



CADERNOS CGI.br Referências

6.3

Internet & Jurisdição e CEPAL: Relatório de Status Regional 2020

Carlos Affonso de Souza



NAÇÕES UNIDAS

CEPAL



INTERNET &
JURISDICTION
POLICY NETWORK



german
cooperation
DEUTSCHE ZUSAMMENARBEIT

cgi.br

Comitê Gestor da
Internet no Brasil



United Nations publication
Copyright © United Nations, 2020
All rights reserved

Internet & Jurisdiction Policy Network publication
Copyright © Internet & Jurisdiction Policy Network, 2020.
All rights reserved



Esta tradução está publicada nos termos da licença Creative Commons Atribuição Não Comercial 4.0 Internacional <<https://creativecommons.org/licenses/by-nc/4.0/deed.pt-br>>

Edição em português publicada com autorização da Comissão Econômica para a América Latina e o Caribe e da Rede de Políticas Internet & Jurisdição. O conteúdo deste relatório é de responsabilidade dos autores envolvidos em sua produção.

Para mais informações, consultar:
<<https://www.cepal.org/>>
<<https://www.internetjurisdiction.net/>>

**Núcleo de Informação
e Coordenação do Ponto BR**



CADERNOS CGI.br Referências

**Internet & Jurisdição
e CEPAL: Relatório
de Status Regional 2020**

Carlos Affonso de Souza

Comitê Gestor da Internet no Brasil
Agosto 2023

Núcleo de Informação e Coordenação do Ponto BR

Diretor Presidente

Demi Getschko

Diretor de Assessoria às Atividades do CGI.br

Hartmut Richard Glaser

Diretor Administrativo

Ricardo Narchi

Diretor de Serviços e Tecnologia

Frederico Neves

Diretor de Projetos Especiais e de Desenvolvimento

Milton Kaoru Kashiwakura

Produção dos Cadernos CGI.br

Diretoria de Assessoria às Atividades do CGI.br

Coordenação Executiva e Editorial

Carlos Francisco Cecconi e Jean Carlos Ferreira dos Santos

Produção Editorial

Carolina Carvalho (Comunicação NIC.br)

Produção desta publicação

Tradução

Ana Zuleika Pinheiro Machado

Projeto Gráfico e Ilustrações

Pilar Velloso

Revisão da Tradução

Christian Perrone e Giovana Carneiro

Revisão Técnica e Preparação

Carlos Francisco Cecconi e Jean Carlos Ferreira dos Santos

Diagramação

Daniele Doneda

Fotos

Shutterstock

Título original

Internet & Jurisdiction and ECLAC Regional Status Report 2020.

Disponível em: <<https://www.internetjurisdiction.net/publications>>

Dados Internacionais de Catalogação na Publicação (CIP)

(Câmara Brasileira do Livro, SP, Brasil)

Souza, Carlos Affonso de

Internet & jurisdição e CEPAL [livro eletrônico] : relatório de status regional 2020 / Carlos Affonso de Souza ; [editor] Núcleo de Informação e Coordenação do Ponto BR ; [tradução Ana Zuleika Pinheiro Machado]. -- 1. ed. -- São Paulo, SP : Comitê Gestor da Internet no Brasil, 2023.

PDF

Título original: Internet & jurisdiction and ECLAC regional status report 2020.

Vários colaboradores. Bibliografia.

ISBN 978-65-86949-93-3

1. Ciberespaço 2. Direito e tecnologia 3. Governança da Internet 4. Internet - Leis e legislação 5. Transnacionalização 6. Regulação

I. Núcleo de Informação e Coordenação do Ponto BR. II. Título.

22-134014

CDD-004.6

Índices para catálogo sistemático:

1. Governança digital : Tecnologia da informação : Relatórios 004.6

Eliete Marques da Silva - Bibliotecária - CRB -8/9380

Esta publicação está disponível também em formato digital em: <<http://www.cgi.br>>

Comitê Gestor da Internet no Brasil (CGI.br)

