchas ciudades de la región²⁶¹. En este contexto, el uso de plataformas en línea en combinación con la Internet de las cosas puede dar lugar a debates sobre la rendición de cuentas, el control y la asignación de responsabilidad.

Iniciativas destacadas de ciudades inteligentes con Internet de las cosas en América Latina y el Caribe

En la Argentina ya son varias las ciudades que han implementado soluciones de Internet de las cosas²⁶². El municipio de Tigre, en el Gran Buenos Aires, fue uno de los primeros de América Latina y el Caribe en implementar un centro de operaciones para proteger a las personas y combatir el delito, empleando, entre otras cosas, cámaras de reconocimiento facial y de placas de autos para rastrear delincuentes y autos robados. Esta iniciativa se pudo concretar gracias a una asociación público-privada con empresas multinacionales y al análisis de datos en la nube²⁶³.

En Chacao y Maracay (República Bolivariana de Venezuela) se diseñó un mecanismo de “semáforos inteligentes” para las rutas. El sistema proporciona una mejor gestión del tráfico, reduciendo el tiempo que se pasa en la carretera y los accidentes de tráfico.

En Medellín (Colombia) se estableció un centro de operaciones integrado que coordina medidas de seguridad y emergencia, lo que permite a los organismos que trabajan en las áreas de seguridad, transporte, atención sanitaria de emergencia, gestión de desastres, medio ambiente y bienestar responder a una llamada de manera coordinada. El programa se basa en el uso extensivo de cámaras de vigilancia y la georreferenciación de llamadas.

²⁵⁸ Banco Interamericano de Desarrollo (BID), “Big Data urbana: una guía estratégica para ciudades”, 2019 [en línea] https://publications.iadb.org/publications/spanish/document/BIG_Data_urbana_Una_gu%C3%ADa_estrat%C3%A9gica_para_ciudades.pdf.

²⁵⁹ Banco Interamericano de Desarrollo (BID), *IoT en ALC 2019: tomando el pulso al Internet de las cosas en América Latina y el Caribe* [en línea] https://publications.iadb.org/publications/spanish/document/iot_en_ALC_2019_Tomando_el_pulso_al_Internet_de_las_Cosas_en_Am%C3%A9rica_Latina_y_el_Caribe_es.pdf.

²⁶⁰ Banco Interamericano de Desarrollo (BID), *La ruta hacia las Smart Cities: migrando de una gestión tradicional a la ciudad inteligente*, 2016 [en línea] <https://publications.iadb.org/publications/spanish/document/la-ruta-hacia-las-smart-cities-Migrando-de-una-gesti%C3%B3n-tradicional-a-la-ciudad-inteligente.pdf>.

²⁶¹ Banco Interamericano de Desarrollo (BID), “Big Data urbana: una guía estratégica para ciudades”, 2019 [en línea] https://publications.iadb.org/publications/spanish/document/BIG_Data_urbana_Una_gu%C3%ADa_estrat%C3%A9gica_para_ciudades.pdf.

²⁶² Véase un resumen de las distintas iniciativas de ciudades inteligentes en la Argentina [en línea] <https://www.camarabilbao.com/ccb/contenidos.downloadatt.action?id=5334087>.

²⁶³ Véase [en línea] <https://www.nec.com/en/case/tigre/index.html>.

En 2017, Chile lanzó un programa piloto en Temuco para buscar soluciones de ciudades inteligentes en una plataforma abierta. Se seleccionaron cuatro áreas principales: vigilancia de la calidad del aire, paradas de autobuses virtuales, gestión de la recolección de basura y gestión de incidentes en la ciudad²⁶⁴.

Itu, en el estado de São Paulo (Brasil), utiliza una asociación público-privada para gestionar la eliminación de desechos. El municipio utiliza un gran número de contenedores e instalaciones subterráneas de almacenamiento de desechos conectados a sensores que indican si es necesario hacer reparaciones o sustituciones, además de notificar los niveles de llenado. Esto permite mejorar el itinerario de los camiones de recogida, lo que reduce el tiempo, los costos y los efectos ambientales²⁶⁵.

El programa Chihuahua Ciudad Digital de México tiene por objeto la inclusión digital y el acceso a servicios digitales. La iniciativa es una asociación público-privada que proporciona cobertura wifi en varias áreas públicas del municipio, incluso en oficinas públicas y parques. El propósito es democratizar el acceso a Internet y a los servicios públicos digitales²⁶⁶.

En la ciudad de Nassau, en las Bahamas, se ha instalado un sistema de gestión de los recursos hídricos que detecta pérdidas, permite la reparación y el reemplazo avanzado de las tuberías, controla la presión y gestiona diferentes niveles de medición. Esto ha permitido al municipio reducir los costos y disminuir la pérdida de agua del 58% al 29%²⁶⁷.

3.2. La agricultura inteligente podría ser una gran oportunidad para la región

Algunos sectores de la economía de América Latina y el Caribe parecen estar más dispuestos que otros a emplear la Internet de las cosas en sus actividades, y el más dispuesto es el sector agrícola, que representa una parte sustancial de la economía en la mayoría de los países de la región y tiende a ser la base de las exportaciones²⁶⁸. El aumento de la productividad en esta esfera puede tener un impacto exponencial en el PIB y, accidentalmente, también puede tener un efecto positivo en el medio ambiente al conducir a un uso más eficiente de la tierra y otros recursos naturales²⁶⁹.

La agricultura inteligente y las empresas emergentes de tecnología agropecuaria pueden representar una importante oportunidad para la región²⁷⁰. La implantación de la tecnología de Internet de las cosas en el sector agrícola puede repercutir en muchas áreas, como la gestión de los cultivos, la agricultura de precisión, la vigilancia del ganado, la agricultura vertical intensiva (de interior y exterior) y el mejor uso de la acuicultura. La Internet de las cosas aplicada a las granjas puede tener un impacto positivo en toda la cadena de valor, al mejorar tanto la toma de decisiones como la eficiencia y la precisión de las medidas adoptadas. Puede revolucionarse desde la siembra hasta la supervisión, la cosecha, la distribución, el almacenamiento y la comercialización²⁷¹.

Una parte importante del valor agregado de la Internet de las cosas en la agricultura proviene del acceso a datos que de otro modo serían muy difíciles de recopilar. Dos ejemplos destacados son la humedad del suelo y los indicadores de microclima, que pueden variar considerablemente. La implementación de tecnologías vinculadas a la Internet de las cosas puede facilitar la planificación y la supervisión de estos indicadores. Los principales beneficios derivan de los análisis avanzados que dependen de la escala y el volumen de los datos disponibles, así como de las capacidades de procesamiento²⁷². Estos dos aspectos podrían dar lugar a que se presten servicios en distintas jurisdicciones y mediante asociaciones con entidades que operan a nivel transnacional²⁷³.

²⁶⁴ Véase [en línea] <https://www.ufro.cl/index.php/noticias/12destacadas/1424-temuco-sera-la-primer-ciudad-inteligente-de-chile-y-piloto-para-otras-ciudades-de-latinoamerica>.

²⁶⁵ Véase [en línea] <https://exame.abril.com.br/revista-exame/o-que-aprender-com-a-excecao/>.

²⁶⁶ Véase [en línea] https://www.researchgate.net/profile/Jose_Bordas-Beltran/publication/339389919_Chapter_11_Smart_territory_initiatives_in_an_emerging_economy/links/5e4ed07592851c7f7f48f66b/Chapter-11-Smart-territory-initiatives-in-an-emerging-economy.pdf.

²⁶⁷ Banco Interamericano de Desarrollo (BID), *La ruta hacia las Smart Cities: migrando de una gestión tradicional a la ciudad inteligente*, 2016 [en línea] <https://publications.iadb.org/publications/spanish/document/la-ruta-hacia-las-smart-cities-Migrando-de-una-gesti%C3%B3n-tradicional-a-la-ciudad-inteligente.pdf>.

²⁶⁸ Banco Interamericano de Desarrollo (BID), *La próxima despensa global: cómo América Latina puede alimentar al mundo. Un llamado a la acción para afrontar desafíos y generar soluciones*, 2018 [en línea] <https://publications.iadb.org/publications/spanish/document/la-pr%C3%BAxima-despensa-global-C%C3%BCmo-Am%C3%A9rica-Latina-puede-alimentar-al-mundo-Un-llamado-a-la-acci%C3%B3n-para-afrontar-desaf%C3%ADos-y-generar-soluciones.pdf>.

²⁶⁹ Banco Interamericano de Desarrollo (BID), *IoT en ALC 2019: tomando el pulso al Internet de las cosas en América Latina y el Caribe* [en línea] https://publications.iadb.org/publications/spanish/document/iot_en_ALC_2019_Tomando_el_pulso_al_Internet_de_las_Cosas_en_Am%C3%A9rica_Latina_y_el_Caribe_es.pdf.

²⁷⁰ Organización de las Naciones Unidas para la Alimentación y la Agricultura (FAO), "Smart farming is key for the future of agriculture", 2018 [en línea] <http://www.fao.org/family-farming/detail/en/c/897026/>.

²⁷¹ Véase [en línea] https://www.researchandmarkets.com/research/lv69c3/globql_iot_in?w=4.

²⁷² Véase [en línea] <https://www.researchandmarkets.com/reports/4600903/iot-in-agriculture-market-outlook-and-forecasts#relat-4669235>.

²⁷³ En un estudio del Banco Mundial se destaca que esas asociaciones son cruciales para el desarrollo del sector. Véase [en línea] <http://documents.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf>.

Pero los aspectos transfronterizos no terminan ahí. Muchas de estas soluciones de Internet de las cosas no vienen de empresas tradicionales del sector agrícola, como las que realizan actividades agrícolas, ni de proveedores convencionales, como los fabricantes o proveedores de equipos agrícolas, o los distribuidores de semillas, fertilizantes o productos químicos. Los desarrolladores de software y las empresas que trabajan en el análisis predictivo de datos cada vez se integran más a las operaciones agrícolas. Muchas de esas empresas no tradicionales no se encuentran radicadas en el mismo país que los usuarios (granjas) ni reciben asistencia o forman parte de una alianza o acuerdo con entidades en otros países. Un ejemplo claro es el uso de los servicios en la nube: la mayoría de los proveedores no están en la región y los datos no se procesan necesariamente a nivel local.

Novedades e iniciativas destacadas en materia de agricultura inteligente

El cultivo de arroz en Colombia se beneficia de un proyecto puesto en marcha en asociación con una empresa japonesa. La solución de Internet de las cosas tiene sensores que recopilan datos ambientales como la temperatura y la humedad del aire y del suelo, y la irradiancia solar. Este proyecto ha permitido tomar mejores decisiones y brindar respuestas más eficientes y oportunas²⁷⁴.

También se está prestando atención a la vigilancia del ganado, ya que es necesario controlar constantemente la ingesta de agua y pienso. En el Brasil, un proyecto puesto en marcha en asociación con empresas multinacionales ha facilitado el pesaje del ganado y el análisis de los datos sobre su crecimiento²⁷⁵. Además, tanto las empresas emergentes como las tradicionales proporcionan tecnología que controla la geolocalización de los rebaños y el estado de salud de los animales²⁷⁶. Otras gestionan toda la cadena “de la granja a la mesa”, agregando sensores e inteligencia agrícola a todos los procesos²⁷⁷. De manera similar, en la Argentina las empresas emergentes están ayudando a vigilar los cultivos y el ganado utilizando diversas estrategias, desde rastreadores de collar hasta drones autónomos, para captar y analizar información sobre las actividades agrícolas²⁷⁸.

En el Perú, algunas iniciativas buscan utilizar la Internet de las cosas para vigilar las condiciones ambientales y meteorológicas. Se despliegan antenas y drones para capturar datos de los campos en una serie de áreas que van desde la topografía hasta la calidad del aire²⁷⁹.

En Chile se están aprovechando recursos naturales disponibles en forma de viñedos genéticamente antiguos, combinándolos con la tecnología para producir, in vitro, un vivero para antiguas variedades de vides²⁸⁰.

En Guanajuato (Méjico) ha comenzado a funcionar un centro de tecnología agropecuaria que promueve una serie de proyectos para empresas, desde vigilancia de los cultivos hasta estrategias de irrigación²⁸¹.

4. Pagos digitales

Internet ha cambiado el panorama de una gran variedad de negocios en todo el mundo. En los últimos tiempos, el sector financiero ha experimentado las consecuencias de este cambio²⁸². Los nuevos servicios y modelos de negocios están aprovechando la conectividad del mundo en línea para reducir los obstáculos de ingreso al mercado financiero, de modo de poder proporcionar más productos y servicios a una base más amplia de clientes. Su naturaleza virtual significa que no necesitan tener sede en un país, pero pueden fomentar y posibilitar las transacciones transfronterizas.

²⁷⁴ Véase [en línea] <https://www.e-kakashi.com/en/case/details01>.

²⁷⁵ Véase [en línea] <https://blog.bosch-si.com/agriculture/connected-agriculture-beefed-up-networking-in-brazil/>. Para acceder a un estudio general sobre su despliegue en el sur del Brasil, véase [en línea] <https://www.lume.ufrgs.br/handle/10183/178439>.

²⁷⁶ Un ejemplo es Allflex (véase [en línea] <http://www.allflex.com.br/identificacao-eletronica/brincos-eletronicos-fdx/>). Otros ejemplos son Intergado, Cowmed e Imeve (véase [en línea] <https://www.beefpoint.com.br/o-olho-do-dono-que-engorda-o-boi-agora-e-digital/>).

²⁷⁷ Por ejemplo, BovControl [en línea] <https://www.bovcontrol.com>; <http://gi.globo.com/tecnologia/blog/startup/post/app-permite-a-fazendeiro-monitorar-bois-e-vacas-na-tela-do-pc.html>.

²⁷⁸ Por ejemplo, Tambero conecta información agrícola a una plataforma de servicio en la nube (véase [en línea] <https://www.tambero.com>). En el otro extremo del espectro, Skyagro usa drones autónomos para recolectar los datos necesarios (véase [en línea] <https://www.infocampo.com.ar/skyagro-drones-hechos-en-argentina-que-toman-y-analizan-imagenes-en-los-campos/>).

²⁷⁹ Dos empresas emergentes peruanas —Spacedat y Qaira— son ejemplos relevantes. Véanse [en línea] <http://www.qairadrone.com/index.php?r=site/nosotros> y <https://www.spacedat.com>.

²⁸⁰ Véase [en línea] <https://www.andeswines.com/business-acceleration-service/>.

²⁸¹ Véase [en línea] <http://agrobioteg.org>.

²⁸² El Banco Mundial y el Fondo Monetario Internacional (FMI) promovieron la Agenda de Bali sobre Tecnofinanzas, donde se destacan las oportunidades y los riesgos a los que se enfrentan los proveedores de servicios financieros innovadores. Véase [en línea] <https://www.worldbank.org/en/topic/fintech>.

Aún sigue habiendo, sin embargo, una gran brecha entre las personas que reciben servicios de instituciones financieras tradicionales y aquellas que no los reciben. Una parte sustancial de la población está desatendida o excluida de los servicios financieros. Estas brechas representan un importante obstáculo para un mercado único digital; o se disuade a las personas de ingresar al mercado o estas simplemente no son capaces de acceder. En consecuencia, los bienes y servicios suministrados a través de Internet también se ven afectados: a una parte importante de la población le resultan inaccesibles o le es muy difícil acceder a ellos.

En América Latina y el Caribe esto se ve agravado por la penetración relativamente baja de los servicios bancarios y las tarjetas de crédito internacionales, una cultura del dinero en efectivo difícil de abandonar y la volatilidad de las divisas. Esto supone una oportunidad para que quienes ingresan al mercado puedan encontrar soluciones novedosas, y no solo ofrecer nuevos productos y servicios, sino también aumentar el acceso al financiamiento²⁸³.

Por consiguiente, las empresas emergentes y los proyectos innovadores están tratando de hacer frente a las asimetrías de la región en materia de acceso financiero²⁸⁴. América Latina y el Caribe está experimentando un auge de empresas que alinean nuevas tecnologías con novedosas oportunidades del mercado financiero²⁸⁵. Se constata un extraordinario crecimiento del llamado “mercado de las tecnofinanzas” con iniciativas que se han extendido a distintas áreas²⁸⁶. Dos han cobrado especial impulso en la región: los pagos digitales, apoyados por el crecimiento de nuevas empresas bancarias (neobancos), y las tecnologías de cadenas de bloques, tanto en forma de criptomonedas como de otras posibles aplicaciones que se analizarán más adelante.

Los interesados que fueron entrevistados y encuestados destacaron esta tendencia y la importancia que están teniendo las tecnofinanzas en la región. Han subrayado su potencial para reducir la desigualdad de acceso a los servicios financieros y para aprovechar el mercado digital. También observaron, sin embargo, que las iniciativas de armonización pueden resultar más difíciles debido a las diferencias que existen en la región en cuanto a tradiciones de regulación financiera y al tamaño y la naturaleza dispar de las economías.

4.1. Efectos jurisdiccionales transfronterizos en las actividades de las empresas de tecnofinanzas

Los mecanismos de pago son cruciales para el desarrollo del comercio digital de bienes y servicios. La capacidad de efectuar pagos en forma digital no es algo que se dé por sentado, sobre todo en las transacciones transfronterizas. Es necesario que los mecanismos de pago sean eficientes y asequibles para que sirvan de conducto a fin de que los fondos fluyan de un lado a otro en una transacción en línea²⁸⁷. Por consiguiente, los aspectos económicos de las transacciones por Internet dependen o pueden resolverse a través de una serie de intermediarios de varios niveles que mantienen la infraestructura de pagos digitales.

Ningún mercado digital puede funcionar correctamente si no existen mecanismos de pago accesibles y asequibles. En América Latina y el Caribe, el entorno financiero está repleto de oportunidades para desarrollar novedosos enfoques, ya sean nuevos modelos de negocio o nuevos productos y servicios. El aumento de la disponibilidad de teléfonos inteligentes y de la conectividad móvil también ha impulsado el cambio hacia los primeros enfoques en línea e incluso móviles.

En la región existen múltiples soluciones bancarias y de pago digital. El mercado se está moviendo hacia novedosos abordajes, lo que ha motivado la creación de un ecosistema de empresas que los proveen.

²⁸³ Banco Interamericano de Desarrollo (BID), *FINTECH: Innovaciones que no sabías que eran de América Latina y el Caribe*, 2018 [en línea] <https://publications.iadb.org/publications/spanish/document/FINTECH-Innovaciones-que-no-sab%C3%ADas-que-eran-de-Am%C3%A9rica-Latina-y-Caribe.pdf>.

²⁸⁴ Banco Interamericano de Desarrollo (BID), *Sandbox regulatorio en América Latina y el Caribe para el ecosistema Fintech y el sistema financiero*, 2018 [en línea] <https://publications.iadb.org/es/publicacion/17483/sandbox-regulatorio-en-america-latina-el-caribe-para-el-ecosistema-fintech-y-el>.

²⁸⁵ Banco Interamericano de Desarrollo (BID)/Finnovista, *Fintech. América Latina 2018: crecimiento y consolidación* [en línea] <https://publications.iadb.org/publications/spanish/document/Fintech-Am%C3%A9rica-Latina-2018-Crecimiento-y-consolidaci%C3%B3n.pdf>.

²⁸⁶ Comisión Económica para América Latina y el Caribe (CEPAL), *Datos, algoritmos y políticas: la redefinición del mundo digital* (LC/CMSI.6/4), Santiago, 2018.

²⁸⁷ Véase [en línea] <https://www.fsb.org/wp-content/uploads/P090420-2.pdf>.

El sector de las tecnofinanzas en América Latina y el Caribe está compuesto por cientos de empresas emergentes y nuevas iniciativas lanzadas por agentes más tradicionales²⁸⁸. En 2018, por ejemplo, el Brasil ya tenía 380 empresas emergentes de tecnofinanzas, en tanto que México tenía 273, Colombia contaba con 148, la Argentina tenía 116 y Chile tenía 84²⁸⁹. Estas empresas realizan distintas actividades. Entre las más importantes se encuentran: soluciones relacionadas con transferencias y gestión de dinero; transferencias y remesas internacionales; puntos de venta móviles; pasarelas de pago y coeficientes de agregación para aceptar, autorizar y procesar pagos en plataformas digitales; y neobancos, entidades de financiamiento de alta tecnología que poseen licencias bancarias propias o de terceros²⁹⁰.

Varias de estas empresas ofrecen servicios transfronterizos (por ejemplo, remesas internacionales) o son empresas transfronterizas que han internacionalizado sus operaciones. Las iniciativas gubernamentales son importantes para ofrecer un marco institucional que promueva el crecimiento y cree las condiciones para nuevas soluciones financieras. Los intentos de fomentar la convergencia regulatoria podrían contribuir a que estas empresas logren asegurar mercados regionales e internacionales. Sin embargo, es necesario tener en cuenta los aspectos jurisdiccionales transfronterizos para promover y no obstaculizar el proceso.

La tendencia a regular el sector tecnofinanciero que ya se verifica ha creado una oportunidad de coordinación y cooperación entre los países de la región. En julio de 2018, por ejemplo, los miembros de la Alianza del Pacífico acordaron un conjunto de principios rectores para la regulación de las tecnofinanzas²⁹¹.

En el plano nacional, los países de la región están explorando dos caminos en lo que respecta a la regulación del sector tecnofinanciero: i) la regulación en su conjunto, lo que incluye los pagos digitales y la nueva banca digital, y ii) la regulación adaptando el marco jurídico vigente²⁹².

México, por ejemplo, ha sido pionero con una legislación general para regular la industria tecnofinanciera²⁹³. La legislación se ocupa de cuatro áreas principales: i) instituciones de tecnología financiera, incluidas empresas de financiamiento colectivo e instituciones de pago electrónico; ii) activos virtuales (criptomonedas); iii) interfaz de programación de aplicaciones (API), y iv) entornos de prueba regulatorios (sandboxes). El Brasil, por su parte, adoptó otro enfoque y optó por integrar las cuestiones de las tecnofinanzas a la reglamentación vigente²⁹⁴. Honduras ha emitido un reglamento para permitir el uso de billeteras electrónicas²⁹⁵, en tanto que el Perú tiene una reglamentación similar²⁹⁶, al igual que El Salvador²⁹⁷. En Colombia, los diferentes actores están debatiendo si es necesario contar con un marco regulatorio específico para el sector tecnofinanciero²⁹⁸.

4.2. La banca abierta y el ecosistema de las tecnofinanzas

La banca abierta es una de las iniciativas que en la región están creciendo desde dentro del ecosistema de las tecnofinanzas. Es una oportunidad para generar la infraestructura jurídica y técnica necesaria para un entorno financiero más competitivo. La banca abierta hace que los diferentes servicios financieros sean interoperables y abre el mercado para que los usuarios puedan elegir compartir sus datos financieros con distintas instituciones financieras y beneficiarse de un conjunto más amplio de productos y servicios. Establece un entorno de intercambio de datos entre industrias, integrando diferentes plataformas e infraestructuras. Por lo general, implica el desarrollo de una interfaz de programación de aplicaciones (API) que permite la interacción de diferentes proveedores de servicios financieros.

²⁸⁸ Banco Interamericano de Desarrollo (BID)/Finnovista, *Fintech. América Latina 2018: crecimiento y consolidación* [en línea] <https://publications.iadb.org/publications/spanish/document/Fintech-Am%C3%A9rica-Latina-2018-Crecimiento-y-consolidaci%C3%B3n.pdf>.

²⁸⁹ Según Finnovista, los números son incluso más altos en 2020. Véase [en línea] <https://www.finnovista.com/tag/fintech-radar/>.

²⁹⁰ Banco Interamericano de Desarrollo (BID)/Finnovista, *Fintech. América Latina 2018: crecimiento y consolidación* [en línea] <https://publications.iadb.org/publications/spanish/document/Fintech-Am%C3%A9rica-Latina-2018-Crecimiento-y-consolidaci%C3%B3n.pdf>.

²⁹¹ Véase [en línea] <https://alianzapacifico.net/wp-content/uploads/Principios-orientadores-para-la-regulaci%C3%B3n-Fintech.pdf>.

²⁹² Fondo Monetario Internacional (FMI), "Fintech: the experience so far", junio de 2019 [en línea] <https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056>.

²⁹³ Ley para regular las instituciones de tecnología financiera, marzo de 2018 [en línea] <https://perma.cc/SB6N-RQY7>.

²⁹⁴ Fondo Monetario Internacional (FMI), "Fintech: the experience so far", junio de 2019 [en línea] <https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056>.

²⁹⁵ Véase [en línea] <https://www.elheraldo.hn/pais/936203-466/uso-de-la-billetera-electr%C3%B3nica-ser%C3%A1-legal-en-honduras>.

²⁹⁶ Véase [en línea] <https://www.mef.gob.pe/es/por-instrumento/decreto-supremo/9970-decreto-supremo-n-090-2013-ef/file>.

²⁹⁷ Véase [en línea] https://www.bcr.gob.sv/regulaciones/upload/NORMAS_PARA_LA_AUTORIZACION_DE_ADMINISTRADORES_DE_SISTEMAS_DE_PAGOS_MOVILES.pdf?y=1589709520.

²⁹⁸ Banco Interamericano de Desarrollo (BID)/Finnovista, "Fintech en Costa Rica: hacia una evolución de los servicios financieros" [en línea] <https://www.finnovista.com/informe/fintech-costa-rica-hacia-evolucion-servicios-financieros/>.

El alcance de la mayoría de estas iniciativas indica que aparentemente hay poca conciencia respecto del potencial transfronterizo de la banca abierta. En virtud de un marco jurídico regional o más amplio, los clientes podrían beneficiarse de los productos y servicios financieros proporcionados por una red mucho más grande de proveedores. Al mismo tiempo, la internacionalización del sector tecnofinanciero de la región conducirá a la exportación de diferentes soluciones de banca abierta que pueden entrar en conflicto o tener que reformarse.

A nivel internacional, las iniciativas han seguido una de dos vías posibles: una impulsada por el mercado, en la que la industria, el gobierno o una asociación de ambos establece directrices y normas comunes, y después deja al mercado libre para desarrollarse sobre esa base; y otra reglamentaria, en la que las autoridades gubernamentales establecen el marco general que deben seguir las instituciones financieras.

En la región, al menos dos países parecen haber tomado la segunda vía. El 4 de mayo de 2020, el Brasil emitió una serie de reglamentos a través de sus instituciones de supervisión financiera. La aplicación se divide en cuatro fases, lo que da cierto margen a la industria para establecer sus propias normas de intercambio de datos y proporcionar acceso a los servicios²⁹⁹. El marco legal propuesto por México para la banca abierta forma parte de sus reglamentos de tecnofinanzas³⁰⁰. En otros países de la región, la propia industria ha impulsado la reglamentación para que el sector pueda avanzar³⁰¹.

4.3. Soluciones reglamentarias innovadoras: el atractivo de los entornos de prueba regulatorios (*sandboxes*)

Las nuevas soluciones financieras de alta tecnología dependen de la experimentación y la innovación en los productos y servicios financieros, y de los modelos de negocios. Sin embargo, esto puede acarrear riesgos individuales o sistémicos que deben explorarse de antemano. Por lo general, la reglamentación tradicional no es capaz de abarcar estos marcos innovadores de manera oportuna. Muchos países, por consiguiente, están probando marcos regulatorios no tradicionales para hacer frente a esos riesgos de manera segura y en un plazo eficiente. Los entornos de prueba regulatorios se propusieron como una estrategia atractiva y algunos Estados, incluidos varios de América Latina y el Caribe, ya los están aplicando.

Los entornos regulatorios controlados permiten que las soluciones innovadoras funcionen para un número restringido de usuarios (clientes) y durante un tiempo limitado. Las iniciativas a menudo están sujetas a obligaciones menos estrictas, a condición de que sean vigiladas y supervisadas continuamente por un órgano gubernamental autorizado.

Estos entornos tienen la ventaja de ser campos de prueba para nuevos proyectos. Limitan el impacto y, por consiguiente, al mismo tiempo restringen los riesgos, permitiendo que las autoridades supervisoras vigilen las reacciones de los agentes y que el mercado proponga enfoques, normas y reglas específicas.

La mayoría de las partes interesadas encuestadas declararon que los enfoques innovadores, como los entornos regulatorios controlados, contribuían a fomentar el crecimiento económico regional. Destacaron las diferencias en las economías de los países de la región, la posible falta de capacidad institucional y la limitada disponibilidad de recursos humanos como posibles obstáculos para la posibilidad de aplicación de estas soluciones regulatorias.

Estas reflexiones ponen de relieve la necesidad y la oportunidad de la cooperación y la coordinación transfronterizas. Los países de la región pueden aprovechar su proximidad y aunar recursos. El establecimiento de normas y enfoques comunes puede facilitar la labor de supervisión y disminuir la variación en materia regulatoria. Como consecuencia se puede brindar servicios a los clientes que están excluidos o desatendidos por el sector de los servicios financieros tradicionales.

²⁹⁹ Véase [en línea] <https://www.bcb.gov.br/en/pressdetail/2284/nota>. Véase el contenido de la Resolución Conjunta N°. 4, 2020 (en portugués) [en línea] <http://www.in.gov.br/en/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055>.

³⁰⁰ Véase [en línea] <https://iupana.com/2020/02/28/mexicos-fintech-law-open-banking-rules-delayed/?lang=en#widget/?lang=en>.

³⁰¹ Véase por ejemplo el estudio presentado por FinteChile y EY sobre el futuro de la banca abierta en Chile [en línea] https://www.ey.com/es_cl/financial-services/open-banking--oportunidades-y-desafios-para-chile. Colombia Fintech ha buscado, en asociación con entidades del Reino Unido, establecer normas para la banca abierta para el entorno colombiano. Véase [en línea] <https://www.ebankingnews.com/noticias/open-banking-desafios-y-oportunidades-en-colombia-0047125>. Véase un análisis del entorno colombiano en D. P. García Abella y J. C. Segura Cárdenas "Open Banking: del concepto a la competencia" [en línea] https://repository.eafit.edu.co/bitstream/handle/10784/14228/DianaPatricia_GarciaAbella_2019_JuanCarlos_SeguraCardenas_2019.pdf?sequence=2&isAllowed=y.

Algunos países de la región ya están implementando estas soluciones y pueden marcar el rumbo. Por ejemplo, en la ley de México que regula las empresas del sector tecnofinanciero³⁰² se incluye la posibilidad de autorizaciones temporales para “nuevos modelos financieros”³⁰³. De manera similar, la Superintendencia Financiera de Colombia ha establecido un marco jurídico que permite el uso de entornos regulatorios controlados para iniciativas financieras innovadoras³⁰⁴. El Brasil tiene iniciativas de entornos regulatorios controlados supervisadas por el Banco Central³⁰⁵ y la Comisión de Valores Mobiliarios (CVM)³⁰⁶. Las asociaciones industriales también han presentado propuestas, y una federación internacional de asociaciones nacionales tiene por objeto crear una sinergia regulatoria en la región³⁰⁷.



Fuente: Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL).

Algunos países de América Latina y el Caribe han utilizado marcos innovadores (por ejemplo, entornos regulatorios controlados) para permitir experimentos en materia de tecnofinanzas y tecnologías de pago digital. ¿Cree que esa estrategia contribuye a fomentar el crecimiento económico regional?

5. Cadena de bloques y criptomonedas

La cadena de bloques es otra tecnología que se está desarrollando para facilitar las transacciones. Por cadena de bloques puede entenderse un registro distribuido en el que se guardan las transacciones entre pares, sin necesidad de que una autoridad central lo coordine. Satoshi Nakamoto conceptualizó la tecnología en 2008 para eliminar el intermediario de confianza habitual en la mayoría de las transacciones³⁰⁸. Se trata de un elemento que ayuda a enfrentar la incertidumbre. Debido a la naturaleza distribuida del registro, su carácter inmutable (a prueba de manipulaciones) y su naturaleza autoejecutable, no es necesario que las partes se conozcan o confíen unas en otras. La confianza es el resultado del uso de la cadena de bloques³⁰⁹.

En el informe *Internet & Jurisdiction Global Status Report 2019* ya se había puesto de relieve el interés con que los sectores tanto público como privado habían acogido esta tecnología a nivel internacional. En este informe, no obstante, también se hace referencia al considerable escepticismo que algunos interesados, especialmente los Estados, han mostrado con respecto a ciertas aplicaciones, en particular las criptomonedas. Bitcoin, de hecho, se ha vuelto muy conocida como una de esas monedas. Las dificultades jurídicas con estas monedas y cadenas de bloques en general surgen de las mismas características que, en la mayoría de los casos, las hacen atractivas: la falta de una autoridad central focal y el hecho de que las personas no tengan que conocerse ni confiar unas en otras.

³⁰² Ley para regular las instituciones de tecnología financiera, marzo de 2018 [en línea] <https://perma.cc/SB6N-RQY7>.

³⁰³ Véase C. Kurc y A. Portilla, “Mexico: Fintech 2019. International Comparative Legal Guides” [en línea] <https://iclg.com/practice-areas/fintech-laws-and-regulations/mexico>.

³⁰⁴ Véase [en línea] <https://forbes.co/2020/02/06/economia-y-finanzas/hacienda-cobijara-con-decreto-el-sandbox-de-la-superfinanciera/>.

³⁰⁵ Véase [en línea] <https://www.centralbanking.com/fintech/4397616/sandbox-initiative-central-bank-of-brazil>. Véase un breve análisis que indica que este puede ser un innovador enfoque sectorial del entorno regulatorio controlado [en línea] <https://www.jota.info/coberturas-especiais/inova-e-acao/banco-central-ganha-premio-de-melhor-initiativa-de-sandbox-do-mundo-04092019>.

³⁰⁶ El 15 de mayo de 2020, la CVM emitió la Instrucción núm. 626/2020 que implementa los entornos regulatorios controlados. Véase [en línea] <http://www.cvm.gov.br/noticias/arquivos/2020/20200515-1.html>.

³⁰⁷ Véase [en línea] http://fintechiberoamerica.com/wp-content/uploads/2018/06/protocolo_implementacion_sandbox_iberoamerica.pdf.

³⁰⁸ S. Nakamoto “Bitcoin: A peer-to-peer electronic cash system”, 2008 [en línea] <https://bitcoin.org/bitcoin.pdf>.

³⁰⁹ Comisión Económica para América Latina y el Caribe (CEPAL), *Datos, algoritmos y políticas: la redefinición del mundo digital* (LC/CMSI.6/4), Santiago, 2018.

El carácter distribuido y desmaterializado del registro hace que las fronteras y los elementos jurisdiccionales tradicionales sean mucho menos relevantes. La cadena de bloques permite el comercio transfronterizo de todo tipo, sin que necesariamente haya un intermediario que lo supervise e inspeccione. Esto significa que puede haber tanto transacciones legales como ilegales sin el conocimiento de las autoridades o la necesidad de fijar jurisdicción.

En consecuencia, los debates sobre la cadena de bloques y las criptomonedas suelen centrarse en los contextos potencialmente ilegales donde pueden producirse las transacciones. Por una parte, pueden apoyar actividades delictivas, ya que todo puede pasar fácilmente de una mano a otra, a distancia y sin que haya una autoridad que controle. Por otra parte, estas tecnologías parecen anónimas porque no se registra ninguna información sobre la identidad de las personas que participan en la transacción. No obstante, esto no necesariamente significa que no se pueda identificar a los implicados. El protocolo de la cadena de bloques permite la trazabilidad de todas las transacciones, lo que hace posible que se pueda recrear todo el recorrido del dinero. En este sentido, es mucho menos anónimo que el dinero en efectivo, al que resulta difícil seguirle el rastro una vez que pasa de una mano a otra.

La cadena de bloques puede tener muchas aplicaciones en diferentes áreas, además de las criptomonedas. Se utiliza sobre todo para el registro de tierras y propiedades, y los llamados “contratos inteligentes”, pero puede desplegarse en muchas esferas, tanto privadas como públicas, donde sirve para crear un registro en línea fiable con funciones automatizadas³¹⁰. En lo que respecta a los “contratos inteligentes”, el término no significa necesariamente que se trate de contratos hechos con una cadena de bloques. Sin embargo, los contratos habilitados por una cadena de bloques se consideran inteligentes de tres maneras: pueden registrarse permanentemente en la cadena de bloques, sus cláusulas pueden estar basadas en un código y hay una “garantía de ejecución” debido a la aplicación automática a través de la red de cadenas de bloques³¹¹. Las implicancias son enormes y pueden cambiar el panorama jurídico de muchos sectores.

La escalabilidad, la privacidad de los datos y la interoperabilidad se consideran grandes desafíos. La primera depende de las operaciones de la red de cadenas de bloques y de la tecnología que la sustenta. En lo que respecta a la privacidad, la cuestión principal es el ejercicio de los derechos del interesado³¹².

La interoperabilidad suele ser uno de los problemas más difíciles. Si no hay normas técnicas comunes bien definidas, el ecosistema puede fragmentarse y los beneficios de la cadena de bloques pueden verse limitados. Por consiguiente, la normalización es esencial para mejorar la competitividad y elevar los niveles generales de cumplimiento de otras normas y valores, como la protección de los derechos humanos y la privacidad, a lo que ya se ha hecho referencia³¹³.

Hasta ahora, la Organización Internacional de Normalización (ISO)³¹⁴ y la UIT³¹⁵ han tomado la iniciativa en la elaboración de normas mundiales. La región de América Latina y el Caribe aún debe hacer un esfuerzo coordinado para participar en los foros mundiales de establecimiento de normas o para establecer sus propias normas regionales.

Sin embargo, hay algunas iniciativas nacionales que apuntan a regular la cadena de bloques. La tendencia es centrarse en los aspectos financieros de la tecnología, en particular en las criptomonedas. Las Bermudas han emitido un reglamento específico que abarca las criptomonedas y tienen previsto convertirse en un centro internacional para el comercio de lo que se define como “activos digitales”, incluidos, entre otros, los activos basados en cadenas de bloques³¹⁶. En Colombia, el Parlamento está debatiendo un proyecto de ley específico sobre criptoactivos y monedas virtuales³¹⁷.

³¹⁰ Véase una amplia gama de posibles aplicaciones en Comisión Económica para América Latina y el Caribe (CEPAL), *Datos, algoritmos y políticas: la redefinición del mundo digital (LC/CMSL6/4)*, Santiago, 2018.

³¹¹ D. Tapscott y A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 2016.

³¹² C. Kuner y otros, “Blockchain versus data protection”, *International Data Privacy Law*, vol. 8, N° 2, mayo de 2018, págs. 103 y 104 [en línea] <https://academic.oup.com/idpl/article/8/2/103/5047578>.

³¹³ Anna-Maria Osula, “The Global Rush for Standards in the Blockchain”, abril de 2020 [en línea] <https://directionsblog.eu/the-global-rush-for-standards-in-blockchain/>.

³¹⁴ ISO/TC 307. [en línea] https://isotc.iso.org/livelink/livelinkfetch/2000/2122/687806/ISO_TC_307__Blockchain_and_distributed_ledger_technologies_.pdf?nodeid=19772644&vernum=2.

³¹⁵ Unión Internacional de Telecomunicaciones (UIT), “Focus Group on Application of Distributed Ledger Technology” [en línea] <https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx>.

³¹⁶ Véase [en línea] <http://www.bermudalaws.bm/laws/Annual%20Laws/2018/Acts/Digital%20Asset%20Business%20Act%202018.pdf>. Véanse las reglamentaciones introducidas por la Autoridad Monetaria de las Bermudas [en línea] <https://www.bma.bm/document-centre/policy-and-guidance-digital-asset-business>.

³¹⁷ Véase [en línea] <http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%200028-18%20Criptomonedas.pdf>.

En la Ley Fintech de México se adopta un enfoque ligeramente distinto y, por ejemplo, se establece un conjunto de normas para trabajar con “activos virtuales”³¹⁸. El Gobierno de Chile está siguiendo un camino similar y ha propuesto regular las aplicaciones financieras de la cadena de bloques en virtud de reglamentaciones de tecnofinanzas³¹⁹. La Argentina, como uno de los principales centros regionales de comercio de criptomonedas, está estudiando una serie de opciones de reglamentación, incluidas regulaciones específicas de tecnofinanzas³²⁰.

Algunas Administraciones han buscado utilizar los reglamentos administrativos emitidos por los bancos centrales y otros organismos de supervisión financiera para proporcionar directrices sobre los criptoactivos³²¹.

En cuanto a los impuestos, varios países han tratado de interpretar su legislación vigente para incluir las criptomonedas y frenar la posibilidad de fraude financiero³²². Aún hay grandes áreas en las que América Latina y el Caribe puede diseñar una iniciativa coordinada y cooperativa.

En los debates que se realicen en el futuro se debería distinguir claramente entre las criptomonedas y la cadena de bloques en tanto tecnología genérica con muchas y muy diversas aplicaciones posibles.

Iniciativas y casos regionales dignos de mención

El Banco Central del Caribe Oriental ha diseñado un programa piloto para facilitar el cumplimiento con las normas internacionales de presentación de informes sobre el blanqueo de dinero y el financiamiento del terrorismo, y ha creado una “moneda basada en cadenas de bloques” que se encuentra a disposición de varios Estados del Caribe³²³.

En 2018, la República Bolivariana de Venezuela anunció un plan para lanzar una criptomoneda respaldada por el petróleo, llamada “petro”. El plan consistía en emitir 100 millones de petros (a un precio equivalente a 6.000 millones de dólares), con la intención de facilitar las transacciones internacionales y reducir la dependencia de monedas como el dólar o el euro³²⁴.

El Banco Interamericano de Desarrollo (BID) lanzó LACChain, una alianza mundial para promover el uso de las cadenas de bloques en América Latina y el Caribe, con el fin de coordinar los esfuerzos y desarrollar la tecnología de cadenas de bloques en la región. Ya se ha identificado la falta de coordinación y normalización como uno de los principales obstáculos que impiden el desarrollo del ecosistema de cadenas de bloques en la región.

6. Corrientes de datos internacionales y regionales: regímenes de protección de datos

La privacidad (o la protección) de los datos ha cobrado impulso en los últimos cinco años en América Latina y el Caribe. Algunos factores son muy importantes para que esto ocurra. El más destacado es el impacto que ha tenido el Reglamento General de Protección de Datos (RGPD) de la Unión Europea en el ordenamiento jurídico transnacional. Este instrumento ha llevado a muchos países a revisar la legislación de protección de datos o crear una propia. El potencial de acceso —o su falta— al mercado europeo de datos es importante para muchos países, y la Unión Europea se considera un modelo regulatorio para los esfuerzos nacionales.

³¹⁸ Ley para regular las instituciones de tecnología financiera, marzo de 2018 [en línea] <https://perma.cc/SB6N-RQY7>. Véase una visión positiva de la aplicación de la cadena de bloques en México en Y. Martínez, “Compartimos los avances y retos de la estrategia digital en el Foro OCDE México 2018”, Gobierno de México, 2018 [en línea] <https://www.gob.mx/mexicodigital/articulos/compartimos-los-avances-y-retos-de-la-estrategia-digital-en-el-foro-ocde-mexico-2018>.

³¹⁹ Véase [en línea] <https://www.criptonoticias.com/gobiernoregulacion/gobierno-chileno-adelanta-proyecto-regulacion-criptoactivos-2019/>.

³²⁰ Véase [en línea] <https://www.ambito.com/politica/criptomonedas/senado-analizo-regular-el-uso-las-la-argentina-n5066872>.