Composição em Agosto 2023

Integrantes

Representantes do Setor Governamental

Carlos Manuel Baigorri
Cláudio Furtado
Débora Peres Menezes
José Roberto de Moraes Rêgo Jr
Luiz Felipe Gondin Ramos
Maximiliano Salvadori Martinhão
Pedro Helena Pontual Machado
Renata Mielli
Rogério Souza Mascarenhas

Representantes do Setor Empresarial

Henrique Faulhaber
José Alexandre Novaes Bicalho
Nivaldo Cleto
Rosauro Leandro Baretta

Representantes do Terceiro Setor

Bia Barbosa
Domingos Sávio Mota
Laura Conde Tresca
Percival Henriques de Souza Neto

Representantes da Comunidade Científica e Tecnológica

Marcos Dantas Loureiro
Rafael de Almeida Evangelista
Tanara Lauschner

Representante de notório saber em assuntos de Internet

Demi Getschko

Coordenadora

Renata Mielli

Secretário Executivo

Hartmut Richard Glaser

Apresentação

por CARLOS AFFONSO SOUZA

Professor da Faculdade de Direito da Universidade do Estado do Rio de Janeiro (UERJ) e Diretor do Instituto de Tecnologia e Sociedade (ITS Rio)

Quando se olha bem de perto, um mosaico é apenas a combinação de pequenas peças, como pedras, vidros ou azulejos. Cada uma delas, por sua vez, conta duas histórias. A primeira diz respeito à peça em si: a sua origem, cor e forma. Uma pedra de calcita branca e outra de basalto negro são o que são. Mas elas adquirem um segundo significado quando colocadas lado a lado, formando o desenho ondulado da calçada de Copacabana. Esse só se revela à distância.

Os mosaicos acompanham a história da humanidade. Eles estão na arte da Mesopotâmia e no revestimento das casas romanas, mas também nas máscaras astecas de pedra turquesa e na cúpula da basílica de Aparecida. Cada região, ao seu modo, compõe os seus mosaicos.

A Internet é uma rede global, que cria desafios e oportunidades que são tanto compartilhadas por todos os países, como também tratadas local e regionalmente de modo distintos. Nessa direção, a América Latina e o Caribe apresentam um mosaico de experiências regulatórias e de governança que ao mesmo tempo refletem transformações globais e particularizam o seu enfrentamento a partir da história e do contexto da região.

O *Relatório de Status Regional 2020* da Rede de Políticas Internet & Jurisdição e CEPAL, com foco na América Latina e no Caribe, procura apresentar esse mosaico, identificando as peças que o compõem - com a abordagem dos principais debates sobre regulação e governança da Internet na região - mas também apresentando o desenho que surge da junção desses elementos - com o apontamento de tendências gerais no debate sobre soluções jurídicas e técnicas.

A partir da experiência da Rede de Políticas Internet & Jurisdição (Internet & Jurisdiction Policy Network), e com o apoio da Comissão Econômica para a América Latina e o Caribe (CEPAL), o relatório apresenta as oportunidades encontradas na região para a construção de um mercado único digital, indicando as possibilidades de harmonização em temas de regulação e governança da rede.

A partir de cuidadosa pesquisa e de entrevistas com diversos atores, representando um conjunto multissetorial de perspectivas, o relatório procura apresentar um panorama de tendências regulatórias em diversos tópicos relacionados com o aspecto transfronteiriço da Internet, evidenciando seus impactos na forma de atuação de governos, empresas e entidades da sociedade civil na região.

Dentre as principais tendências observadas no estudo, podemos destacar a crescente inclusão digital como fator para o desenvolvimento econômico e para a inovação, levando-se em consideração os desafios existentes para levar conexão à Internet para mais pessoas em contextos de forte desigualdade socioeconômica.

Ao mesmo tempo, a crise sanitária desencadeada pela pandemia de COVID-19 acelerou os processos de digitalização, reforçando a relevância de temas como cibersegurança nas atividades desenvolvidas on-line. Na mesma velocidade, um cenário regulatório em constante transformação evidencia como soluções encontradas no exterior podem influenciar atores nacionais. O relatório indica, por exemplo, como a adoção na Europa de um regulamento geral sobre proteção de dados impulsionou o debate sobre o tema na região.