³²¹ El Brasil y Costa Rica son dos ejemplos. Véase Banco Central del Brasil, *Comunicado*, N°. 31.379, 16 de noviembre de 2017 [en línea] <https://perma.cc/G4GM-8HV6>; Banco Central de Costa Rica, *Posición del Banco Central de Costa Rica (BCCR) y sus Órganos de Desconcentración Máxima (ODM) con respecto a las criptomonedas*, octubre de 2017 [en línea] <https://perma.cc/KD4P-WX88>.

³²² Fondo Monetario Internacional (FMI), “Fintech in Latin America and the Caribbean: Stocktaking”, 2019 [en línea] <https://www.imf.org/en/Publications/WP/Issues/2019/03/26/Fintech-in-Latin-America-and-the-Caribbean-Stocktaking-46677>.

³²³ Véase [en línea] <https://www.eccb-centralbank.org/news/view/eccb-to-issue-worlds-first-blockchain-based-digital-currency>.

³²⁴ Véase [en línea] <https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/>.

Otro evento importante fue el escándalo de Cambridge Analytica. La empresa, con sede en el Reino Unido, hizo un perfil del electorado para prestar servicios de consultoría electoral, tratando de inferir quién votaría por cada partido y de influir en las opiniones de los indecisos, supuestamente bombardeándolos con opiniones unilaterales o desinformación en el proceso. A raíz de este caso, países de todo el mundo decidieron que sería prudente contar con leyes de protección de datos lo suficientemente fuertes como para desalentar ese comportamiento y salvaguardar el proceso democrático.

Además, la digitalización de distintos aspectos de la sociedad, incluidos los servicios públicos, y las violaciones de la ciberseguridad que vinieron después han despertado una mayor conciencia en la población. La gente sabe que sus datos personales se recolectan y que si se produce una violación cualquiera podría acceder a ellos.

6.1. Fuerte desarrollo de reglamentos de protección de datos en los países de América Latina y el Caribe

En la región se ha registrado un aumento de las iniciativas de reglamentación relativas a la protección de datos. En 2012, según un estudio realizado por la OEA, 24 países de la región no contaban con legislación sobre protección de datos o los instrumentos internos de los que disponían solo abarcaban algunos sectores específicos, lo que hacía que muchos aspectos de los datos personales no estuvieran protegidos por ningún instrumento jurídico en particular³²⁵.

En la actualidad, 16 países cuentan con una reglamentación específica de protección de datos: Antigua y Barbuda, Argentina, Bahamas, Brasil, Chile, Colombia, Costa Rica, México, Nicaragua, Panamá, Perú, República Dominicana, Saint Kitts y Nevis, Santa Lucía, Trinidad y Tabago y Uruguay. Seis países están discutiendo un proyecto de ley (Barbados, Ecuador, Guatemala, Honduras, Jamaica y Paraguay) y 11 países aún no tienen una reglamentación específica de protección de datos (Belice, Bolivia (Estado Plurinacional de), Cuba, Dominica, El Salvador, Granada, Guyana, Haití, San Vicente y las Granadinas, Suriname y Venezuela (República Bolivariana de)).

No obstante, la mayoría de los 11 países que no cuentan con una reglamentación general de protección de datos ha adoptado medidas para proteger los datos personales a algún nivel. Dominica, Granada y San Vicente y las Granadinas son partes en la Organización de Estados del Caribe Oriental (OECS), que ha aprobado el proyecto de ley de protección de datos como parte del E-Government for Regional Integration Project (Proyecto de gobierno electrónico para la integración regional)³²⁶. Belice, Guyana, Haití y Suriname, en su calidad de miembros de la CARICOM, también han participado en iniciativas relacionadas con la protección de datos: la Harmonization of ICT Policies, Legislation and Regulatory Procedures in the Caribbean (HIPCAR) (Armonización de las políticas, la legislación y los procedimientos reglamentarios en materia de TIC en el Caribe) ofrece una serie de políticas de protección de datos que sirven de directrices reglamentarias³²⁷.

Cabe resaltar algunos puntos. Los países que ya cuentan con una legislación general de protección de datos están experimentando un proceso de reforma y modernización que ha dado lugar a la adopción de normas similares a las del Reglamento General de Protección de Datos (RGPD) de la Unión Europea. La Argentina³²⁸ y Chile³²⁹ son dos ejemplos destacados. Barbados también está estudiando la posibilidad de promulgar una legislación de protección de datos inspirada en la reglamentación europea³³⁰.

6.2. ¿Hacia un marco regional de protección de datos?

Los interesados entrevistados destacaron las disparidades institucionales que existen en la región en materia de protección de datos personales. Uno de los encuestados hizo hincapié en la necesidad de una coordinación regional y el establecimiento de normas comunes de protección de datos personales que sean verdaderamente regionales.

³²⁵ Organización de los Estados Americanos (OEA), "Estudio comparativo: protección de datos en las Américas. Diversos regímenes jurídicos, políticas y mecanismos de aplicación existentes para la protección de datos personales, incluidas leyes, reglamentos y autorregulación nacionales", 2012, pág. 8 [en línea] <https://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12.pdf>.

³²⁶ Organización de Estados del Caribe Oriental (OECS), "Data Protection Act", 2016 [en línea] <https://www.oecs.org/en/procurement/e-gov/data-protection-act>.

³²⁷ Véase [en línea] <https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx>.

³²⁸ En la Argentina se han realizado varios cambios en las reglamentaciones de protección de datos, incluida una gran reforma de la legislación general de protección de datos, a fin de asemejarla más al RGPD de la Unión Europea. Véase [en línea] <https://www.oecd-ilibrary.org/sites/5f8ec188-en/index.htm?itemId=/content/component/5f8ec188-en>.

³²⁹ Jaime Urzúa, "Avances en el Proyecto de ley sobre protección de datos personales", septiembre de 2019 [en línea] <https://www.alessandri.legal/avances-en-el-proyecto-de-ley-sobre-proteccion-de-datos-personales/>.

³³⁰ Bartlett D. Morgan, "Barbados: a modern data protection regime", septiembre de 2019 [en línea] <https://platform.dataguidance.com/opinion/barbados-modern-data-protection-regime>.

Algunos países de la región, como la Argentina³³¹ (2000), el Uruguay³³² (2008) y México (2010), han promulgado leyes de protección de datos en la última década, mientras que otros, como el Brasil (2018) y Panamá³³³ (2019), concluyeron el proceso en los últimos años, inspirándose en el RGPD de la Unión Europea.

Dado que las iniciativas regionales han abordado la privacidad y la protección de los datos como un tema importante en los esfuerzo orientados a promover la integración y el crecimiento económicos, se espera que se pongan en marcha nuevos esfuerzos para fomentar el diálogo regional sobre la protección de los datos, vinculando las experiencias de algunos países cuyas leyes ya han sido reconocidas como adecuadas en virtud de las normas de la Unión Europea (como las de Argentina y el Uruguay) con las de otros países que están a punto de hacer frente a los retos que supone la aplicación de un nuevo reglamento de protección de datos³³⁴. Chile sigue el mismo camino, con propuestas legislativas que están en sintonía con gran parte de la lógica del RGPD³³⁵. Lo mismo ocurre con la legislación de protección de datos del Brasil, cuyo diseño se inspira en las normas europeas.

Igualmente importante es el hecho de que la protección de los datos haya pasado a formar parte del programa de comercio digital en el marco de foros comerciales regionales como la Alianza del Pacífico y el MERCOSUR. El Protocolo Adicional al Acuerdo Marco de la Alianza del Pacífico exige a los países partes que mantengan o aprueben una legislación sobre protección de datos³³⁶. En la agenda digital de la Alianza, el enfoque adoptado es que los países deben seguir las mejores normas internacionales, adoptando una visión máxima de la protección de los datos personales³³⁷. En el plan de acción conjunto entre el MERCOSUR y la Alianza del Pacífico, los países han manifestado su intención de colaborar para encontrar un terreno común en la regulación de los datos personales. Consideran que el tema es un importante peldaño de política con miras al establecimiento de un mercado digital común³³⁸. Se están elaborando propuestas para el MERCOSUR que parecen ser una opción oportuna³³⁹.

6.3. Restricciones a la privacidad de los datos en las transferencias transfronterizas de datos

A diario se producen transferencias transfronterizas de datos en una amplia gama de situaciones, desde simples contratos de comercio electrónico hasta complejas transacciones internacionales. Esas transferencias por lo general están relacionadas con mercados o zonas comerciales regionales, pero los datos personales cruzan las fronteras incluso sin esos acuerdos comerciales internacionales.

América Latina y el Caribe, en tanto gran consumidora de servicios digitales, debe lidiar continuamente con servicios transnacionales que operan en la región y, en muchos casos, exportan datos a sus servidores en el extranjero. Este ha sido un importante tema de debate respecto de muchas áreas, en particular los servicios en la nube, y ha motivado propuestas para ejecutar la localización de ciertas categorías de datos dentro del territorio nacional de cada país (véase un examen más detallado de la localización de datos en la sección III.B.6).

Sin embargo, las corrientes transnacionales no se ven restringidas únicamente por las estrategias de localización de datos. La legislación de protección de datos destinada a garantizar normas estrictas de protección de los datos para los ciudadanos también puede crear mecanismos que repercutan indirectamente en la circulación de datos fuera de las fronteras de los países o la obstaculicen. En muchos países de la región han surgido reglamentos sobre la transferencia internacional de datos personales basados en reglamentos europeos (primero la Directiva 95/46/CE de la Unión Europea y ahora el RGPD). Colombia, por ejemplo, ha establecido una lista de países que han cumplido las normas de transferencia de datos y con los que, en determinadas circunstancias, los datos pueden circular libremente; para todos los demás países existe un procedimiento elaborado que por lo general incluye

³³¹ Véase [en línea] https://www.oas.org/juridico/PDFs/arg_ley25326.pdf.

³³² Véase [en línea] <https://www.impo.com.uy/bases/leyes/1831-2008>.

³³³ Véase [en línea] https://www.sucrelaw.com/blog/media/2019/04/Ley-81-de-2019_Sobre-Proteccion-de-Datos.pdf.

³³⁴ Véase [en línea] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

³³⁵ Véase [en línea] <https://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doctoInformeAsesoria&id=7045>.

³³⁶ Véase [en línea] http://www.sice.oas.org/Trade/PAC_ALL/Pacific_Alliance_Text_s.asp#ci3_d13_8.

³³⁷ Véase [en línea] <https://alianzapacifico.net/wp-content/uploads/Hoja-de-Ruta-SGAD2016-2017.pdf>.

³³⁸ Véase [en línea] <http://www.cartillaciudadania.mercosur.int/oldAssets/uploads/Plan%20de%20Acción%20-%20Anexo%20declaración%20Puerto%20Vallarta.pdf>.

³³⁹ Banco Interamericano de Desarrollo (BID), “Fueling Digital Trade in MERCOSUR: A Regulatory Roadmap”, 2018 [en línea] <https://publications.iadb.org/publications/english/document/Fueling-Digital-Trade-in-Mercosur-A-Regulatory-Roadmap.pdf>.

estrictas cláusulas contractuales³⁴⁰. De manera análoga, las legislaciones de la Argentina, las Bahamas, el Brasil, Colombia, Costa Rica, México, Nicaragua, Panamá, el Perú, la República Dominicana, Santa Lucía, Trinidad y Tabago y el Uruguay contienen disposiciones que limitan las transferencias internacionales.

Entre los países mencionados se destacan la Argentina y el Uruguay por haber sido reconocidos por la Unión Europea como países aprobados para la transferencia de datos personales. Se han levantado las restricciones unilaterales entre los dos países y la Unión Europea en ambas direcciones, lo que asegura que los datos personales puedan fluir entre cada uno de ellos y toda la Unión Europea³⁴¹.

7. Corrientes transfronterizas de datos internacionales y regionales

7.1. Las corrientes de datos internacionales y regionales son la piedra angular del comercio digital

Las corrientes internacionales de datos han registrado un marcado aumento en los últimos tiempos³⁴². El creciente comercio internacional de servicios –sobre todo en sectores en los que la prestación solía ser exclusivamente nacional, como la educación, la atención de la salud y la banca– y las tecnologías con gran densidad de datos de la Internet de las cosas y la inteligencia artificial, entre otras, han conferido una nueva urgencia a los esfuerzos destinados a determinar normas de protección de datos³⁴³. Las posibles repercusiones económicas transfronterizas son de gran magnitud. Por lo tanto, las cuestiones relativas a los datos personales están adquiriendo cada vez más importancia en la agenda del comercio internacional.

Dado que organizaciones internacionales como la Organización Mundial del Comercio (OMC) y la Organización de Cooperación y Desarrollo Económicos (OCDE) aún no han encontrado una base sólida para resolver los problemas del comercio electrónico, el comercio digital, la protección de datos y las corrientes transfronterizas de datos, los acuerdos comerciales regionales y bilaterales han comenzado a consagrarse sus propias normas³⁴⁴. En América Latina y el Caribe, varios países son partes en acuerdos comerciales (bilaterales o de otro tipo) que contienen cláusulas específicas sobre esos temas.

Uno de los primeros acuerdos que contenía una disposición sobre el comercio electrónico fue el Acuerdo de Asociación Económica entre la Unión Europea y el Foro del Caribe del Grupo de Estados de África, del Caribe y del Pacífico, que entró en vigor en 2008 y en el que participaron Antigua y Barbuda, las Bahamas, Barbados, Belice, Dominica, Granada, Guyana, Jamaica, la República Dominicana, San Vicente y las Granadinas, Saint Kitts y Nevis, Santa Lucía, Suriname y Trinidad y Tabago³⁴⁵. Países como Belice, Colombia, Costa Rica, El Salvador, Guatemala, Honduras, México, Nicaragua, Panamá y el Perú también han concertado acuerdos que contienen cláusulas de comercio electrónico con Estados de fuera de la región. A nivel intrarregional también hay casos como los acuerdos concertados por Colombia con los países del Triángulo del Norte Centroamericano (El Salvador, Guatemala y Honduras), con Costa Rica y con el Perú; los celebrados por México con Centroamérica y Panamá, y el establecido entre Chile y el Uruguay. El alcance y el contenido de los acuerdos varían, pero por lo general establecen políticas sobre una amplia gama de cuestiones, desde la protección del consumidor en línea hasta la protección de los derechos de propiedad intelectual en el ciberspacio³⁴⁶.

³⁴⁰ Red de Políticas de Internet y Jurisdicción, "Colombia establishes list of countries with adequate data protection for cross-border transfers", *I&J Retrospect Database*, julio de 2017 [en línea] https://www.internetjurisdiction.net/publications/retrospect#article-6188_2017-07.

³⁴¹ Véase una lista completa de los países cuyas protecciones son consideradas adecuadas por la Unión Europea [en línea] https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

³⁴² Según un estudio de McKinsey, las corrientes transfronterizas de datos tienen un impacto más importante en la economía mundial que el comercio de mercancías. McKinsey Global Institute, *Digital Globalization: The New Era of Global Flow*, 2016 [en línea] <https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>.

³⁴³ Véase [en línea] <https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/>.

³⁴⁴ Véase, por ejemplo, el debate de la Organización de Cooperación y Desarrollo Económicos (OCDE) sobre la apertura de Internet y las corrientes de datos, el debate del Foro Económico Mundial sobre la gobernanza de las corrientes de datos internacionales, la propuesta del Japón al G20 de una corriente de datos libre con confianza, que representa un posible acuerdo internacional sobre las corrientes transfronterizas de datos, o la controversia de la OMC sobre el comercio electrónico. Véase [en línea] https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en;jsessionid=dFRe-gxHPx7Res_noe9wGNEb.ip-10-240-5-180; http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf; <https://pecc.org/resources/digital-economy/2016-data-free-flow-with-trust-and-data-governance/> file y https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm.

³⁴⁵ Haití firmó el tratado, pero aún no lo ha ratificado. Véase [en línea] <https://ec.europa.eu/trade/policy/countries-and-regions/regions/caribbean/>.

³⁴⁶ Banco Interamericano de Desarrollo/Centro Internacional de Comercio y Desarrollo Sostenible, *Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System*, 2017 [en línea] <https://www.ictsd.org/themes/global-economic-governance/research/digital-trade-related-provisions-in-regional-trade>.

Sin embargo, no todos los acuerdos contienen cláusulas de protección de datos. El Acuerdo de Asociación Transpacífico, que incluye a tres países de la región (Chile, México y Perú), es uno de los que sí las contiene. Su capítulo sobre comercio electrónico trata de varios aspectos importantes, como la privacidad y la protección de datos, las corrientes transfronterizas de datos y la localización de datos. Reconoce los beneficios de la legislación sobre protección de datos y ordena a los países miembros que mantengan o adopten un “marco jurídico” para proteger la “información personal”. El contenido de ese marco es abierto: cada país puede decidir cómo se regularán exactamente los datos personales. Sin embargo, una disposición importante reconoce la necesidad de crear mecanismos “que promuevan la compatibilidad entre sus diferentes regímenes”³⁴⁷.

El Tratado entre México, los Estados Unidos y el Canadá (T-MEC) es otro ejemplo. El capítulo sobre comercio digital, el primero de este tipo, sigue, en gran medida, la misma estrategia que el Acuerdo de Asociación Transpacífico, que fue negociado con anterioridad y es mucho más amplio³⁴⁸. Hay disposiciones que exigen que cada Estado establezca leyes para proteger los datos personales (“información personal” en virtud del acuerdo). El tratado no establece, sin embargo, una norma mínima común que deba seguirse, sino que solo señala que al regular la “información personal”, “cada Parte deberá tener en consideración los principios y directrices de los organismos internacionales correspondientes”³⁴⁹.

Cuanto más se afiancen los bienes y servicios conexos (en particular los bienes con servicios de información incorporados), más importante será disponer de normas comunes de protección de datos. Esto significa no solo normas aplicables a nivel nacional, sino también normas que permitan que los datos fluyan en el plano internacional. Diferentes enfoques pueden repercutir en el comercio internacional al dificultar que las empresas ganen escala y operen en distintos mercados. Las divergencias en las reglamentaciones de protección de datos hacen necesario adaptar los bienes y servicios para cumplir con los requisitos reglamentarios de cada mercado específico. Del mismo modo, las restricciones a las corrientes a través de las fronteras repercuten en las ofertas transfronterizas de bienes y servicios. Tomando el ejemplo de la Internet de las cosas, en el primer caso, la arquitectura y la configuración de la privacidad tienen que adaptarse antes de que el dispositivo pueda ofrecerse en un determinado país. En el segundo caso, la infraestructura utilizada para prestar el servicio subyacente que necesita los datos podría ser mucho más compleja, y la corriente de datos quedaría confinada dentro de las fronteras del país o los procedimientos para permitir la transferencia internacional de datos tendrían que establecerse de antemano. Esto puede repercutir en la competencia entre empresas nacionales y extranjeras, lo que puede plantear problemas de discriminación arbitraria o injustificable. Por lo tanto, hay dos tipos de iniciativas que son importantes: la armonización de las normas de protección de datos y la facilitación de corrientes internacionales de datos responsables y seguras.

7.2. Regionalización: desafíos y oportunidades a través de las fronteras

En varias de las recientes iniciativas comerciales en las que participa América Latina y el Caribe se ha previsto la circulación transfronteriza de datos. Estas iniciativas reconocen que leyes diferentes pueden ofrecer oportunidades y condiciones diferentes para las corrientes internacionales de datos. Tratan de proporcionar un marco que facilite los flujos estableciendo las condiciones que deben cumplirse o el alcance del tema para el que se permiten los flujos de datos personales.

El artículo 14(11)(2) del Acuerdo de Asociación Transpacífico establece que deben permitirse las corrientes transfronterizas de datos siempre que la corriente “sea para la conducción de un negocio de una persona cubierta”. El artículo 19.11 del T-MEC impone la misma obligación. Ambos añaden un lenguaje similar al de los tratados internacionales, como el artículo XX del Acuerdo General sobre Aranceles Aduaneros y Comercio (GATT) y el artículo XIV del Acuerdo General sobre el Comercio de Servicios (AGCS), permitiendo a los países regular con “un objetivo legítimo de política pública”.

La cláusula relativa a los servicios financieros del Acuerdo de Asociación Económica entre los Estados del CARIFORUM y la Unión Europea (artículo 107) también establece que los países deben permitir el flujo de datos para la realización de ese tipo de negocios (servicios financieros). El tratado agrega una cláusula más específica que establece que las partes adoptarán las salvaguardias adecuadas para

³⁴⁷ Acuerdo de Asociación Transpacífico, art. 14(8)(5). Véase [en línea] <https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14-Electronic-Commerce-Chapter.pdf>.

³⁴⁸ Véase [en línea] <https://www.cfr.org/blog/coming-north-american-digital-trade-zone>.

³⁴⁹ Tratado entre México, los Estados Unidos y el Canadá, art. 19(8), 30 de noviembre de 2018. Véase [en línea] <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>.

proteger la privacidad, los derechos fundamentales y la libertad personal de los interesados, lo que debe incluir la protección de los datos y la privacidad.

En el caso del Tratado de Libre Comercio entre México y la Unión Europea que se está negociando, el capítulo sobre comercio digital no especifica ningún régimen para las corrientes transfronterizas de datos, pero incluye una “cláusula de *rendez-vous*” que prevé un período de tres años para evaluar si es necesario incluir “disposiciones sobre el libre flujo de datos”³⁵⁰.

Algunos acuerdos comerciales bilaterales de la región contienen cláusulas relativas a las corrientes bilaterales de datos. El artículo 14(10) del Tratado de Libre Comercio México-Panamá establece que los datos pueden cruzar las fronteras, pero con la salvedad de que ello debe hacerse de conformidad con los requisitos de protección de datos personales y tomando en consideración las prácticas internacionales. Otros solo subrayan la necesidad de cooperación para facilitar y mantener las corrientes de datos, como ocurre en los casos del Tratado de Libre Comercio Colombia-Costa Rica, el Acuerdo de Libre Comercio Chile-Colombia y el Tratado de Libre Comercio Colombia-El Salvador, Guatemala y Honduras.

Estos acuerdos constituyen la base de entendimientos comunes sobre la forma en que los datos pueden fluir a través de las fronteras. Los acuerdos limitan las posibles tensiones entre los regímenes y las restricciones de las corrientes de datos, y se tiende a dar prioridad a las corrientes internacionales. Todavía no existe un acuerdo general o regional que incluya a los países de América Latina y el Caribe. Un acuerdo de este tipo probablemente aportaría una mayor seguridad a los flujos de datos y mejoraría el comercio, sobre todo en la economía digital.

7.3. Las iniciativas regionales fomentan la estandarización de las transferencias de datos a través de las fronteras

A nivel regional e internacional no existen acuerdos generales que abarquen la protección de la reputación de una persona o que permitan (o impidan) la libre circulación de datos. No obstante, algunas organizaciones regionales han elaborado principios rectores con el fin de armonizar las normas vigentes en los distintos países.

En los Principios de la OEA sobre la Protección de la Privacidad y los Datos Personales, particularmente en el principio 11 “Flujo transfronterizo de datos y responsabilidad”, se reconoce la necesidad armonizar las normas de protección de los datos para no obstaculizar el flujo de datos a través de las fronteras³⁵¹.

Las normas de protección aprobadas por la Red Iberoamericana de Protección de Datos, de la que son parte varios de los países de la región, también contienen una recomendación de que las transferencias transfronterizas de datos se sometan a una serie de requisitos que siguen pautas similares a las de la legislación europea, indicando que o bien los países deben tener una protección considerada adecuada o bien las partes que deseen transferir datos al extranjero deben seguir procedimientos preestablecidos³⁵².

³⁵⁰ Svetlana Yakovleva y Kristina Irion, “Pitching trade against privacy: reconciling EU governance of personal data flows with external trade”, *International Data Privacy Law*, 30 de marzo de 2020 [en línea] <https://doi.org/10.1093/dpl/ipac003>. Véase el texto del acuerdo negociado [en línea] http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf.

³⁵¹ Véase [en línea] <http://scm.oas.org/pdfs/2016/CP3545JERREPORTCJI.pdf>.

³⁵² Véase [en línea] https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf.

CAPÍTULO III

PRINCIPALES ENFOQUES DE LOS DILEMAS TRANSFRONTERIZOS DE INTERNET EN AMÉRICA LATINA Y EL CARIBE

En el *Internet & Jurisdiction Global Status Report 2019* se sostenía que no era exagerado decir que se estaba desarrollando una carrera armamentista legal entre muchos de los principales actores internacionales, sobre todo los Estados Unidos, la Unión Europea, China y, en cierta medida, la Federación de Rusia. Como se señaló anteriormente, las medidas que adoptan repercuten directamente en la región. Muchos Estados de América Latina y el Caribe están adoptando e implementando en sus jurisdicciones internas soluciones técnicas y jurídicas que se asemejan o se inspiran en las soluciones normativas y técnicas adoptadas por otros agentes internacionales.

De ahí que las iniciativas de América Latina y el Caribe reflejen en gran medida las propuestas en otros lugares. Entre ellas figuran la legislación nacional de amplia aplicación extraterritorial, las órdenes judiciales locales con repercusiones mundiales, las multas y sanciones a empresas sin presencia física en el país y el filtrado de contenidos obligatorio, la localización de datos y el bloqueo de aplicaciones. Sin embargo, en la aplicación real tienden a adquirir un matiz regional pues las soluciones se transfieren de un contexto a otro totalmente distinto.

Como se mencionó en el capítulo II, las peculiaridades sociales, económicas, políticas y jurídicas tienen el efecto de modificar la forma en que las soluciones técnicas se implementan en los distintos países. En una región tan diversa como América Latina y el Caribe, todas esas condiciones desempeñan un papel importante en la determinación del éxito de las soluciones jurídicas y técnicas a los dilemas transfronterizos.

Sin embargo, estas soluciones jurídicas y técnicas se han aplicado en su mayor parte sin un debate adecuado sobre sus efectos transfronterizos. Por consiguiente, en esta parte del informe se procura analizar una selección de dichas iniciativas y arrojar luz sobre sus repercusiones transfronterizas.

A. Principales tendencias legales

La medida en que los Estados de América Latina y el Caribe utilizan soluciones jurídicas para los problemas que perciben respecto de la regulación de Internet varía de un país a otro. En general, existe una tendencia cada vez más difundida a ampliar la aplicabilidad de las leyes nacionales a situaciones que van más allá de las fronteras físicas de los países. Cada vez es más habitual determinar la competencia jurisdiccional en virtud de lo que se denomina “doctrina de los efectos” o de una “prueba de selección”. Los tribunales han emitido órdenes para retirar (o eliminar) y mantener contenidos en línea. También se hace hincapié en asociar la regulación aplicable a Internet con elevadas multas y sanciones. Las condiciones de servicio y las directrices de la comunidad creadas por las principales plataformas internacionales de Internet desempeñan un papel cada vez más importante y fundamental para guiar el comportamiento en línea.

1. Los Estados recurren cada vez más a una “doctrina de los efectos” para hacer valer su jurisdicción

Entre los Estados existe una amplia tendencia a hacer valer su jurisdicción respecto de conductas y actividades que tienen origen en otro Estado o territorio, siempre que tengan una conexión relevante con el país que afirma su jurisdicción. En general, se entiende que las actividades que crean esa conexión incluyen dirigirse a los consumidores, hacer negocios, causar un daño o afectar de alguna manera concreta a personas o bienes situados dentro de las fronteras de un país.

Con arreglo al derecho internacional, se suele entender que este enfoque se encuadra en el marco de una “doctrina de los efectos”. La lógica es que los Estados deberían poder ejercer su jurisdicción sobre las conductas y actividades que tienen un impacto (“efecto”) en las personas o los bienes en su territorio. Esto se justifica por la intención, porque el participante activo sabía o al menos debería haber sabido que la actividad o conducta tendría consecuencias en ese país, o sobre la base de que los Estados deberían poder regular las actividades que afectan a sus mercados, sus ciudadanos o los bienes en su territorio³⁵³.

Este enfoque se elaboró originalmente a efectos de la legislación sobre competencia y antimonopolio, pero cobró impulso con la difusión de Internet. Se suele abordar con referencia a una “prueba de selección”. En los primeros ejemplos de este enfoque, la atención se centró en el establecimiento de una competencia jurisdiccional con especial referencia a la difamación (y el discurso perjudicial) y el comercio electrónico. En el caso *Young v. New Haven Advocate*, se pidió a un tribunal de apelaciones de los Estados Unidos que decidiera si los tribunales de un estado tenían jurisdicción para decidir sobre un caso de difamación relacionado con un periódico (digital e impreso) destinado a ser distribuido en otro estado. El tribunal dictaminó que no bastaba con que estuviera disponible en el segundo estado, o que se discutieran asuntos relacionados con ese estado; el hecho de que su público objetivo estuviera en el otro estado fue el punto clave³⁵⁴.

En los casos conjuntos de *Peter Pammer v. Reederei Karl Schlüter GmbH & Co. KG y Hotel Alpenhof GesmbH v. Oliver Heller*, se pidió al Tribunal de Justicia de la Unión Europea que decidiera las características que determinarían la jurisdicción en los casos relativos al comercio electrónico, es decir, a un consumidor que compra bienes y servicios en línea. El tribunal europeo afirmó que debían tenerse en cuenta varios elementos, como el carácter internacional del servicio, los itinerarios desde otros Estados miembros (cómo se llegaba al lugar desde donde operaba la empresa), el idioma y las opciones monetarias del sitio web o la aplicación, los números de teléfono con códigos internacionales prefijados, los nombres de dominio de nivel superior distintos de aquel del Estado miembro en el que tenía su sede el comerciante y la mención de una clientela internacional compuesta por clientes domiciliados en varios Estados miembros.

En la decisión también se explicitaba que el mero hecho de que el servicio estuviera disponible en línea en el país del consumidor no era una conexión suficiente (esto repercute en la utilización de las tecnologías de geolocalización, como se examina más adelante)³⁵⁵. El fundamento de esas decisiones es que los comerciantes solo deben ser regulados a nivel de la Unión Europea si se dirigen primero al mercado de la Unión Europea. Este enfoque se reprodujo en la razón 23 del Reglamento General de Protección de Datos³⁵⁶ y ha servido de base para otros procesos regulatorios de la Unión Europea³⁵⁷.

Este punto de vista también ha tenido un impacto en América Latina. Los casos de diferentes países, desde Colombia hasta el Brasil, han establecido que la jurisdicción sobre las actividades en Internet debe determinarse en función de los efectos previstos o esperados de las medidas adoptadas en línea³⁵⁸. El ciberspacio se considera omnipresente, pero se entiende que las acciones y la conducta de los que participan en él tienen un foco, un objetivo. Al hacer valer la jurisdicción, los tribunales suelen decidir teniendo en cuenta el lugar en que se produjo el daño, considerando la intención aparente de los agentes implicados.

³⁵³ Véase B. Simma y A. Müller, “Exercise and limits of jurisdiction”, *The Cambridge Companion to International Law*, J. Crawford y M. Koskenniemi (eds.), Cambridge, Cambridge University Press, 2012.

³⁵⁴ Véase Tribunal de Apelaciones del Cuarto Circuito de los Estados Unidos, *Young v. New Haven Advocate*, N° 315 F.3d 256, Richmond, 13 de diciembre de 2002.

³⁵⁵ Véase Tribunal de Justicia de la Unión Europea, *Sentencia del Tribunal de Justicia (Gran Sala) de 7 de diciembre de 2010 (peticiones de decisión prejudicial planteadas por el Oberster Gerichtshof – Austria) – Peter Pammer/Reederei Karl Schlüter GmbH & Co.KG (C-585/08), Hotel Alpenhof GesmbH/Oliver Heller*, N° 2011/C 55/06, Luxemburgo, 19 de febrero de 2011.

³⁵⁶ Reglamento General de Protección de Datos, razón 23: “debe determinarse si es evidente que el responsable o el encargado proyecta ofrecer servicios a interesados en uno o varios de los Estados miembros de la Unión. Si bien la mera accesibilidad del sitio web del responsable o encargado o de un intermediario en la Unión, de una dirección de correo electrónico u otros datos de contacto, o el uso de una lengua generalmente utilizada en el tercer país donde resida el responsable del tratamiento, no basta para determinar dicha intención, hay factores, como el uso de una lengua o una moneda utilizada generalmente en uno o varios Estados miembros con la posibilidad de encargar bienes y servicios en esa otra lengua, o la mención de clientes o usuarios que residen en la Unión, que pueden revelar que el responsable del tratamiento proyecta ofrecer bienes o servicios a interesados en la Unión⁴. Véase [en línea] <https://www.privacy-regulation.eu/es/r23.htm>.

³⁵⁷ Véanse Comisión Europea, *Proposal for a directive of the European Parliament and of the Council laying down harmonised rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings*, N° COM(2018) 226 final, Estrasburgo, 17 de abril de 2018 [en línea] <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN>; *Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, N° COM(2018) 225 final, Estrasburgo, 17 de abril de 2018 [en línea] <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN>.

³⁵⁸ Véase un panorama general de los casos de difamación [en línea] https://www.palermo.edu/cele/cele/pdf/english/Internet-Free-of-Censorship/Jurisdiction_Eduardo%20Bertoni.pdf.

En el caso de Jerónimo A. Uribe, la Corte Suprema de Justicia de Colombia dictaminó que el discurso en línea, incluidas las amenazas de muerte, no debía entenderse como algo que ocurriera únicamente en el lugar donde se encontraba el orador, es decir, su lugar de residencia habitual³⁵⁹. De manera similar, en el caso del Centro Comercial Campanario, la misma Corte Suprema dictaminó que la jurisdicción debía asignarse al lugar donde se produjo el daño, es decir, en un caso de fraude en línea, el lugar donde se encuentra la víctima³⁶⁰.

Siguiendo un razonamiento similar, el Tribunal Superior de Justicia del Brasil³⁶¹ ha dictaminado en varios casos que la ubicación de los servidores es irrelevante a la hora de determinar la jurisdicción y que, en cambio, la jurisdicción debe asignarse al lugar en que la víctima reside y trabaja, ya que es allí donde la actividad o el discurso perjudicial tendrá los mayores efectos y repercusiones³⁶².

En la Argentina, asimismo, varias sentencias han determinado la jurisdicción en función del lugar donde se produjo el daño o donde se encuentra la víctima³⁶³. Esto adquiere un aspecto diferente cuando el presunto autor del delito es una publicación de noticias que tiene una presencia tanto en línea como fuera de línea. El razonamiento es que el lugar donde “se imprimen los materiales” es el criterio que rige. El principio subyacente parece ser que, a pesar de la presencia en línea, el público al que se dirige es el del lugar donde se distribuye la edición impresa³⁶⁴.

En la mayoría de los casos de la región, el principal criterio para determinar la jurisdicción es simplemente el lugar en que se experimenta el daño, como el lugar de residencia o de negocios de la víctima. Ese enfoque selectivo también se observa en algunas legislaciones, incluidas las leyes de protección de datos de la Argentina, el Brasil³⁶⁵, Colombia³⁶⁶, México³⁶⁷ y el Perú³⁶⁸. Otro ejemplo es la Ley Especial contra los Delitos Informáticos de la República Bolivariana de Venezuela.

La principal dificultad de este enfoque de selección es comprender el perfil del objetivo. ¿El hecho de que un sitio web esté disponible en línea, sin limitaciones geográficas, significa que se dirige a todo el mundo, o al menos que sus propietarios aceptan el riesgo de actuar como si así fuera? ¿Es importante un cambio de idioma? ¿Cuáles son los criterios precisos para determinar el público al que se dirige? Podría parecer relativamente fácil determinar la jurisdicción en el caso de una aplicación de mensajería entre pares, pero ¿qué cambiaría si el mismo mensaje se enviara a través de una red social abierta al público?

El elemento controvertido aquí es la cuestión de si la jurisdicción es justa para todas las partes involucradas. Por una parte, limitar la jurisdicción al domicilio de la persona que presta el servicio, vende el producto o publica el mensaje dejaría a la otra parte con muy pocos recursos. Por otra, si la parte potencialmente perjudicada recibe demasiada protección, el proveedor de servicios, vendedor o editor de contenidos podría tener que defenderse ante los tribunales en cualquier parte del mundo en virtud de una ley cuya aplicación tal vez no esperaba.

2. La expansión del alcance jurisdiccional

Un número considerable de los interesados encuestados señaló que existía un desequilibrio de poder y que, aunque muchos países estaban aplicando leyes de alcance extraterritorial, no todos los Estados estaban en condiciones de hacerlas cumplir. Algunos también indicaron que, si bien ese tipo de regulaciones podría resultar más eficaz si formara parte de los acuerdos regionales, sigue siendo muy difícil encontrar un terreno común.

³⁵⁹ Véase Corte Suprema de Justicia de Colombia, *Caso Jerónimo A. Uribe*, N° 33.474/2010, Bogotá, 10 de febrero de 2010.

³⁶⁰ Véase Corte Suprema de Justicia de Colombia, *Caso Centro Comercial Campanario*, N° 34.564/2010, Bogotá, 25 de agosto de 2010.

³⁶¹ Véase Tribunal Superior de Justicia, *Conflito de competência*, N° 66.981, Brasilia, 16 de febrero de 2009 [en línea] https://www2.stj.jus.br/processo/revista/inteiroteor/?num_registro=200601611027&dt_publicacao=05/03/2009.

³⁶² Véase Tribunal Superior de Justicia, *Conflito de competência*, N° 66.981, Brasilia, 16 de febrero de 2009; *Conflito de competencia*, N° 107.938, Brasilia, 27 de octubre de 2010; *Agravo de instrumento*, N° 1.375.009, Brasilia, 15 de marzo de 2011.

³⁶³ Véase Cámara Federal de Apelaciones de Salta, *J. G. R. vs. Google Inc.*, Salta, 4 de julio de 2011; Cámara Nacional Criminal y Correccional de la Capital Federal, *N.N. s/ injurias*, N° 1589/09, Buenos Aires, 21 de octubre de 2009.

³⁶⁴ Véanse Cámara Nacional de Casación Penal, *Alifano, Roberto Francisco s/recurso de queja*, N° 9375, Buenos Aires, 3 de marzo de 2009; Corte Suprema de Justicia de la Nación, *Verazay, Santos Justo s/ querella por calumnias e injurias*, N° 1085, Buenos Aires.

³⁶⁵ Véase Presidencia de la República del Brasil, Ley N° 12.965 de 23 de abril de 2014, que establece principios, garantías, derechos y deberes para el uso de Internet en el Brasil, Brasilia, 2014 [en línea] http://www.planalto.gov.br/ccivil_03/_ato2011-2014/lei/l12965.htm.

³⁶⁶ Véase Congreso de Colombia, *Ley Estatutaria 1581 de 2012*, Bogotá, 2012 [en línea] https://www.defensoria.gov.co/public/Normograma%202013_.html/Normas/Ley_1581_2012.pdf.

³⁶⁷ Véase Instituto Nacional de Desarrollo Social (INDESOL), *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Ciudad de México, 2010; *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares*, Ciudad de México, 2011; Secretaría de Economía, “Lineamientos del aviso de privacidad”, *Diario Oficial de la Federación*, Ciudad de México, 17 de enero de 2013.

³⁶⁸ Perú, Ley n° 29.733 de 2011, Ley de Protección de Datos Personales.

En el contexto de una Internet mundial sin fronteras, en la que las conductas y acciones iniciadas en una parte del mundo pueden repercutir –y de hecho causar daños– en otra, los países han tratado de extender sus poderes más allá de su propio territorio. Han tratado unilateralmente de cerrar la brecha de la gobernanza y la regulación internacionales en lo que respecta a las acciones y conductas en línea, reivindicando una jurisdicción que va más allá de lo que tradicionalmente se reconoce como su territorio, en algunos casos sin tener en cuenta si hay alguna perspectiva de aplicación real o efectiva.

Un ejemplo de la región se encuentra en el artículo 11 del Marco Civil de Internet del Brasil, que establece que en toda operación de recolección, almacenamiento, custodia y procesamiento de datos personales o comunicaciones por parte de proveedores de conexión y aplicaciones de Internet en la que al menos uno de estos actos ocurra en el territorio nacional, se debe respetar la legislación brasileña³⁶⁹. En el párrafo 2 se incluyen incluso las actividades realizadas por una persona jurídica con sede en el extranjero, siempre que ofrezca servicios al público brasileño o que por lo menos un miembro del mismo grupo económico tenga un establecimiento en el Brasil³⁷⁰.

La tendencia a reivindicar una jurisdicción ampliada se ha visto reforzada por el ejemplo del artículo 3 del Reglamento General de Protección de Datos europeo. Esta regulación ha tenido efectos en el diseño de la nueva legislación en los países de América Latina y el Caribe. El Brasil, por ejemplo, incluyó en su Ley General de Protección de Datos Personales un artículo 3 propio inspirado en su homólogo europeo, en el que se establece que la Ley se aplica a cualquier operación de procesamiento realizada por una persona física o una persona jurídica constituida con arreglo al derecho público o privado, independientemente del medio, del país en que se encuentren la persona o la sede de la entidad o del país en que se encuentren los datos, siempre que: i) la operación de procesamiento se realice en territorio brasileño; ii) la actividad de procesamiento tenga por objeto la oferta o el suministro de bienes o servicios o el procesamiento de datos de personas situadas en territorio brasileño; o iii) los datos personales objeto del procesamiento se hayan recogido en territorio brasileño. El artículo 3.1 de la Ley General de Protección de Datos Personales del Brasil también establece que se considerará que los datos personales se han recogido en territorio brasileño cuando la persona a la que se refieren se encuentre en territorio brasileño en el momento de la recolección³⁷¹.

Lo mismo ocurre en países como Colombia,³⁷² México³⁷³ y el Perú³⁷⁴, que también han ampliado su normativa de protección de datos para darle una dimensión extraterritorial. Desde el punto de vista de una nación en desarrollo, este enfoque puede considerarse una muestra de fortaleza frente a las empresas extranjeras que pueden incidir en los mercados nacionales desde lejos, especialmente cuando la regulación va acompañada de fuertes multas y sanciones (que se examinan en la sección V.A.4). Esto parece aceptarse a nivel internacional cuando lo que se está protegiendo son los derechos y valores fundamentales del país que promulga la ley.

Sin embargo, toda reivindicación jurisdiccional, relacionada tanto con la jurisdicción judicial como con la prescriptiva, vive o muere por la posibilidad de que se aplique. La falta de capacidad real para obligar a las partes a cumplir puede disminuir la legitimidad de la regulación. Este enfoque también ha sido criticado por: i) conducir a una aplicación arbitraria (con demasiados posibles agentes no cumplidores, las autoridades tienen que elegir a cuál perseguir); ii) socavar la certeza jurídica (demasiados autores no son enjuiciados, lo que da la impresión de que la ley es letra muerta); y iii) crear posibles conflictos transfronterizos de cumplimiento (las normas de dos o más países pueden exigir la adopción de medidas diferentes respecto de la misma conducta, lo que puede dar lugar a conflictos y obligar a las entidades a elegir la ley que han de cumplir).

Una de las partes interesadas encuestadas dijo que, hasta ahora, los tribunales superiores de América Latina habían mostrado moderación y no habían dictado órdenes de alcance mundial sobre cuestiones relativas a Internet. Otro interesado opinó que en muchos países de la región aún no se ha determinado el posible alcance mundial de los derechos en línea individuales.