Nesse contexto surgem também visões sobre como compatibilizar noções de soberania nacional em uma rede global de dispositivos conectados, que permite o armazenamento e o tratamento remoto de dados. O relatório aponta como as discussões sobre soberania digital e territorialidade começam a ser enfrentadas na região.

Dessa forma, o relatório procura traduzir informações técnicas em pontos de atenção (e de ação) para os formuladores de políticas públicas, revelando as últimas tendências em tópicos-chave como o papel dos intermediários, privacidade, liberdade de expressão, inteligência artificial e Internet das Coisas. Todas

as peças de um mosaico de experiências que revela o potencial de originalidade e de adaptação da América Latina e do Caribe frente aos desafios e no encontro das oportunidades existentes em um contexto cada vez mais digital.

Gostaria de agradecer à equipe da Rede de Políticas Internet & Jurisdição pela produção deste relatório e pela confiança dedicada durante a sua elaboração. Agradeço à assessoria do Comitê Gestor da Internet no Brasil (CGI.br) pela iniciativa de traduzir o documento para o Português, ampliando assim o acesso ao seu conteúdo. De modo especial, gostaria de agradecer o apoio de Christian Perrone e de Giovana Carneiro, do Instituto de Tecnologia e Sociedade (ITS Rio), sem os quais esse trabalho não teria sido possível.

Este Relatório foi encomendado pelo Secretariado da Rede de Políticas Internet & Jurisdição (I&JPN) e pela Comissão Econômica para a América Latina e o Caribe das Nações Unidas (CEPAL), e é de autoria de Carlos Affonso de Souza. O Relatório representa os melhores esforços do autor para mapear o ecossistema atual e as tendências na América Latina e no Caribe, com base em pesquisas documentais e entrevistas com atores. No entanto, a exaustividade das informações não pode ser garantida, uma vez que este Relatório constitui a primeira linha de referência regional sobre jurisdição e Internet.

A CEPAL e o Secretariado da I&JPN agradecem o apoio financeiro e institucional da Agência Alemã para Cooperação Internacional (GIZ), agindo em nome do Ministério Federal Alemão de Cooperação Econômica e Desenvolvimento (BMZ), que permitiu a elaboração do Relatório.

As opiniões expressas neste documento são dos autores e não refletem necessariamente as opiniões do Secretariado da I&JPN, da CEPAL, dos atores envolvidos com os trabalhos da I&JPN ou daqueles que forneceram apoio financeiro à execução do Relatório.

Publicação das Nações Unidas
LC/TS.2020/141 / Distribuição: L
Direitos autorais © Nações Unidas
Todos os direitos reservados
Impresso nas Nações Unidas,
Santiago S.19-01092

Internet & Jurisdiction Policy
Network publication
Copyright © Internet & Jurisdiction Policy Network, 2020
Todos os direitos reservados.

Esta publicação deve ser citada como: Souza, Carlos Affonso de. *Internet & Jurisdição e CEPAL: relatório de status regional 2020*. São Paulo: Comitê Gestor da Internet no Brasil, 2023.

Os pedidos de autorização para reprodução total ou parcial deste trabalho devem ser enviados à Comissão Econômica para a América Latina e o Caribe (CEPAL), Divisão de Publicações e Serviços Web, <publicaciones.cepal@un.org>, e Internet & Jurisdiction Policy Network (I&JPN), <report@internetjurisdiction.net>. Qualquer entidade interessada na reprodução deve mencionar a fonte e a informar a CEPAL e I&JPN sobre tal reprodução. Os Estados-membros e suas instituições governamentais podem reproduzir este trabalho sem autorização prévia, mas devem mencionar a fonte e informar a CEPAL sobre tal reprodução.*