³⁶⁹ Véase Internet & Jurisdiction Policy Network, "Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction", París, 2014 [en línea] https://www.internetjurisdiction.net/publications/retrospect#article-5002_2014-04.

³⁷⁰ Ibídem.

³⁷¹ Véase [en línea] https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf.

³⁷² Colombia, Ley Estatutaria núm. 1581 de 2012. Véase [en línea] https://www.defensoria.gov.co/public/Normograma%202013_Html/Normas/Ley_1581_2012.pdf.

³⁷³ Véase Instituto Nacional de Desarrollo Social (INDESOL), Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Ciudad de México, 2010; Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Ciudad de México, 2011; Secretaría de Economía, "Lineamientos del aviso de privacidad", Diario Oficial de la Federación, Ciudad de México, 17 de enero de 2013.

³⁷⁴ Perú, Ley núm. 29.733 de 2011, Ley de Protección de Datos Personales.

El debate va más allá de si los tribunales tienen jurisdicción sobre determinadas personas o tipos de materia o si la legislación se aplica a una situación que podría entenderse que se encuentra fuera de lo que tradicionalmente se entiende como el territorio de un país. Lo que está en juego es el alcance de los efectos de la jurisdicción: el alcance de la jurisdicción correctiva³⁷⁵.

Se ha informado que el juez Alexandre de Moraes, del Supremo Tribunal Federal (STF) del Brasil, ha ordenado a las redes sociales Facebook y Twitter que bloquen el acceso a las cuentas de 16 personas que están siendo investigadas por presunta difusión de desinformación y discursos de odio en línea³⁷⁶. Se informa que el magistrado ha solicitado un alcance mundial (que el acceso se bloquee independientemente del origen de la dirección IP del espectador) sobre la base de un informe policial en el que se afirma que ha habido incidentes en los que las personas investigadas han eludido la restricción impuesta por la orden anterior y siguieron utilizando sus cuentas para publicar mensajes en contravención de la orden judicial vigente, en particular los discursos de odio.

El evento tuvo una repercusión adicional, ya que una de las 16 personas que tenían sus cuentas bloqueadas a nivel mundial pudo utilizar otra cuenta para hacer una declaración muy controvertida contra el aborto. El comentario no solo incluía la expresión de opiniones sobre el asunto, sino que también incluía datos personales de una niña de 10 años que había sido violada y estaba siendo sometida a un procedimiento legal en el hospital. Otro juez instruyó a las mismas dos redes sociales y a Google para eliminar los mensajes que contenían los detalles de la menor³⁷⁷. Se informó que un miembro del parlamento había pedido que este incidente se añadiera a las investigaciones que dieron lugar a la orden mundial dictada por el juez Moraes del Supremo Tribunal Federal (STF)³⁷⁸.

Los casos relativos al llamado derecho al olvido se han ocupado de los límites (alcance) del procedimiento de supresión de la lista o desindexación, es decir, si es suficiente que esto se haga dentro del territorio del país (o de Europa) o debe ser mundial. El bloqueo geográfico (que se examina en la sección V.B.1) se está considerando y tratando en función de la eficiencia y la precisión de la técnica³⁷⁹.

El debate sobre los derechos de propiedad intelectual también ha avanzado. La lógica es que existe un alto grado de armonización internacional en este ámbito (en particular de la legislación sobre derecho de autor). Así, una orden de un tribunal de un país puede tener repercusiones mundiales, a menos que se demuestre que las normas de otro país obligan a la plataforma a actuar de manera diferente³⁸⁰.

La Red de Políticas de Internet y Jurisdicción ha publicado recientemente una publicación en la que se ofrece orientación a los gobiernos y las entidades privadas sobre la forma de abordar el alcance geográfico de las restricciones de contenido. En esta se definen cuatro categorías de “coherencia normativa internacional” que reflejan el grado de convergencia entre los diferentes cuerpos de legislación en lo que respecta a la ilegalidad del contenido. Estas categorías deberían servir de base para una escala con diferentes niveles de alcance geográfico para la eliminación de contenido, desde el más proporcionado y limitado hasta el más global³⁸¹.

En la región, la tendencia a imponer órdenes de supresión global todavía no ha cobrado mucha fuerza. Esto no significa que no haya habido algunas órdenes que solicitaran a las plataformas un procedimiento de supresión o desindexación global³⁸². El alcance mundial previsto en algunas jurisdicciones también ha alentado a los ciudadanos de América Latina y el Caribe a solicitar reparación internacional. Un ciudadano paraguayo solicitó a la Agencia Española de Protección de Datos (AEPD) que ordenara a

³⁷⁵ Véase D. Jerker, “Jurisdiction in 3D – “scope of (remedial) jurisdiction” as a third dimension of jurisdiction”, *Journal of Private International Law*, vol. 12, Nº 1, Milton Park, Taylor & Francis, 2016.

³⁷⁶ Véase [en línea] <https://www.reuters.com/article/us-facebook-brazil/facebook-puts-global-block-on-brazils-bolsonaro-supporters-idUSKCN24X3BN>.

³⁷⁷ Véase [en línea] <https://www.bbc.com/news/world-latin-america-53820497>.

³⁷⁸ Véase [en línea] <https://revistaforum.com.br/politica/alexandre-padilha-aciona-stf-contra-sara-winter-por-incitar-fundamentalistas-contra-menina-de-10-anos/>.

³⁷⁹ Véase Tribunal de Justicia de la Unión Europea, *Google LLC, successor in law to Google Inc. v Commission nationale de l'informatique et des libertés (CNIL)*, Nº C-507/17, Luxemburgo, 24 de septiembre de 2019 [en línea] <http://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17;Eva Glawischnig-Piesczek v Facebook Ireland Limited, Nº C-18/18>, Luxemburgo, 3 de octubre de 2019 [en línea] <http://curia.europa.eu/juris/liste.jsf?num=C-18/18>.

³⁸⁰ Véase Corte Suprema de Canadá, *Google Inc. v. Equustek Solutions Inc.*, Nº SCC 34, Ottawa, 2017.

³⁸¹ Véase [en línea] <https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-102-Geographic-Scope-Content-Restrictions.pdf>.

³⁸² Véase Tribunal de Justicia del Estado de São Paulo, *Google Brasil Internet Ltda. v. Clóvis de Barros Filho*, São Paulo, 2019.

Google la supresión de la lista de una serie de artículos informativos en los que aparecía. La Agencia denegó su solicitud, pero esto demuestra el impacto de las órdenes con implicaciones globales³⁸³.

Los casos de supresión de listas agregan algunos matices al tema. En algunos casos, el Tribunal de Justicia del Estado de São Paulo (Brasil), por ejemplo, ha ordenado a Google Brasil que elimine ciertos resultados de búsqueda de su sitio web o que retire videos de YouTube a escala mundial. En otros casos, el mismo Tribunal ha cuestionado la forma en que sus fallos podrían incidir en otras jurisdicciones. En el caso Centro Espírita Beneficente União do Vegetal vs. Google Brasil Internet Ltda., el juez decretó que el tribunal no tenía jurisdicción para determinar que el video indicado en la petición inicial no fuera divulgado en territorio extranjero, como Colombia y Alemania, so pena de traspasar su ámbito de competencia e incurrir en una violación de la soberanía de los demás países³⁸⁴.

3. Órdenes de retiro, eliminación y mantenimiento de los tribunales

Internet ha hecho posible que el contenido se vea y se comparta en todo el mundo, tanto en entornos privados como públicos. Cada día se intercambian miles de millones de mensajes y se cargan millones de fotos y horas de videos y música, y una gran proporción se encuentra en plataformas globales accesibles a personas de todas partes del mundo. Esta abundancia de información está destinada a tener un impacto y afectar a las personas, incluso causando daño. A pesar del alto valor que se atribuye a la libertad de expresión, es evidente que los requisitos normativos, que pueden variar de un país a otro, deberán imponer algunos límites.

América Latina y el Caribe no es ajena a la tendencia mundial de emisión de órdenes judiciales que exigen que las plataformas retiren, eliminen y mantengan contenidos publicados en línea. La falta de consenso respecto de los estándares de protección de distintos derechos, en particular la libertad de expresión, es una importante fuente de controversias transfronterizas.

Es bastante común que esas órdenes tengan elementos transfronterizos. La plataforma puede ser de origen extranjero, la tecnología utilizada puede proceder del extranjero y los datos pueden estar guardados en servidores fuera del país. En resumen, una amplia gama de situaciones significa que muchas de esas órdenes tienen efectos fuera del territorio del país en el que se originan.

Además, no todos los países emiten esas órdenes por razones legítimas. Estas pueden utilizarse para limitar la expresión, perseguir a los oponentes políticos o discriminar, entre otras posibles violaciones de los derechos humanos. Todo análisis de estas medidas está inextricablemente vinculado a la materia subyacente que pretenden regular y al derecho sustantivo nacional e internacional que las regula. El capítulo IV del presente informe se centra en algunas de las cuestiones más importantes que llevan a los tribunales a dictar órdenes de retiro (y de eliminación o permanencia) o a exigir a los proveedores que supriman de la lista, desindexen y desreferencien o incluso borren, bloqueen o eliminen contenido.

Las órdenes de retiro de contenido son las más comunes y por lo general se emiten en relación con procesos vinculados a actos ilícitos civiles en los que se busca una indemnización monetaria. La reparación consiste en prohibir que el contenido se siga mostrando. No obstante, pueden tener otros objetivos específicos, como la eliminación de información engañosa o que pueda dañar la reputación de alguien.

En 2012, durante una campaña electoral, un juez local del Brasil emitió una orden para que Google retirara de su plataforma de YouTube un video crítico de un candidato político. Mientras la apelación estaba pendiente, el mismo juez emitió una orden de arresto contra el Director de Google Brasil por desacatar su petición judicial de retiro³⁸⁵.

En enero de 2016, la Corte Suprema de Justicia de Chile ordenó la eliminación de una publicación periodística que había dañado la reputación de un individuo y concedió a la empresa tres días para cumplir con la orden³⁸⁶.

³⁸³ Véase [en línea] <https://blog.cuatrecasas.com/propiedad-intelectual/derecho-al-olvido-audiencia-rechaza-aplicacion-extraterritorial/>.

³⁸⁴ Véase Tribunal de Justicia del Estado de São Paulo, *Centro Espírita Beneficente União do Vegetal vs. Google Brasil Internet Ltda.*, São Paulo, 11 de agosto de 2016 [en línea] <https://www.conjur.com.br/dl/justica-local-nao-obrigar-google2.pdf>.

³⁸⁵ Véase [en línea] <https://www.bbc.com/news/world-latin-america-19753158>.

³⁸⁶ Corte Suprema de Justicia de Chile, decisión del 21 de enero de 2016. Véase [en línea] <https://bit.ly/2MbDW6m>.

En la región también se emiten numerosas órdenes de eliminación. Estas se ocupan de un punto débil particular de las órdenes de retiro: la posibilidad de volver a publicar el contenido que se ha retirado prácticamente sin costo. La eliminación, por lo tanto, impone la obligación de que el contenido no reaparezca. Esto crea dos problemas potencialmente difíciles: i) las plataformas están obligadas a vigilar las futuras cargas para evaluar si tienen el mismo contenido ilegal y ii) para acelerar esta vigilancia y hacerla menos intensiva en recursos, se les induce a utilizar técnicas automatizadas, es decir, filtros impulsados por la inteligencia artificial.

Esto puede crear un régimen privatizado de censura y la percepción de que las plataformas son las encargadas de controlarlo. Además, los filtros automatizados podrían dar lugar a una prohibición general de ciertos tipos de discurso, que como resultado nunca verán la luz del día.

Este tipo de disposiciones es más fácil justificar en los casos en que hay pocas dudas sobre la ilegalidad del contenido y es probable que el riesgo de “bloqueo excesivo” o “filtración excesiva” por parte de las plataformas tenga menos repercusiones en el discurso protegido o que pueda considerarse legal. Un ejemplo es el material relativo al maltrato infantil, pues existe un fuerte consenso sobre su ilegalidad.

También se discute si un individuo debe indicar la dirección URL específica que se debe retirar, o si basta con indicar el contenido. En este último caso, se deja a las plataformas la tarea de establecer dónde se publicó el material y luego retirarlo.

En 2007, un juez brasileño dio instrucciones a la plataforma de YouTube para que retirara un video con contenido sexual de una famosa modelo que había sido publicado sin su consentimiento. En vista de que el video se volvía a cargar constantemente, el magistrado ordenó que se bloqueara el acceso al sitio web³⁸⁷. La orden se modificó al día siguiente para no restringir el acceso a YouTube en el país.

En 2012, un tribunal argentino ordenó la eliminación “permanente” de las imágenes sexuales de una modelo de un motor de búsqueda. El tribunal declaró que la plataforma tenía los medios para hacerlo³⁸⁸.

En 2017, la Corte Constitucional de Colombia ordenó a Google que suprimiera un blog anónimo de su plataforma Blogger porque estaba violando el derecho al desarrollo personal y a la privacidad³⁸⁹.

Las decisiones de mantenimiento no son tan comunes todavía, pues muy pocos países las han emitido. El entendimiento en cuanto a la libertad de expresión en línea es que las plataformas deben respetar esta libertad. Sin embargo, tienen cierto margen de maniobra para hacer cumplir algunas restricciones, principalmente basadas en sus condiciones de servicio y en las directrices de la comunidad.

Sin embargo, algunos países como Alemania y, en la región, el Brasil han considerado que hay circunstancias en las que la expresión está protegida y no debe ser limitada por las plataformas. En consecuencia, los tribunales han ordenado que el contenido que se había retirado se publicara nuevamente³⁹⁰.

En un ejemplo reciente, en diciembre de 2019 el Tribunal de Justicia del Distrito Federal y Territorios del Brasil dictó un mandato judicial contra Facebook exigiéndole que mantuviera en línea una publicación de un parlamentario, Eduardo Bolsonaro, en la que criticaba a algunos periodistas por un artículo sobre su esposa. Facebook declaró que los periodistas habían denunciado el uso no autorizado de sus imágenes, lo que constituía una violación de las condiciones de servicio de la plataforma³⁹¹. En una decisión de febrero de 2020 se falló a favor de Facebook en el fondo del caso, al considerar que no se había interferido indebidamente en la libertad de expresión del parlamentario³⁹².

³⁸⁷ Véase [en línea] https://www.nytimes.com/2007/01/05/business/worldbusiness/05fbriefs-JUDGEBLOCKSY_BRF.html.

³⁸⁸ Véase [en línea] <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Internet-Jurisdiction-Synthesis-2-Dec-2012.pdf>.

³⁸⁹ Véase Corte Constitucional de Colombia, *Acción de tutela interpuesta por John William Fierro Caicedo, contra Google Inc. y otros, N° T-063A/17*, Bogotá, 9 de mayo de 2018 [en línea] <http://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm>; Internet & Jurisdiction Policy Network, “Colombian Constitutional Court rules that Google must delete a blogger.com blog that contained defamatory statements”, París, 2017 [en línea] <https://www.internetjurisdiction.net/publications/retrospect#eyJ0byl6ijwMjAtMDgjifQ==>.

³⁹⁰ Véase D. Keller, “Why DC Pundits’ must-carry claims are relevant to global censorship”, Stanford, Center for Internet and Society (CIS), 13 de septiembre de 2018 [en línea] <http://cyberlaw.stanford.edu/blog/2018/09/why-dc-pundits-must-carry-claims-are-relevant-global-censorship>.

³⁹¹ Véase [en línea] <https://www.uol.com.br/tilt/noticias/redacao/2019/12/03/posts-de-novo-no-ar-facebook-perde-para-eduardo-bolsonaro-na-justica.htm>.

³⁹² Véase [en línea] <https://www.migalhas.com.br/quentes/323429/facebook-nao-indenizara-eduardo-bolsonaro-por-remover-posts-que-violaram-regras-da-rede-social>.

En conjunto, estas órdenes pueden tener importantes consecuencias para la moderación del contenido de las plataformas en los distintos países. Es difícil encontrar un mínimo común denominador entre las normas de los distintos países cuando algunos tribunales pueden ordenar que se retire cierto contenido mientras otros pueden ordenar que el mismo contenido se mantenga. Existe así un potencial real de conflicto jurisdiccional. Las plataformas están llamadas a ser los guardianes del equilibrio y no pueden retirar contenidos de manera excesiva o insuficiente.

La Red de Políticas de Internet y Jurisdicción, a través de su programa temático Content & Jurisdiction, ha propuesto una serie de marcos y soluciones para que tanto los gobiernos como las plataformas puedan lograr un equilibrio y gestionar el contenido, teniendo en cuenta la diversidad de leyes, costumbres y culturas en todo el mundo y, específicamente, en América Latina y el Caribe³⁹³.

4. Multas y sanciones

Las sanciones administrativas impuestas por las autoridades locales son un instrumento importante para hacer cumplir la regulación relativa a Internet. Las autoridades involucradas pueden variar en función de la cuestión específica de que se trate, como la protección del consumidor, antimonopolio, del medio ambiente o de los datos. Las sanciones por lo general consisten en advertencias, multas, suspensión o terminación de determinada actividad.

Como se ha descrito en secciones anteriores, muchas de las normas de protección de datos de la región se inspiraron en el marco jurídico europeo, que prevé duras sanciones administrativas. Una diferencia notable, sin embargo, es que las normas europeas prevén la cooperación internacional entre los países, mientras en América Latina y el Caribe la mayoría de las normas relativas a la responsabilidad administrativa tienen un alcance nacional.

Las sanciones administrativas por violación de la privacidad de los datos personales en la región incluyen multas de hasta 100.000 pesos (aproximadamente 1.500 dólares) en la Argentina³⁹⁴ y hasta 10.000 balboas (aproximadamente 10.000 dólares) en Panamá. En Trinidad y Tabago, las sanciones legales se basan en la facturación anual de una empresa, y se puede aplicar una multa de hasta el 10% de esta³⁹⁵. En el Brasil hay disposiciones específicas que exigen que las autoridades consideren los ingresos totales de la empresa en cuestión, lo que podría significar multas menores para las empresas más pequeñas³⁹⁶.

Aunque las leyes nacionales prevén la cooperación entre las autoridades de protección de datos, es justo decir que las sanciones y las órdenes se están imponiendo en un contexto nacional³⁹⁷. Los organismos reguladores competentes suelen verse enfrentados a la búsqueda de jurisdicción por parte de empresas que almacenan datos en un país distinto de aquel en el que se encuentran o residen las personas a las que se refieren los datos (y en el que se aplica la ley). El 1 de abril de 2020, la Superintendencia de Industria y Comercio de Colombia reafirmó su autoridad para imponer órdenes administrativas no solo a Facebook Colombia, sino también a Facebook Inc., situada en los Estados Unidos, y a Facebook Ireland, con sede en Irlanda³⁹⁸.

Un experto entrevistado afirmó que las recientes regulaciones de protección de datos se estaban convirtiendo cada vez más en una especie de ley extraterritorial, pues producían efectos en otros países y al mismo tiempo fomentaban una especie de “reconceptualización de la soberanía”. Este efecto extraterritorial se hace evidente cuando los organismos reguladores imponen sanciones que exigen explícitamente acciones de una empresa con sede en otro lugar. A fin de garantizar un ecosistema regulatorio que preserve el aspecto transnacional de Internet, las autoridades deberían ejercer sus competencias de cooperación internacional y considerar la posibilidad de concertar acuerdos bilaterales o multilaterales. La cooperación internacional es una de las principales líneas de acción para hacer cumplir la privacidad y debería tratarse como tal³⁹⁹.

Otra situación que se presenta en algunos países de la región es la incertidumbre sobre cuáles son los organismos competentes para aplicar las sanciones administrativas. En el Brasil, donde la Autoridad Nacional de Protección de Datos todavía no está plenamente operativa, la Secretaría Nacional del

³⁹³ Véase [en línea] <https://www.internetjurisdiction.net/news/content-jurisdiction-program-outcomes>.

³⁹⁴ Ley n.º 25.326, artículo 31. Véase [en línea] <https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/> actualización.

³⁹⁵ Data Protection Act, 2011, artículo 96. Véase [en línea] <http://www.ttparliament.org/legislations/a2011-13.pdf>.

³⁹⁶ Brasil, Ley n.º 13.709, artículo 52.4. Véase [en línea] http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

³⁹⁷ Véase, por ejemplo, Nicaragua, Ley n.º 787 de 2012, artículo 29.1.

³⁹⁸ Superintendencia de Industria y Comercio (SIC), resolución n.º 12192 de 2020. Véase [en línea] <https://www.sic.gov.co/sites/default/files/files/2020/Res%2012192%2001IV2020%20SIC%20Facebook%20Inc.pdf>.

³⁹⁹ Véase A. Brian, “Data protection and enforcement in Latin America and in Uruguay”, *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, D. Wright y P. de Hert (eds.), Berlín, Springer, 2016.

Consumidor (SENACON) ya ha ejecutado procedimientos administrativos y órdenes relativas a la protección de datos, incluidas multas tanto para Facebook Inc. como para Facebook Serviços Online do Brasil Ltda.⁴⁰⁰. Es cierto que las normas sobre datos, consumidores y competencia crean un margen para imponer sanciones, pero la medida en que se requieren en cada caso podría no estar aún clara. Así, en algunos casos se necesita una mayor cooperación y cohesión no solo en el contexto internacional, sino también en el nacional.

Muchos países de la región han aprobado leyes que imponen duras sanciones por el incumplimiento de las normas sectoriales que podrían aplicarse a las actividades de Internet, inspiradas en su mayoría en las normas europeas. Esto es particularmente frecuente en el campo de la protección de datos.

5. Las condiciones de servicio están entrelazadas con las leyes nacionales

Las condiciones de servicio creadas por las empresas multinacionales se han entrelazado con las leyes nacionales en algunos aspectos, y sirven como importante fuente de orientación sobre lo que está y no está permitido en esas plataformas. Por una parte, las empresas se enfrentan al reto de equilibrar la libertad de expresión con un contenido potencialmente dañino. Por otra, tienen que abordar los cambios significativos del panorama jurídico en esferas como la propiedad intelectual, la privacidad de los datos, las limitaciones de la responsabilidad y la protección del consumidor.

Las condiciones de servicio y las directrices de la comunidad implementan las obligaciones legislativas (en particular en lo que respecta al procedimiento), pero las complementan con las opiniones de las propias empresas sobre cómo debería ser el entorno de la plataforma. Varios de los temas que se presentan en este informe derivan de los conflictos entre las regulaciones nacionales y las condiciones de servicio y las directrices de la comunidad de los proveedores.

Un aspecto transfronterizo importante es que esas plataformas suelen construirse sobre una estructura de escala mundial o al menos regional. De este modo, muchos elementos de las condiciones de servicio que apoyan esa estructura tienen un núcleo común. Las normas desarrolladas por las plataformas cubren vastas áreas del mundo y tienen una influencia acorde. Las normas regulatorias y consuetudinarias nacionales pueden entrar en conflicto con esas condiciones y directrices, lo que hace necesaria una adaptación.

El problema es más grave en los casos en que las entidades que están detrás de las plataformas tienen menos recursos o son empresas emergentes. El rápido crecimiento puede ser particularmente disruptivo y conducir a conflictos regulatorios y culturales. Estos pueden surgir de un exceso de autorregulación, cuando las condiciones son más invasivas que las leyes del país o proporcionan soluciones diferentes (o, la mayoría de las veces, son más liberales o están menos desarrolladas), o tienen lagunas o vacíos, no abordando los tipos de comportamiento que deberían cubrirse, ya sea por exigencias regulatorias o por necesidades culturales.

Un tema estrechamente relacionado con esto es la moderación del contenido. Las condiciones de servicio y las directrices de la comunidad desempeñan un papel muy importante. El entorno de la plataforma se ve afectado por los tipos de discurso que se permiten y se fomentan. Los servicios de Internet dirigidos a los niños deben limitar algunos tipos de discurso que pueden ser legales pero que no son apropiados para los niños. En el otro extremo del espectro, los servicios dirigidos a una clientela más adulta pueden ser más liberales en lo que respecta a los tipos de contenido permitidos, pero deben tener en cuenta las normas relativas al contenido sexual en línea. Las situaciones relacionadas con la pornografía infantil y la pornografía de venganza (como se señala en la sección IV.A.4) suelen requerir una respuesta rápida.

Las condiciones y las directrices sirven para determinar el contenido que se mantiene y el contenido que se retira. Los gobiernos tienden a recurrir a esos instrumentos para presionar a las empresas a fin de que sostengan ciertos valores morales o alcancen determinados objetivos (como la aplicación de la ley). Para equilibrar estas necesidades, algunas plataformas han sugerido que se establezcan órganos de supervisión que puedan sugerir líneas de acción en casos particularmente espinosos⁴⁰¹.

Esto también es válido para la propiedad intelectual. La Unión Europea actualizó su Directiva sobre los derechos de autor en el mercado único digital y creó incentivos para que las plataformas proporcionen mecanismos de moderación de contenidos, incluso antes de su publicación. Esta Directiva ha tenido

⁴⁰⁰ Véase Ministerio de Justicia y Seguridad Pública, "MJSP multa Facebook em R\$ 6,6 milhões", Brasilia, 30 de diciembre de 2019 [en línea] <https://www.gov.br/mj/pt-br/assuntos/noticias/mjsp-multa-facebook-em-r-6-6-milhoes>.

⁴⁰¹ Véase The Economist, "Facebook unveils details of its content-oversight board", Londres, 30 de enero de 2020 [en línea] <https://www.economist.com/business/2020/01/30/facebook-unveils-details-of-its-content-oversight-board>.

cierto impacto en los países de la región y algunos han iniciado procedimientos para reformar su legislación de propiedad intelectual. El Brasil, por ejemplo, realizó una consulta e inició un extenso estudio sobre una nueva estrategia nacional en materia de propiedad intelectual. Uno de los temas se refiere a los mecanismos de protección contra la piratería en línea y se basa mucho en los últimos avances del derecho europeo⁴⁰².

Algunos Gobiernos de América Latina y el Caribe han presionado a las plataformas de comercio electrónico o incluso celebrado acuerdos con ellas para mejorar las medidas que toman contra la piratería y la venta de productos falsificados. Estas acciones han llevado a muchas plataformas de comercio electrónico a autorregularse y a incluir medios no judiciales de solución de controversias en sus términos y condiciones. Utilizan métodos internos (en la mayoría de los casos automáticos) para encontrar y eliminar posibles infracciones (falsificación o piratería). Por lo general, estos mecanismos alternativos de solución de controversias brindan la oportunidad de que tanto el propietario como el presunto responsable de la infracción expresen su opinión.

Además de los sistemas de solución de controversias establecidos por el sector privado, los Gobiernos de la región promueven distintas iniciativas de corregulación. Estas iniciativas se inspiran en el Memorando de entendimiento sobre la venta de productos falsificados a través de Internet, facilitado por la Comisión Europea y acordado por varias plataformas, titulares de derechos y asociaciones⁴⁰³.

En muchos casos, en las condiciones de servicio se establecen la jurisdicción para la solución de controversias y el derecho aplicable. Estas se consideran contratos (aunque contratos de adhesión) que regulan la relación con los usuarios y asuntos como la autonomía de las partes. En la región, no obstante, la tradición de protección del consumidor es sólida y existe la percepción de que la autonomía de las partes debe limitarse, en particular cuando interviene un consumidor que no puede negociar las cláusulas del contrato. Esto refleja una tendencia emergente, ya identificada en el informe *Internet & Jurisdiction Global Status Report 2019*, a que los tribunales no confirmen las cláusulas de elección del foro y la jurisdicción aplicables de las condiciones de servicio de las plataformas de Internet internacionales.

B. Principales enfoques técnicos

América Latina y el Caribe no es una excepción a la regla de que varias de las cuestiones jurídicas más importantes relacionadas con Internet y la jurisdicción suelen abordarse mediante soluciones técnicas. Algunas de ellas han seguido líneas similares a las de las soluciones alcanzadas en otros países del mundo, pero otras han adquirido un color regional muy particular. En esta sección se procura presentar y analizar los enfoques técnicos más significativos como se presentaron en la región y destacar las peculiaridades que se han registrado entre los países de América Latina y el Caribe. El análisis se ha realizado desde la perspectiva de los efectos transfronterizos que pueden tener y sus consecuencias prácticas y legales.

La mayoría de los enfoques técnicos que se presentan aquí tiene por objeto abordar la manera de controlar y limitar el acceso al contenido. Han sido la fuente de grandes disputas en Internet durante la última década. En cierta medida, los países comenzaron por adoptar un enfoque de *laissez faire* más liberal en la producción y distribución de contenidos. Se pidió a los intermediarios que se autorregularan y los productores de contenidos eran responsables de los contenidos que divulgaban. A mediados de la década, algunos países de la región comenzaron a cuestionar esta visión y a desarrollar y desplegar las técnicas que se examinan en el presente informe.

Las tecnologías de geolocalización, que en el pasado rara vez formaban parte de la arquitectura de los servicios de Internet, se consideran ahora más pertinentes. En el *Internet & Jurisdiction Global Status Report 2019* se señala, y la encuesta realizada para ese informe lo confirma, que hay opiniones divergentes sobre la conveniencia de introducir esas técnicas a mayor escala. Tal vez la divergencia más importante se relaciona con el filtrado de contenidos. En una serie de iniciativas nacionales se ha estudiado la conveniencia de imponer tecnologías de filtrado para determinadas partes de Internet, en particular las grandes redes de medios sociales.

El bloqueo de servicios y aplicaciones de Internet (apps) es una cuestión importante. En varios casos, los gobiernos, los tribunales y las propias empresas han impedido el acceso a determinados servicios y

⁴⁰² Véanse [en línea] <http://cultura.gov.br/ministerio-da-cidadania-abre-consulta-publica-sobre-reforma-da-lei-de-direitos-autoriais/>; <http://www.mdic.gov.br/index.php/ultimas-noticias/3948-grupo-interministerial-de-propriedade-intelectual-inicia-atividades>.

⁴⁰³ Véase [en línea] https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en.

aplicaciones, con diversos grados de transparencia y garantías procesales debidas. En muchos casos, esto se ha hecho para cumplir una ley local o una orden judicial de otra naturaleza. También se han producido cortes de toda Internet, pero normalmente han sido temporales y limitados a zonas específicas.

Otros enfoques técnicos que se han aplicado incluyen las limitaciones del Sistema de Nombres de Dominio impuestas en virtud de órdenes judiciales que requieren la suspensión, la supresión, la no resolución, la incautación y la transferencia, o el bloqueo o la desviación de direcciones IP y el bloqueo del Localizador Uniforme de Recursos (URL). Por último, algunos países han examinado y, en cierta medida, implementado la localización obligatoria de los datos. Todas esas técnicas limitan el funcionamiento de Internet como se previó originalmente y están cambiando rápidamente el panorama regulatorio. Los enfoques técnicos pueden ser útiles para hacer frente a los desafíos jurídicos transfronterizos, pero es necesario comprender sus consecuencias y buscar un consenso sobre la conveniencia de su aplicación.

1. Tecnologías de geolocalización

Si se trazara un mapa de Internet, la versión original no tendría fronteras. Los protocolos que controlan Internet fueron diseñados para ignorar las fronteras de los países, dándole así un carácter sin fronteras. Sin embargo, las tecnologías de geolocalización han servido para dar un cierto grado de geografía a Internet. En términos generales, estas tecnologías son capaces de determinar la posición geográfica de los usuarios, lo que permite a los proveedores de servicios adaptar algunos atributos a las peculiaridades de ese lugar, cambiar características como el idioma predeterminado, proporcionar resultados más precisos (por ejemplo, mostrar dónde se encuentra el restaurante más cercano) e incluso limitar el acceso a determinados componentes o contenidos en función de las costumbres y normas culturales, sociales o jurídicas.

La tecnología de la geolocalización no es uniforme, sino que se basa en una serie de aspectos como las direcciones IP, el Sistema de Posicionamiento Global (GPS), el idioma por defecto del dispositivo o las actividades para las que se utiliza (correr, caminar, conducir), la triangulación de las torres de telefonía móvil e incluso las señales de wifi y Bluetooth. El grado de certeza y precisión con que se localiza el dispositivo varía en consecuencia. Otro aspecto que puede afectar su precisión es el uso de una tecnología de enmascaramiento, como una red privada virtual (VPN), que emplea técnicas que bloquean o informan erróneamente sobre la ubicación de la persona o el dispositivo.

En muchos lugares del mundo, el debate sobre el uso de las tecnologías de geolocalización ha madurado en las dos últimas décadas. En Europa, sobre todo, el debate comenzó con una discusión sobre la posibilidad de implementar esas técnicas, dado su nivel de precisión, y ha evolucionado para centrarse en su idoneidad y el alcance de su utilización. Además de las políticas para constituir un mercado único digital europeo, la Unión Europea ha incluso promulgado la regulación núm. 2018/302 relativa al bloqueo geográfico, una de las posibles funciones de las tecnologías de geolocalización.

Esta regulación limita el uso de esas tecnologías en casos de “bloqueo geográfico injustificado”, que se entiende ocurre en tres circunstancias: i) la venta de bienes sin entrega física (los clientes tienen derecho a comprar productos vendidos por tiendas situadas en países distintos de aquel en el que se encuentran); ii) la venta de servicios suministrados electrónicamente (un cliente puede optar por utilizar un servicio suministrado por un proveedor de otro país y no se le debe exigir el pago de honorarios adicionales); iii) la venta de servicios prestados en un lugar físico determinado (por ejemplo, precios con descuento para las personas en un lugar determinado).

En América Latina y el Caribe, el debate sobre el bloqueo geográfico no tiene todavía la especificidad normativa que tiene en otros países y regiones. Sin embargo, existe un floreciente debate político y jurídico sobre las repercusiones de las tecnologías de geolocalización en relación con la protección de los consumidores y los datos, especialmente el bloqueo geográfico y la fijación de precios geográficos.

En el Brasil, por ejemplo, la empresa de viajes en línea Despegar ha sido multada por someter a sus clientes tanto al bloqueo geográfico como al precio geográfico. El caso se refería a la discriminación de clientes de la Argentina y el Brasil, ya que algunos hoteles se ofrecían con precios medios más altos para los clientes brasileños que para los argentinos. Además, la empresa bloquearía el acceso a determinados hoteles y servicios (alquiler de determinados autos) a los clientes de un país y no del otro⁴⁰⁴.

⁴⁰⁴ Véase Secretaría Nacional del Consumidor (SENACON), *Nota Técnica*, N° 92/2018, Brasilia, 16 de junio de 2018.

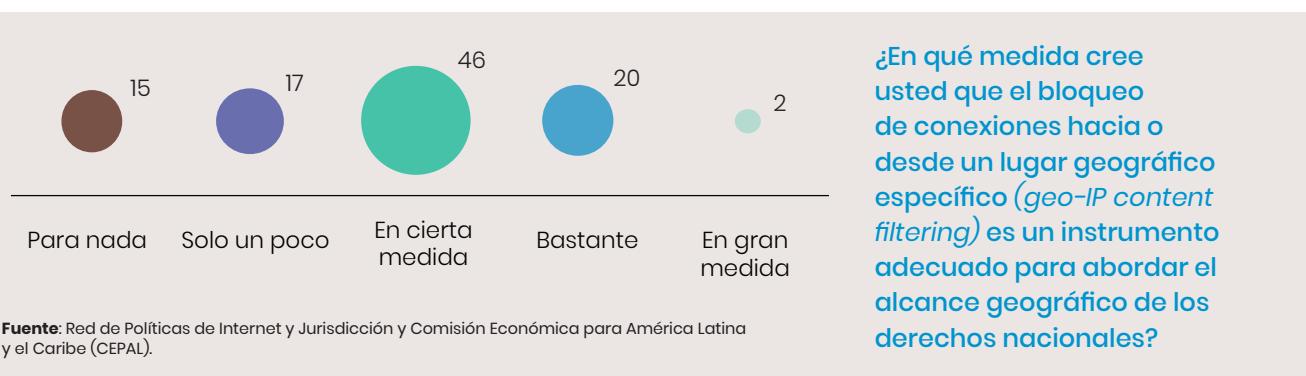
Las leyes de protección de datos prevén que las actividades de procesamiento de datos se dirijan a un país o lugar determinado. Esto implica cierto grado de georreferenciación y el uso de tecnologías de geolocalización. El Reglamento General de Protección de Datos (RGPD), por ejemplo, entra en juego cuando las empresas dirigen sus actividades al mercado común. Lo mismo puede verse en la Ley General de Protección de Datos Personales del Brasil.

Al igual que en el *Internet & Jurisdiction Global Status Report 2019*, las cuestiones planteadas por los interesados encuestados se centraron en tres temas: i) estas tecnologías pueden evitarse fácilmente y pueden no ser particularmente eficaces, ii) pueden repercutir en la libertad de expresión y el acceso a la información y iii) pueden aplicarse en determinadas circunstancias comerciales. La similitud entre las observaciones realizadas por los encuestados mundiales y regionales es sorprendente, aunque los expertos de la región parecen opinar que esas tecnologías podrían ser más útiles en un entorno comercial que en un entorno público. Un experto mencionó que las tecnologías de geolocalización podrían no ser apropiadas para los procesos democráticos. La preocupación en la región parece ser sobre el acceso a la información. Así pues, existe la opinión de que las tecnologías de geolocalización pueden impedir el acceso a la información almacenada fuera del país.

Mientras la lucha contra la pandemia de COVID-19 continúa, los países de la región tratan de hacer un mayor uso de los datos para afrontar mejor la propagación del virus. Las tecnologías de geolocalización desempeñan un papel cada vez más importante en la determinación del grado de distanciamiento físico adoptado por grupos numerosos o el mapeo de las rutas y los contactos de las personas infectadas.

La preocupación por la privacidad y la protección de los datos es cada vez mayor, ya que el carácter transfronterizo de Internet facilita el almacenamiento de datos delicados en un país extranjero. Además, en los países con una historia reciente de regímenes autoritarios se registran manifestaciones públicas de personas que afirman que el uso de datos de geolocalización para luchar contra la pandemia es una excusa para introducir un control sin precedentes de los ciudadanos.

Cabe esperar que, como legado de la lucha contra el COVID-19, en la región se desarrolle un debate más informado sobre el uso de las tecnologías de geolocalización, entrelazado con cuestiones políticas, jurídicas y técnicas.



2. El filtrado de contenidos aumenta, a medida que los países luchan contra el discurso de odio y la desinformación

Casi ningún país de América Latina y el Caribe organizó sus redes a priori para bloquear (o filtrar) el contenido entrante o vigilar el contenido producido localmente. Esas restricciones no se instalaron como parte integrante de la red en la infraestructura de los países de la región (también conocida como la columna vertebral Internet). Sin embargo, muchos gobiernos han buscado imponer a los proveedores de acceso o a los proveedores de servicios de Internet la obligación de vigilar, filtrar o eliminar ciertas categorías de contenido en un breve período. En algunas circunstancias, esas regulaciones pueden tener objetivos legítimos y aplicarse con límites y controles razonables. En otras, pueden tener un impacto similar a la censura y pueden incluso dar forma al discurso político y cultural, repercutiendo inadvertidamente en la libertad de expresión o incluso ampliando las protecciones del derecho de autor sin justificación.

En cuanto al filtrado incorporado en la columna vertebral de Internet, se ha informado que el Gobierno de Cuba ha establecido medidas técnicas capaces de filtrar el contenido de Internet⁴⁰⁵. En los informes se afirma que los mensajes que contienen palabras específicas como “democracia” o “dictadura” nunca llegan a su destino, y que ciertos servicios de Internet considerados incompatibles con los valores del Estado cubano no están disponibles en línea.

El Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) ha analizado la estructura institucional que restringe y filtra el contenido disponible en Internet en Cuba⁴⁰⁶. Entre las regulaciones relevantes que ha detectado, cabe mencionar la resolución núm. 127 de 2007, relativa a la seguridad de las tecnologías de la información, y la resolución núm. 179 de 2008, una regulación para los proveedores de servicios de Internet que se ocupa del acceso público a Internet. Mientras la primera prohíbe la circulación de datos o información contrarios al “interés social o a la moral y las buenas costumbres”, la segunda impone a los proveedores de servicios de Internet la obligación de vigilar y “regular” el contenido en línea y establece un régimen de responsabilidad directa para los intermediarios⁴⁰⁷. Se considera que estos reglamentos afectan la libertad de expresión y la libertad de acceso a la información⁴⁰⁸.

En la República Bolivariana de Venezuela, la Ley de Responsabilidad Social en Radio, Televisión y Medios Electrónicos (Ley RESORTE) establece que los proveedores de servicios de Internet pueden ser considerados responsables de la información que se ponga a disposición y que fomente la zozobra en la ciudadanía, desconozca a las autoridades legítimamente constituidas, incite a la alteración del orden público, y difunda o promueva el incumplimiento del ordenamiento jurídico vigente⁴⁰⁹.

A principios de 2019, la Asamblea Nacional Constituyente de la República Bolivariana de Venezuela presentó un proyecto de ley denominado Ley Constitucional del Ciberespacio de la República Bolivariana de Venezuela. Se informa que se han previsto amplias facultades para que el gobierno regule Internet dentro del país, incluido el filtrado obligatorio de contenidos⁴¹⁰. Este es un tipo de panorama regulador en el que los proveedores y los proveedores de servicios de Internet en general tienen incentivos para filtrar el contenido.

Además, en noviembre de 2017 la República Bolivariana de Venezuela aprobó una Ley contra el Odio que autoriza a las autoridades a revocar las licencias y bloquear los servicios de Internet si los proveedores de servicios de Internet muestran contenidos (incluidos los de terceros) que el gobierno considera que promueven el odio o la intolerancia⁴¹¹. Si bien no requiere de por sí la aplicación de filtros de contenido, la dureza de las sanciones crea un entorno que incentiva el empleo de estas tecnologías.

Las autoridades de otros países de la región están preocupadas por la difusión de la desinformación, en particular durante las elecciones. El escándalo en el que se ha visto involucrada Cambridge Analytica, una empresa acusada de utilizar datos personales para crear campañas de desinformación personalizadas, ha llevado a muchos países de América Latina y el Caribe a revisar sus leyes relativas al papel de los intermediarios de Internet.

Algunos países han impulsado una legislación que obligaría a los proveedores de servicios a instrumentar mecanismos para detectar y, en algunos casos, eliminar contenidos que desinformen, sobre todo durante las elecciones. El Relator Especial para la Libertad de Expresión ha declarado que, de conformidad con las normas del sistema interamericano de protección de los derechos humanos, toda regulación que requiera que los proveedores de servicios de Internet implementen el bloqueo o el filtrado de contenidos debe limitarse a casos excepcionales como la pornografía infantil, la propaganda de guerra y el discurso de odio que constituyan una incitación a la violencia o al genocidio, con la protección adicional de que un juez independiente determine la ilegalidad del contenido.

⁴⁰⁵ Véase A. Shahbaz y A. Funk, *Freedom on the Net 2019: The Crisis of Social Media*, Washington, D.C., Freedom House, 2019 [en línea] <https://www.freedomonthenet.org/country/cuba/freedom-on-the-net/2019#B1>.

⁴⁰⁶ Véase Relator Especial para la Libertad de Expresión, *Special Report on the Situation of Freedom of Expression in Cuba*, Washington, D.C., 2019.

⁴⁰⁷ *Ibidem*.

⁴⁰⁸ *Ibidem*.

⁴⁰⁹ Véase [en línea] <http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electrónicos.pdf>.