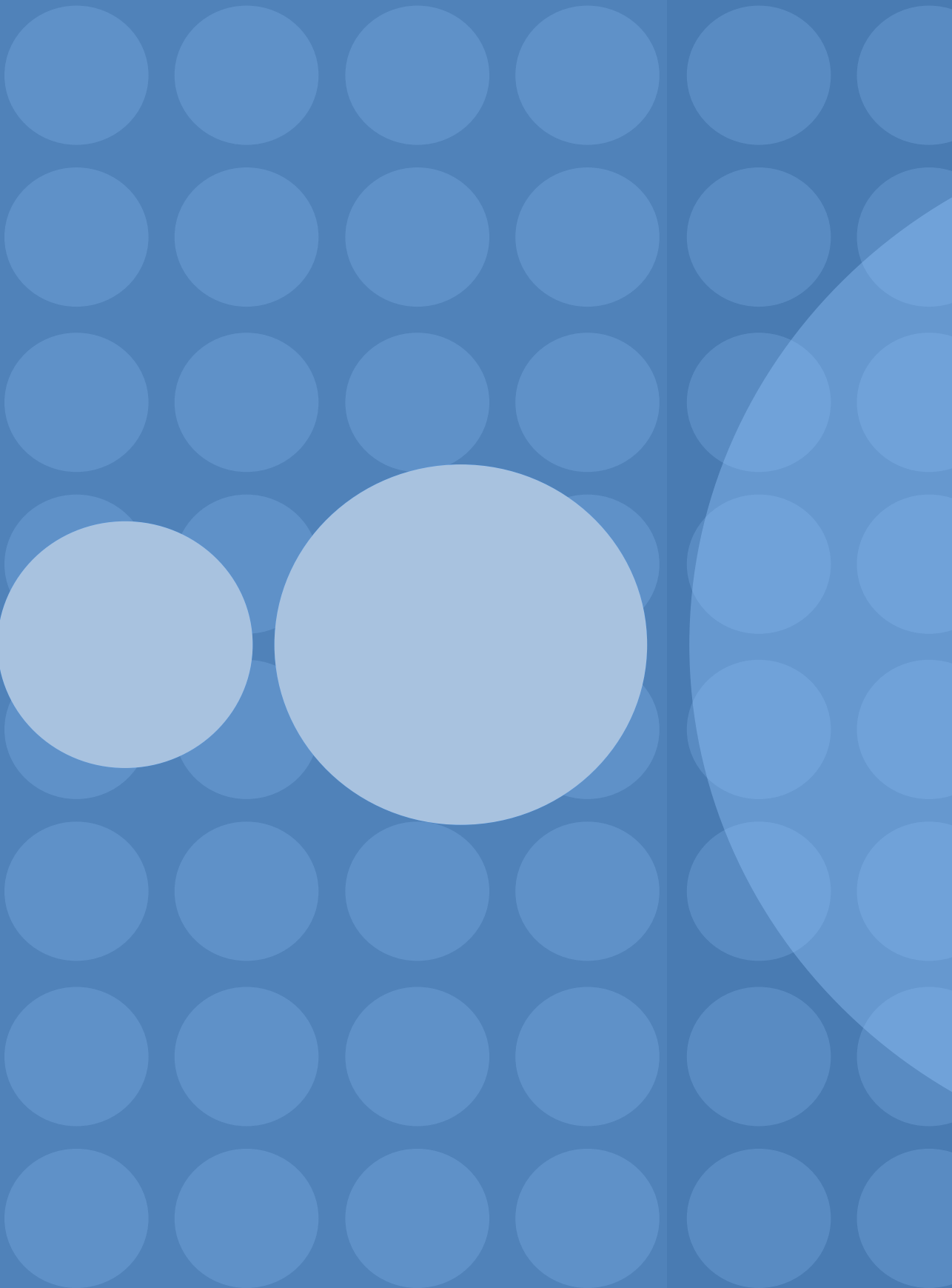
* A tradução e a publicação deste relatório foram autorizadas pela CEPAL e I&JPN por meio de acordo firmado com o Núcleo de Informação e Coordenação do Ponto BR.