⁴¹⁰ Véase [en línea] <https://www.accessnow.org/a-bill-in-venezuela-seeks-to-give-the-government-absolute-control-over-the-internet/>.

⁴¹¹ Véase [en línea] <https://www.bloomberg.com/news/articles/2017-11-08/venezuela-passes-anti-hate-law-threatening-media-censorship>.

3. El Sistema de Nombres de Dominio: suspensiones y bloqueos derivados de notificaciones y órdenes judiciales y administrativas

El Sistema de Nombres de Dominio se encuentra en la raíz misma de Internet, funcionando como un sistema de direcciones que ayuda a los usuarios a encontrar su camino en la red. Cada uno de los dispositivos conectados a la red tiene una dirección única, una serie de números llamada dirección IP. El Sistema permite que esas series de números se conviertan en conjuntos de letras, facilitando así a los usuarios su memorización.

Como se menciona en el *Internet & Jurisdiction Global Status Report 2019*, cada vez se envían más solicitudes transfronterizas de suspensión de nombres de dominio a operadores técnicos en relación con contenidos o actividades presuntamente abusivos en los sitios web subyacentes⁴¹². Este enfoque es atractivo para los solicitantes porque la suspensión de un nombre de dominio tiene un efecto global directo e inmediato.

Los efectos de gran alcance de la manipulación del Sistema de Nombres de Dominio hacen necesario un análisis muy cauteloso de las presuntas infracciones y una reflexión sobre la proporcionalidad de la medida. La suspensión o el bloqueo de un nombre de dominio completo significa que todo el contenido de un sitio web determinado deja de estar disponible. Por lo tanto, los operadores deben considerar la manipulación del Sistema de Nombres de Dominio como una medida de último recurso que solo se utilizará si no hay otra forma de abordar la conducta o el contenido supuestamente infractor.

Debido a que tienen el efecto práctico de sacar rápidamente el contenido fuera de línea en todo el mundo, las suspensiones y bloqueos a nivel del Sistema de Nombres de Dominio se han utilizado para abordar cuestiones muy diferentes, desde las infracciones a los derechos de propiedad intelectual hasta el discurso perjudicial. La decisión de retirar un determinado nombre de dominio puede ser motivada simplemente por una notificación de la víctima de una presunta infracción, pero también puede ser exigida por órdenes administrativas y judiciales.

Naturalmente, las notificaciones de suspensión o bloqueo de nombres de dominio pueden tener un impacto transfronterizo. El nombre de dominio “1dmx.org” se registró para albergar un sitio web de protesta contra el uso excesivo de la fuerza por parte de la policía en México. El nombre de dominio era una referencia al día en que Enrique Peña Nieto prestó juramento como Presidente en diciembre de 2012. Ese día estallaron varias protestas que fueron reprimidas por la policía. Docenas de estudiantes y manifestantes fueron detenidos, y un manifestante murió. Un año después, el sitio web fue cerrado a raíz de una solicitud de suspensión del nombre de dominio recibida por GoDaddy, el registro de nombres de dominio, del Departamento de Seguridad Nacional de los Estados Unidos. El motivo del retiro fue que el sitio web era “parte de una investigación policial en curso”⁴¹³ y que su contenido violaba las condiciones de servicio de la empresa⁴¹⁴.

Algunos gobiernos de la región son conocidos por sus prácticas de bloqueo del Sistema de Nombres de Dominio, aunque esta medida no se ha extendido a toda la región. Recientemente, el Gobierno de la República Bolivariana de Venezuela bloqueó la red Tor, una herramienta que permite a los usuarios navegar por Internet de forma anónima. El bloqueo fue ejecutado por el proveedor de servicios de Internet de propiedad del gobierno CANTV, el mayor proveedor de servicios de Internet del país⁴¹⁵. Para acceder a la herramienta bloqueada, los usuarios venezolanos debían recurrir a las redes privadas virtuales (VPN) para eludir la regulación gubernamental.

Con respecto a Cuba, se ha informado que varios sitios web, incluidos medios de comunicación, han sido bloqueados en los “parques wifi” (nombre que se da a los espacios públicos donde se puede acceder a Internet)⁴¹⁶.

Siguiendo una tendencia mundial, las órdenes judiciales de bloqueo o suspensión de nombres de dominio están aumentando en América Latina y el Caribe. En la Argentina, por ejemplo, la Cámara Argentina de Productores de Fonogramas y Videogramas (CAPIF) y otras empresas de gestión de derechos de autor presentaron una demanda y se les concedió un mandato judicial⁴¹⁷ para bloquear

⁴¹² Véase D. Jerker, *Internet & Jurisdiction Global Status Report 2019*, París, Internet & Jurisdiction Policy Network, 2019.

⁴¹³ Véase [en línea] <https://www.civicus.org/documents/reports-and-publications/SOCs/2017/essays/freedom-of-expression-in-latin-america-the-struggle-continues-in-the-digital-environment.pdf>.

⁴¹⁴ Véase L. García, “Political Internet censorship: a reality in Mexico (with a little help from the United States and GoDaddy.com)”, *Digital Rights: Latin America and the Caribbean*, E. Magrani (ed.), Rio de Janeiro, GV Direito Rio, 2018 [en línea] <https://itsrio.org/wp-content/uploads/2018/01/digital-rights.pdf>.

⁴¹⁵ Véase Access Now, “Venezuela blocks access to the Tor network”, Nueva York, 2018 [en línea] <https://www.accessnow.org/venezuela-blocks-tor/>.

⁴¹⁶ Véase The Tor Project, “Measuring Internet Censorship in Cuba’s parknets”, 2017 [en línea] <https://blog.torproject.org/measuringinternet-censorship-cubas-parknets>.

⁴¹⁷ Véase [en línea] https://www.scribd.com/fullscreen/232015119?access_key=key-2j7jKuMaBADAeV4XpAOw&allow-share=true&escape=false&view_mode=scroller/.

Pirate Bay, un sitio web de intercambio de archivos muy popular⁴¹⁸. El mandato judicial ordenaba a los proveedores de servicios de Internet que bloquearan varios nombres de dominio asociados con el sitio web de intercambio de archivos, como thepiratebay.org y thepiratebay.se⁴¹⁹.

Como señaló la organización no gubernamental (ONG) Derechos Digitales, “en vez de bloquear los enlaces que apuntan a obras sobre las que se sospecha infracción, a la obra de un artista en particular, un grupo de artistas o los enlaces a obras musicales o fonográficas en general, se ha decidido prohibir el acceso al sitio completo”⁴²⁰.

Varios relatores para la libertad de expresión recordaron recientemente que el bloqueo de sitios web enteros, direcciones IP, puertos o protocolos de red dispuesto por el Estado es una medida extrema que solo puede justificarse cuando está estipulada por ley y es necesaria para proteger un derecho humano u otro interés público legítimo, lo que incluye que sea proporcionada, que no haya medidas alternativas menos invasivas que puedan preservar ese interés y que respeten las garantías procesales debidas^{421 422}.

4. Bloqueo de sitios y aplicaciones

La interrupción del acceso o los servicios de Internet o el bloqueo de aplicaciones es una medida que se aplica en muchos países del mundo. En el *Internet & Jurisdiction Global Status Report 2019* se mencionó esta tendencia y se destacaron sus repercusiones transfronterizas. La mayoría de las veces, los proveedores de servicios son empresas extranjeras y es difícil que las interrupciones estén claramente delimitadas.

Debido a la arquitectura de Internet y a su naturaleza interconectada, una interrupción del servicio en un lugar puede perjudicar el acceso o la posibilidad de uso en otro. Si el corte se implementa en la capa de infraestructura de Internet, es aún más probable que tenga repercusiones más allá del territorio previsto originalmente. Es posible que los usuarios no se limiten a un solo país y que los servicios se presten a través de un sistema transnacional.

Los países de América Latina y el Caribe no son diferentes. Una de las partes interesadas entrevistadas señaló que la infraestructura de Internet de la región es compartida por muchos países y empresas. Algo que ocurre en determinado lugar puede tener repercusiones en otros, incluso en diferentes Estados. En muchos casos, gobiernos, tribunales y empresas han bloqueado algunos servicios de Internet y aplicaciones, con consecuencias más allá de la zona o el servicio al que se apuntaba. Otro interesado mencionó que lo que antes era una táctica de último recurso, hoy se ha convertido en una práctica común.

En diciembre de 2015, un juez brasileño ordenó bloquear durante 48 horas la aplicación del servicio de mensajería instantánea WhatsApp ante la negativa a entregar datos de comunicaciones de interés para investigaciones criminales en curso. A este, que no fue un caso aislado, le siguieron otras dos órdenes en virtud de las cuales se bloqueó la misma aplicación en distintos estados del país. Todas las órdenes judiciales fueron revocadas rápidamente, pero el asunto sigue pendiente de una decisión en dos casos constitucionales ante el Supremo Tribunal Federal (STF) del Brasil. Estos casos se refieren al alcance de las facultades de los jueces para ordenar el bloqueo de servicios de esta manera y al argumento de que es técnicamente imposible acceder a los datos debido al cifrado de extremo a extremo utilizado por el servicio de mensajería.

La orden de bloqueo fue emitida para las empresas de telecomunicaciones, que las cumplieron mediante la interrupción del acceso a nivel de infraestructura. Se informó que los usuarios de la aplicación en la Argentina y Chile también se vieron afectados y no pudieron acceder al servicio⁴²³.

Un experto entrevistado mencionó un mandato judicial de un juez electoral de Santa Catarina (Brasil) que exigía el bloqueo de Facebook por desobedecer una orden judicial relativa a un presunto perfil falso que se burlaba de un alcalde. Facebook argumentó que había cumplido con la orden original y por lo tanto el mandato judicial no fue ejecutado⁴²⁴.

⁴¹⁸ Véase [en línea] <https://www.derechosdigitales.org/7608/internet-bajo-censura-bloquean-pirate-bay-en-argentina/>.

⁴¹⁹ Véase [en línea] <https://www.lanacion.com.ar/tecnologia/la-comision-nacional-de-comunicaciones-ordena-el-bloqueo-de-the-pirate-bay-en-la-argentina-nid1705910/>.

⁴²⁰ Véase [en línea] <https://www.derechosdigitales.org/7608/internet-bajo-censura-bloquean-pirate-bay-en-argentina/>.

⁴²¹ Véase Organización para la Seguridad y la Cooperación en Europa (OSCE) y otros, *Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade*, Viena, 2019 [en línea] <https://www.osce.org/representative-on-freedom-of-media/42528?download=true>.

⁴²² Véase [en línea] http://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf.

⁴²³ Véase [en línea] <https://www.nytimes.com/2015/12/18/world/americas/brazil-whatsapp-facebook.html>.

⁴²⁴ Véase [en línea] <https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24-horas/62909>.

En otras ocasiones, los jueces brasileños han ordenado la eliminación de aplicaciones de las tiendas de aplicaciones de Google y Apple. En el caso de la aplicación Secret, el fundamento era que constituía un “santuario para el ciberacoso”⁴²⁵. En un caso similar, un juez ordenó a Microsoft eliminar la aplicación Cryptic, que ofrecía un servicio similar de mensajería anónima, de los teléfonos Windows⁴²⁶.

En octubre de 2019, coincidiendo con las protestas en Quito por la publicación por parte del Presidente Lenin Moreno del decreto núm. 883, que instauraba medidas de austeridad, se informó que algunos servicios de mensajería e intercambio multimedia como Facebook y WhatsApp no estaban disponibles en el Ecuador⁴²⁷.

Mediante un decreto emitido en Buenos Aires, el 13 de abril de 2016 se exigió a la plataforma de automóviles compartidos Uber que dejara de operar en la ciudad. Los proveedores de servicios de Internet recibieron instrucciones de cerrar la aplicación móvil y la plataforma en línea de Uber⁴²⁸. El servicio de la empresa multinacional no solo se interrumpió en la ciudad de Buenos Aires, como estaba previsto, sino que también se vieron afectadas zonas fuera de la capital.

El 20 de diciembre de 2019, la Superintendencia de Industria y Comercio (SIC) de Colombia falló en contra de la aplicación de automóviles compartidos Uber, afirmando que la empresa había violado las leyes de competencia y antimonopolio del país⁴²⁹. El fallo instruyó a los proveedores de servicios de Internet a bloquear el acceso a la aplicación. Los interesados sostuvieron que esta orden violaba el principio de neutralidad de la red⁴³⁰.

En 2019, se informó que la República Bolivariana de Venezuela sufrió algún tipo de restricción del servicio que duró 171 horas y afectó particularmente a Twitter, WhatsApp, YouTube y Periscope⁴³¹. También se difundió ampliamente que la enciclopedia en línea Wikipedia había sido bloqueada tras lo que se denominó una “guerra de edición” sobre si Juan Guaidó o Nicolás Maduro era el Presidente legítimo del país⁴³².

El 14 de noviembre de 2019, el Ministerio de Transportes y Comunicaciones (MTC) del Perú emitió el decreto núm. 035/2019, que otorga facultades para bloquear, de manera unilateral y sin una orden judicial, las aplicaciones de transporte que se considere que ofrecen servicios ilegales (esto incluye bicicletas, taxis y monopatines eléctricos)⁴³³. Se informa que el Ministerio ha dado instrucciones a los proveedores de servicios de Internet para bloquear ciertas aplicaciones de transporte y a las tiendas de aplicaciones de Apple y Google para que dejen de mostrarlas⁴³⁴.

5. Cortes de servicio

Los cortes de Internet son una interrupción deliberada del acceso a Internet ordenada por las autoridades locales por períodos breves, por lo general en situaciones en que existe una amenaza, real o supuesta, al orden público. Estos cortes pueden tener consecuencias desestabilizadoras, ya que no solo impiden la comunicación sino también el acceso a la información. Sin acceso a Internet, la capacidad de la población para realizar muchas actividades diarias se ve afectada. Las personas pueden verse imposibilitadas de comunicarse en línea, realizar actividades de investigación e incluso acceder a servicios básicos, algunos de ellos públicos.

A medida que las transacciones financieras migran cada vez más a Internet, el acceso al dinero y a diferentes recursos también puede verse interrumpido. Las consecuencias más duraderas se relacionan con la confianza del consumidor y la necesidad de que las empresas migren a alternativas más costosas debido a la inestabilidad de la red.

⁴²⁵ Véase Internet & Jurisdiction Policy Network, “Blocking apps: Brazil orders Apple, Google to remove Secret from stores and devices”, París, 2014 [en línea] <https://www.internetjurisdiction.net/publications/retrospect/#eyJ0byl6ijlwMTktMTIifQ==>.

⁴²⁶ Véase [en línea] <https://www.sfgate.com/business/article/Brazil-wants-no-Secret-on-app-stores-5701537.php>.

⁴²⁷ Véase [en línea] <https://www.accessnow.org/disrupciones-de-internet-en-ecuador-como-ocurrieron-y-como-eludirlas/>; <https://twitter.com/cidh/status/1183475097727832066>; C. Botero, “Ecuador restringe redes sociales durante las protestas de esta semana”, *El Espectador*, Bogotá, 11 de octubre de 2019 [en línea] <https://www.elespectador.com/opinion/ecuador-restringe-redes-sociales-durante-las-protestas-de-esta-semana-columna-885505>.

⁴²⁸ Véase Internet & Jurisdiction Policy Network, “Argentina: Uber faces blocking order and investigation by the DPA”, París, 2016 [en línea] <https://www.internetjurisdiction.net/publications/retrospect/#eyJ0byl6ijlwMTktMTIifQ==>.

⁴²⁹ Véase [en línea] <https://www.sic.gov.co/slider/superindustria-ordena-cese-de-la-prestacion-del-servicio-de-transporte-uber>.

⁴³⁰ Véase [en línea] <https://www.elespectador.com/tecnologia/que-tiene-que-ver-la-neutralidad-de-red-y-la-orden-de-suspender-uber-en-colombia-articulo-898079>.

⁴³¹ Véase S. Woodhams y S. Migliano, *The Global Cost of Internet Shutdowns in 2019*, Londres, Top10VPN, 2020 [en línea] <https://www.top10vpn.com/cost-of-internet-shutdowns/>.

⁴³² Véanse [en línea] <https://netblocks.org/reports/wikipedia-blocked-in-venezuela-as-internet-controls-tighten-XaAwR08M>; A. Azpúrrua y otros, “From the blocking of Wikipedia to social media: Venezuela’s political crisis”, *VeSinFiltro*, Caracas, 29 de enero de 2019 [en línea] <https://vesinfiltro.com/noticias/report-jan-2019/>.

⁴³³ Véase [en línea] <https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-precisa-disposiciones-sobre-el-servicio-decreto-supremo-n-035-2019-mtc-1826768-5/>.

⁴³⁴ Véase [en línea] <https://www.accessnow.org/blocking-apps-by-ministerial-decree-enables-illegal-content-takedowns-in-peru/>.

Los efectos de los cortes de Internet no se limitan a la dimensión nacional. Se impide el funcionamiento de una serie de servicios internacionales, lo que puede obstaculizar los planes de inversión en el país e incluso detener completamente la provisión de esos servicios, ya que las empresas pueden decidir marcharse. Las comunicaciones con el mundo exterior también se ven restringidas. Es posible que los miembros de una familia no puedan contactarse entre sí. Esto puede ser particularmente preocupante dado que los cortes de Internet suelen ocurrir en situaciones de disturbios civiles o políticos. En vista de un pasado en el que las desapariciones forzadas eran una práctica no poco común en muchos países de la región, la imposibilidad de ponerse en contacto con un ser querido puede tener un impacto social perturbador y consecuencias duraderas.

En la República Bolivariana de Venezuela, por ejemplo, no solo se han bloqueado aplicaciones y servicios de Internet, sino que se han producido cortes de Internet o interrupciones de la conectividad en zonas enteras durante breves períodos. Esos casos suelen estar relacionados con acontecimientos políticos importantes. En 2019, se informó que en varias ocasiones se habían producido cortes de Internet o grandes interrupciones de la conectividad, en particular vinculados al proveedor estatal de Internet. En la mayoría de los casos, estos acontecimientos coincidían con actividades políticas de Juan Guaidó (Presidente de la Asamblea Nacional de la República Bolivariana de Venezuela y autoproclamado Presidente del país). Un corte especialmente destacable de Internet se produjo durante una reunión entre Juan Guaidó y el Presidente de Colombia en la frontera entre ambos países.

En forma análoga, en 2018, en medio de protestas en diferentes partes de Nicaragua, se informó que Internet se había cortado o interrumpido en diferentes zonas de la capital, Managua⁴³⁵. El gobierno no reconoció la interrupción de Internet, pero se observó que existía una correlación entre las medidas adoptadas por las fuerzas gubernamentales y las regiones en las que Internet se interrumpió⁴³⁶.

Algunas instituciones regionales de derechos humanos, como el Sistema Interamericano de Derechos Humanos, a través de su Relatoría Especial para la Libertad de Expresión, condenaron los cortes y las interrupciones de Internet. Cuando estas iniciativas son tomadas por los gobiernos o en virtud de órdenes gubernamentales, se consideran como una “medida extrema—análoga a la prohibición de un periódico o una emisora de radio o televisión—. Dichos bloqueos o restricciones no pueden justificarse, ni siquiera por razones de orden público o seguridad nacional, y no pueden utilizarse como medidas de censura o como mecanismos para impedir el acceso a la información de la población”⁴³⁷.

La misma Relatoría se ha sumado a otras organizaciones internacionales para deplorar las interrupciones y los cortes arbitrarios para restringir el acceso a las redes de telecomunicaciones y a Internet⁴³⁸. De acuerdo con algunas organizaciones de la sociedad civil que se ocupan del tema, a pesar de esas condenas el número de interrupciones en la región aumentó de 1 a 14 entre 2018 y 2019, en países como Nicaragua, la República Bolivariana de Venezuela y el Ecuador⁴³⁹.

6. Localización obligatoria de los datos

La naturaleza de los datos es que sean fácilmente transmisibles y accesibles en todo el mundo. Sin embargo, el hecho de que sean accesibles en cualquier lugar pero deban almacenarse en alguna parte dificulta la supervisión de las disposiciones de seguridad para almacenarlos y asegurar un acceso continuo a ellos.

Varios países de la región han debatido sobre el almacenamiento de datos a nivel local y algunos incluso lo han ordenado. Los argumentos más importantes a favor de esa localización forzosa de los datos suelen estar relacionados con la seguridad nacional (tanto respecto de incidentes deliberados como no deliberados) y el acceso a los datos pertinentes por parte de los agentes encargados de hacer cumplir la ley. La lógica es que el acceso a los datos almacenados en servidores dentro del territorio bajo la jurisdicción del Estado es más fácil, lo que brinda más seguridad y control.

Esos posibles beneficios deben sopesarse frente a las posibles limitaciones de las transacciones de comercio electrónico que dependen de proveedores de servicios financieros extranjeros, por ejemplo, o de empresas que operan a través de la nube o, de hecho, de pequeñas y medianas empresas (pymes) que no

⁴³⁵ Véase [en línea] <https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9>.

⁴³⁶ Véase [en línea] <https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf>.

⁴³⁷ Véase Relatoría Especial para la Libertad de Expresión, “La Relatoría Especial condena cierre de Radio Caracas Radio 750 AM, censura de canales de televisión, restricciones en internet, y la detención de periodistas en Venezuela”, *Comunicado de Prensa*, N° RI16/19, Washington, D.C., 15 de mayo de 2019 [en línea] <http://www.oas.org/es/cidh/expresion/showarticle.asp?partID=1140&ID=2>.

⁴³⁸ Véase Organización para la Seguridad y la Cooperación en Europa (OSCE) y otros, *Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade*, Viena, 2019 [en línea] <https://www.osce.org/representative-on-freedom-of-media/425282?download=true>.

⁴³⁹ Véase [en línea] <https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf>.

pueden cumplir fácilmente los requisitos de localización para entrar en nuevos mercados. También puede obstaculizar la creación de mercados digitales unificados y limitar la prestación de servicios transfronterizos, lo que supone una desventaja especial para las empresas que aplican una estrategia centralizada⁴⁴⁰.

La localización de los datos no tiene que obedecer a un mandato explícito, pero puede ser el resultado *de facto* de una política. Puede haber requisitos que obstaculicen las transferencias transfronterizas de datos: esto se ha denominado localización condicional o blanda, en contraposición a la localización obligatoria⁴⁴¹. Los requisitos de las leyes de privacidad que condicionan las transferencias a un procedimiento que garantice los derechos de las personas a las que se refieren los datos pueden incluirse en esta categoría. La mayor parte de la legislación de protección de datos en América Latina y el Caribe suele seguir el modelo europeo y exige una decisión sobre la idoneidad o un procedimiento o mecanismos que garanticen la intención de la otra parte de cumplir con los mismos estándares de protección que se aplican en el país. Esto no limita directamente el flujo de datos, pero puede crear obstáculos.

Desde el escándalo de las revelaciones de Snowden en 2013, cuando datos relativos a altos funcionarios de muchos países se volvieron accesibles o fueron filtrados o entregados al Organismo Nacional de Seguridad de los Estados Unidos, varios gobiernos de la región han considerado la posibilidad de exigir que por lo menos algunos datos particularmente confidenciales se almacenen en servidores dentro de su territorio⁴⁴².

Un ejemplo muy significativo es una propuesta de enmienda al llamado Marco Civil de Internet del Brasil, que tiene por objeto ordenar la localización de los datos de manera muy general⁴⁴³. La enmienda está redactada de la siguiente manera: el Poder Ejecutivo, mediante decreto, podrá obligar a los proveedores de conexión y de aplicaciones de Internet previstos en el art. 11 que realicen sus actividades de manera organizada, profesional y con fines económicos a instalar o utilizar estructuras de almacenamiento, gestión y difusión de datos en el territorio nacional, teniendo en cuenta el tamaño de los proveedores, su facturación en el Brasil y la amplitud de la oferta de servicios al público brasileño⁴⁴⁴.

La propuesta fue rechazada, pero en la ley, tal como fue aprobada, se especifica que la legislación brasileña es aplicable cuando las empresas, incluso las extranjeras, ofrecen servicios al público brasileño⁴⁴⁵.

Si bien a veces no existe una legislación clara que obligue a la localización de los datos, se sigue cuestionando la disponibilidad o la conveniencia de permitir que ciertos datos se almacenen en servidores situados en otro territorio. Un ejemplo se refiere a los datos judiciales. El 21 de febrero de 2019, el Consejo Nacional de Justicia (CNJ) del Brasil suspendió los procedimientos de contratación para obtener servicios de computación en la nube de Microsoft, debido a la preocupación de que las bases de datos de los tribunales brasileños contenían información sobre la vida, la economía y la sociedad brasileña que podría poner en peligro la seguridad y los intereses nacionales del Brasil⁴⁴⁶. Aunque no había ninguna orden que exigiera el almacenamiento de los datos judiciales en territorio brasileño, la suspensión tuvo la consecuencia indirecta de bloquear el servicio debido a la ubicación transfronteriza de los servidores.

De manera similar, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia expresó su preocupación por los riesgos de depender del almacenamiento en la nube para implementar servicios básicos. Como medida de mitigación, la autoridad pidió a la Procuraduría General de la Nación que impusiera requisitos de localización de los datos para la adquisición de servicios en la nube por parte de los organismos gubernamentales⁴⁴⁷.

Con respecto a los mandatos indirectos de localización de los datos, la Dirección Nacional de Protección de Datos Personales de la Argentina emitió la disposición núm. 18/2015, que trata el almacenamiento en la

⁴⁴⁰ Véase Comisión Económica para América Latina y el Caribe (CEPAL), “Mercado digital regional: aspectos estratégicos”, *Documentos de Proyectos* (LC/TS.2018/30), Santiago, 2018.

⁴⁴¹ Véase [en línea] <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>.

⁴⁴² Véanse G. Greenwald, “NSA collecting phone records of millions of Verizon customers daily”, *The Guardian*, Londres, 6 de junio de 2013 [en línea] <http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>; G. Greenwald, R. Kaz y J. Casado, “EUA espionaram milhões de e-mails e ligações de brasileiros”, *O Globo*, Brasilia, 7 de diciembre de 2013 [en línea] <http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934#ixzz2IEHzqYwh>.

⁴⁴³ Véanse [en línea] https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa__pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf; <https://igarape.org.br/marcocivil/en/>; Internet & Jurisdiction Policy Network, “Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction”, París, 2014.

⁴⁴⁴ Véase Congreso Nacional, “Substitutivo ao Projeto de Lei 2126 de 2011”, 2013 [en línea] <http://infojustice.org/wp-content/uploads/2013/11/Marco-Civil-English-Translation-November-2013.pdf>.

⁴⁴⁵ Véase [en línea] <https://www.camara.leg.br/noticias/429574-camara-aprova-projeto-do-marco-civil-da-internet>.

⁴⁴⁶ Véase [en línea] <https://www.conjur.com.br/dl/cnj-proibe-tj-sp-contratar-microsoft.pdf>. Esta decisión fue apelada y confirmada el 25 de junio de 2019. Véase [en línea] <https://www.conjur.com.br/dl/voto-schiefler-contrato-tj-sp-microsoft.pdf>.

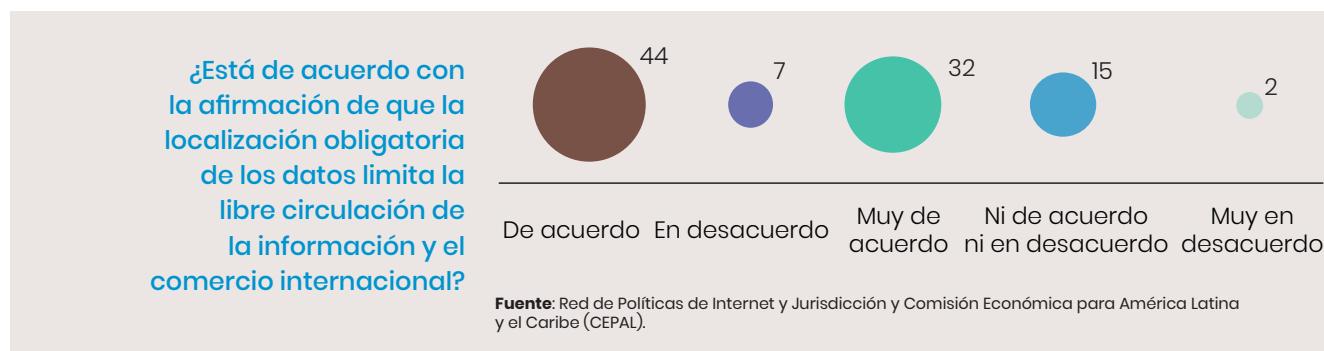
⁴⁴⁷ Colombia, proyecto Servicios Digitales Básicos. Véase [en línea] <https://estrategia.gobiernoonlinea.gov.co/w3-article-18756.html>.

nube como una transferencia internacional de datos, lo que significa que las aplicaciones que se ejecuten en un servicio de computación en la nube deben cumplir con la Ley de Protección de los Datos Personales⁴⁴⁸. Esto puede constituir una barrera al flujo de datos y limitar este tipo de aplicación. La obligación de obtener una autorización expresa adicional del usuario también representa un obstáculo. Las aplicaciones que utilizan servidores dentro del país tienen una ventaja sobre las que utilizan la computación en la nube.

Se informa también que la República Bolivariana de Venezuela tiene requisitos de localización de los datos. Estos parecen ser particularmente importantes en lo que respecta a la infraestructura de pago electrónico y procesamiento de pagos, pues los datos de los pagos deben procesarse localmente⁴⁴⁹.

En el otro extremo del espectro, México ha firmado un acuerdo con los Estados Unidos y el Canadá (Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá (T-MEC)) cuyas cláusulas de comercio digital incluyen una que prohíbe toda legislación que requiera que los servidores se encuentren dentro de la propia jurisdicción de un país miembro⁴⁵⁰.

Más del 70% de las partes interesadas encuestadas está de acuerdo o muy de acuerdo en que la localización obligatoria de los datos limita la libre circulación de la información y el comercio internacional.



Varios interesados mencionaron en sus observaciones que es natural que en una economía mundial en red los datos fluyan sin obstáculos a través de las fronteras y que la localización obligatoria de los datos restringe y agrupa Internet. Como cuestión técnica, uno de los interesados destacó la forma en que la localización obligatoria de los datos podría repercutir en la velocidad de la red y en la calidad de los servicios. Puede haber costos no solo en términos de precios más altos, sino también en el potencial de innovación. Una de las partes interesadas manifestó su preocupación por el hecho de que esas obligaciones restringieran la escala a la que podrían aspirar los actores más pequeños, ya que solo las empresas más grandes podrían sufragar los costos de infraestructura para mantener servidores en diferentes países.

Algunos de los interesados señalaron que el almacenamiento de los datos dentro del país podría estar justificado en algunos casos, por ejemplo cuando se trata de información confidencial, datos relativos a la administración pública y datos de seguridad nacional. Manifestaron preocupación con respecto a la computación en la nube y sugirieron que debería ser objeto de regulación. Un interesado observó, sin embargo, que se trataba de cumplir las leyes locales. Otro señaló que no todos los países tenían los recursos y los instrumentos necesarios para hacer cumplir las leyes nacionales, en particular cuando la aplicación de la ley tenía un componente extraterritorial.

Cabe señalar que, a pesar de la tendencia a la globalización, la localización nacional voluntaria de los datos se produce con mayor frecuencia en América Latina y el Caribe. Hay muchos factores posibles detrás de esto, pero la percepción de control y el deseo de satisfacer mejor los requisitos locales podrían ser los más comunes. Las opciones nacionales y la política pública pueden favorecer indirectamente el almacenamiento local de los datos.

La coherencia de políticas necesaria para construir un ecosistema digital regional próspero e integrado exige la misma coherencia en las definiciones que dan forma al debate. Internet fue creada hace más de 50 años y la World Wide Web ha superado su trigésimo aniversario.

⁴⁴⁸ Véase [en línea] <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

⁴⁴⁹ Véase [en línea] <https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>

⁴⁵⁰ Tratado entre los Estados Unidos Mexicanos, los Estados Unidos de América y Canadá (T-MEC) (30 de noviembre de 2018), artículo 19.12, Ubicación de las Instalaciones Informáticas: "Ninguna Parte podrá exigir a una persona cubierta usar o ubicar las instalaciones informáticas en el territorio de esa Parte, como condición para la realización de negocios en ese territorio". Véase [en línea] http://www.sice.oas.org/Trade/USMCA/USMCA_ToC_PDF_s.asp.

GLOSARIO

Algunos conceptos han madurado a lo largo de los años y han servido como puntos de partida bien conocidos para el debate político, mientras que otros siguen siendo muy polémicos ya que intentan captar los aspectos esenciales de las nuevas tendencias tecnológicas. Este breve glosario tiene por objeto poner al día a los nuevos actores en este campo respecto de los conceptos clave que se mencionan en el informe, añadiendo claridad a las tendencias y a las soluciones jurídicas y tecnológicas que se mencionan.

1. **Internet** es el sistema mundial de redes informáticas interconectadas que se basan en el conjunto de protocolos Internet (TCP/IP) para la comunicación entre redes y dispositivos.
2. **IP (protocolo Internet)** es el protocolo de comunicación Internet que permite a las redes de dispositivos comunicarse a través de una variedad de vínculos físicos. Cada dispositivo o servicio de Internet tiene al menos una dirección IP que lo identifica de forma exclusiva respecto de otros dispositivos o servicios de Internet⁴⁵¹.
3. **World Wide Web (WWW)** es un sistema de información en el que los documentos y otros recursos están interconectados por hipertexto y son accesibles a través de Internet, lo que hace fácil para cualquiera itinerar, navegar y contribuir⁴⁵².
4. **Sistema de Nombres de Dominio (Domain Name System (DNS))** es el sistema de nombres que ayuda a los usuarios a navegar en Internet. Cada computadora de la Internet tiene una dirección única, que consiste en una cadena de números (la “dirección IP”), por lo que el DNS facilita el uso de Internet permitiendo que se utilice una cadena conocida de letras (el “nombre de dominio”, como www.internetjurisdiction.net) en lugar de la dirección IP⁴⁵³.
5. **Jurisdicción** tiene diferentes significados en el derecho internacional. En este informe el término se utiliza para hacer referencia a la facultad de oír o tomar decisiones sobre un asunto específico, por parte de una autoridad o un órgano jurídico oficialmente constituido. Suele estar relacionado con la idea de territorio, pero no siempre es así, en particular cuando se trata de temas relacionados con Internet debido a su naturaleza transfronteriza⁴⁵⁴.

Como se ha señalado anteriormente en *Internet & Jurisdiction Global Status Report 2019*:

A menudo se hace una distinción entre la jurisdicción personal y la jurisdicción en razón de la materia. La jurisdicción personal se refiere a la jurisdicción de un tribunal sobre una persona jurídica o física determinada. La jurisdicción en razón de la materia se refiere a la jurisdicción de un tribunal sobre el tipo de controversia en cuestión. Sin embargo, en litigios recientes se ha puesto de relieve un tercer tipo de cuestión jurisdiccional: el alcance de la jurisdicción. El alcance de la jurisdicción se refiere al ámbito geográfico de las órdenes dictadas por un tribunal que tiene jurisdicción personal y jurisdicción en razón de la materia.

Esta cuestión —que se superpone al derecho de los recursos— se ha planteado últimamente en los tribunales que dictan órdenes de carácter mundial de bloqueo, desreferenciación o eliminación de contenido. Las consideraciones sobre el alcance apropiado de la jurisdicción están intrínsecamente vinculadas a la solidez de la reclamación pertinente de jurisdicción personal, así como a la elección de la ley. Por ejemplo, cuando un tribunal tiene una reclamación relativamente débil de jurisdicción personal, puede no estar en condiciones de optar por un ámbito de jurisdicción más amplio. Un tribunal que opte por un ámbito de jurisdicción más amplio tampoco podrá aplicar solo su propia ley, dado el impacto que su decisión tendrá en el extranjero⁴⁵⁵.

⁴⁵¹ Véase [en línea] <https://www.icann.org/resources/en/glossary>.

⁴⁵² Véase [en línea] <https://www.w3.org/WWW>.

⁴⁵³ Véase [en línea] <https://www.icann.org/resources/en/glossary>.

⁴⁵⁴ Véanse más detalles en D. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford, Oxford University Press, 2017, págs. 14-25.

⁴⁵⁵ Internet & Jurisdiction Policy Network, *Internet & Jurisdiction Global Status Report 2019*, París, 2019 [en línea] <https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report>.

6. **Elección de la ley aplicable** es la capacidad de las partes contractuales de elegir la ley que regirá las eventuales controversias entre las partes y la interpretación del contrato. En el Informe se aborda este concepto al referirse a la cláusula de elección de ley que suele incluirse en las condiciones de servicio y directrices comunitarias de las plataformas internacionales de Internet. En este tipo de acuerdos en línea se suele cuestionar la autonomía de las partes en la elección de esta ley, ya que el usuario se enfrenta a condiciones contractuales predeterminadas unilateralmente.
7. **Cifrado (encryption)** es el proceso de codificar los datos para que solo puedan ser interpretados por los destinatarios previstos⁴⁵⁶. Se utiliza como una característica clave de seguridad y privacidad en varias aplicaciones de amplio uso, como el comercio electrónico, la banca por Internet, los mensajes instantáneos o las aplicaciones de videocomunicación.
8. **Cadena de bloques (blockchain)** es un registro de transacciones compartido entre las partes de una red, no controlado por una única autoridad central. La cadena de bloques funciona como un libro de registro ya que incluye y almacena todas las transacciones entre los usuarios en orden cronológico. En lugar de que una autoridad controle este libro (como el libro de cuentas de un banco), todos los usuarios de la red tienen una copia idéntica del libro llamada nodo⁴⁵⁷.
9. **Tecnología financiera, sector tecnofinanciero (fintech o FinTech)** se refiere a las entidades que se especializan en la prestación de servicios financieros principalmente a través de plataformas en línea habilitadas tecnológicamente⁴⁵⁸.
10. **Entornos de prueba regulatorios (regulatory sandboxes)** son espacios que se ofrecen a las empresas para que experimenten con el funcionamiento de productos o servicios innovadores de forma limitada con normas menos estrictas bajo la supervisión de una autoridad gubernamental reguladora⁴⁵⁹.
11. **Noticias falsas (fake news)** es un término que sirvió en la última década como calificativo políticamente sesgado para referirse a cualquier información falsa y engañosa, disfrazada y difundida como noticia⁴⁶⁰. El debate académico sobre un término más apropiado sigue en curso y los autores sugieren el uso de definiciones como “desinformación” o “información errónea”. En ese sentido, la desinformación puede definirse como información falsa que se crea o difunde deliberadamente con el propósito expreso de causar daño. Los productores de desinformación suelen tener motivaciones políticas, financieras, psicológicas o sociales. La información errónea, por otro lado, es información falsa, pero que no tiene la intención de causar daño. Por ejemplo, las personas que no saben que una información es falsa pueden difundirla en los medios sociales en un intento de ser útiles⁴⁶¹.
12. **Ultrafalso (deepfake)** es un término que se utiliza actualmente para describir las comunicaciones fabricadas con inteligencia artificial. El procesamiento de elementos de archivos de video o audio anteriores permiten la creación de un nuevo contenido en el que los individuos usan palabras y realizan acciones que no están basadas en la realidad⁴⁶². A medida que la tecnología evolucione, es probable que la información ultrafalsa se utilice cada vez más en campañas de desinformación⁴⁶³.

⁴⁵⁶ C. Wardel, “Information disorder: the essential glossary”, julio de 2018 [en línea] https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x25702.

⁴⁵⁷ Véase [en línea] <https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf>.

⁴⁵⁸ Véanse más detalles en W. Magnuson, “Regulating fintech”, *Vanderbilt Law Review*, vol. 71, N° 4, 2018.

⁴⁵⁹ D. Herrera y S. Vadillo, “Regulatory sandboxes in Latin America and the Caribbean for the fintech ecosystem and the financial system”, *Discussion Paper*, N° IDB-DP- 573, Banco Interamericano de Desarrollo (BID) [en línea] <https://publications.iadb.org/publications/english/document/Regulatory-Sandboxes-in-Latin-America-and-the-Caribbean-for-the-FinTech-Ecosystem-and-the-Financial-System.pdf>.

⁴⁶⁰ Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), *Periodismo, “noticias falsas” & desinformación*, París, 2020 [en línea] <https://unesdoc.unesco.org/ark:/48223/pf0000373349.locale=es>.

⁴⁶¹ Wardle, C. & H. Derakshan (27 de septiembre de 2017) *Information Disorder: Toward an interdisciplinary framework for research and policy making*, Consejo de Europa, <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>.

⁴⁶² Ibídem. Véanse más detalles en Y. Li, M. Chang y S. Lyu, “In ictu oculi: exposing AI generate fake videos by detecting eye blinking,” junio de 2018 [en línea] <https://arxiv.org/pdf/1806.02877.pdf>.

⁴⁶³ Véanse más detalles en R. Chesney y D. Citron, “Deepfakes: a looming crisis for national security, democracy and privacy?”, *Lawfare*, 21 de febrero de 2018 [en línea] <https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy>.

13. **Internet de las cosas (IoT)** es un sistema de dispositivos interrelacionados con la capacidad de reunir y transferir datos a través de una red sin necesidad de una interacción humana continua. En un escenario más complejo, la IoT puede definirse como una red autoconfigurable, adaptable y compleja que interconecta “cosas” a Internet mediante el uso de protocolos de comunicación estándar. Las cosas interconectadas tienen una representación física o virtual en el mundo digital, capacidad de detección/actuación, una característica de programabilidad y son identificables de manera única. La representación contiene información que incluye la identidad, la situación, la ubicación o cualquier otra información comercial, social o privada relevante de la cosa. Las cosas ofrecen servicios, con o sin intervención humana, mediante la explotación de la identificación única, la captura y comunicación de datos y la capacidad de actuación. El servicio se explota mediante el uso de interfaces inteligentes y se pone a disposición en cualquier lugar, en cualquier momento y para cualquier cosa teniendo en cuenta la seguridad⁴⁶⁴.

⁴⁶⁴ Véase https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf.

El informe *Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL): informe sobre la situación regional 2020* es el primer ejercicio integral de la región para mapear las diferentes tendencias de política relativas al carácter transfronterizo de Internet y la forma en que afecta a los diferentes interesados, como los gobiernos, las empresas y la sociedad civil.

¿De qué manera las diferentes normas nacionales y regionales pueden crear barreras que obstaculicen el comercio electrónico transfronterizo y la inversión en los mercados digitales? ¿Qué beneficios económicos y sociales podrían obtenerse mediante la armonización de los marcos regulatorios en toda la región? Una mejor comprensión de este escenario es un factor clave para fomentar la confianza de los inversionistas, promover la innovación y la diversificación económica, incrementar la confianza en el uso del comercio electrónico e impulsar un mercado de más de 600 millones de personas, creando oportunidades para las empresas y, en particular, para las pequeñas y medianas empresas.

A la inversa, la acción descoordinada de una amplia gama de agentes e iniciativas supone el riesgo de obstaculizar la digitalización de las economías, los gobiernos y las sociedades. A fin de ayudar a los encargados de la formulación de políticas a navegar por los desafíos que se avecinan, la Red de Políticas de Internet y Jurisdicción, en coordinación con la CEPAL, presenta esta publicación informe *Red de Políticas de Internet y Jurisdicción y Comisión Económica para América Latina y el Caribe (CEPAL): informe sobre la situación regional 2020*.