Sumário

18	AGRADECIMENTOS
25	PREFÁCIO
29	APRESENTAÇÃO
33	MÉTODO
38	SUMÁRIO EXECUTIVO
50	INTRODUÇÃO
68	1. TENDÊNCIAS GERAIS
70	A. O aumento da conectividade é necessário, mas pode reforçar as desigualdades socioeconômicas
75	B. Um cenário tecnológico em mudança
75	1. Mudanças nas percepções: da euforia tecnológica ao <i>techlash</i>
76	2. O transnacionalismo é uma nova dinâmica emergente
77	3. Multinacionais estrangeiras são influentes na região
79	4. O ambiente de negócios para <i>start-ups</i> na região é variável
82	C. Iniciativas regulatórias estrangeiras estão inspirando propostas regionais e nacionais
84	1. As iniciativas de políticas têm proliferado à medida que aumenta o apetite para regular o ciberespaço
86	2. Inspiração legislativa e judicial: fertilização cruzada ou imitação?
86	D. Preocupações com a influência internacional e pluralidade normativa
87	1. As regras são definidas para (e por) atores internacionais grandes e bem estabelecidos
88	2. O papel crescente das normas da empresa: o status “constitucional” dos termos de serviço
91	E. O papel da territorialidade e o exercício da soberania são diferentes em uma rede global
94	1. O crescente alcance extraterritorial das leis nacionais
95	2. Extraterritorialidade traz desafios de execução
96	F. Espera-se que os intermediários desempenhem novos papéis
97	1. Uma responsabilidade cada vez maior está sendo colocada sobre os operadores privados
98	2. Os intermediários são cada vez mais solicitados a fornecer dados para apoiar investigações

- 99 3. A transparência é essencial para aumentar a confiança, mas a implementação varia
 - 102 4. Crescente atenção tem sido dada ao devido processo nas atividades de moderação de conteúdo
- 104 2. PRINCIPAIS TENDÊNCIAS DA ATUALIDADE NA AMÉRICA LATINA E NO CARIBE**
- 106 A. Expressão**
- 106 1. *Fake news* e desinformação
 - 111 2. Difamação
 - 115 3. Bullying on-line
 - 117 4. Distribuição não consensual de mídia sexualmente explícita
 - 122 5. O “direito ao esquecimento” se depara com as características particulares da região
- 126 B. Segurança**
- 126 1. É necessária maior coordenação de cibersegurança para lidar com incidentes generalizados na região
 - 127 2. Investigações transfronteiriças e provas eletrônicas
 - 136 3. Vigilância
 - 145 4. Segurança cibernética
- 152 C. Economia**
- 152 1. Comércio eletrônico: a aspiração a um mercado único digital
 - 165 2. Propriedade intelectual
 - 171 3. A Internet das Coisas (IoT)
 - 183 4. Meios de pagamento digitais
 - 191 5. *Blockchain* e criptomoedas
 - 195 6. Fluxos internacionais e regionais de dados: regimes de proteção de dados
 - 200 7. Fluxos transfronteiriços de dados internacionais e regionais
- 207 3. PRINCIPAIS ABORDAGENS PARA OS DILEMAS TRANSFRONTEIRIÇOS DA INTERNET NA AMÉRICA LATINA E NO CARIBE**
- 208 A. Principais tendências jurídicas**
- 209 1. Os Estados estão cada vez mais recorrendo a uma “doutrina dos efeitos” na afirmação de sua jurisdição
 - 213 2. A expansão do alcance jurisdicional
 - 219 3. Ordens judiciais de retirada (*take-down*), manutenção [da retirada] (*stay-down*) e permanência [de conteúdo] (*stay-up*)

	223	4. Multas e sanções
	225	5. Os termos de serviço estão interligados com as leis nacionais
228	B. Principais abordagens técnicas	
	230	1. Tecnologias de geolocalização
	233	2. A filtragem de conteúdo está crescendo à medida que os países combatem discurso de ódio e desinformação
	236	3. O Sistema de Nomes de Domínio: suspensões e bloqueios resultantes de notificações e ordens judiciais ou administrativas
	238	4. Bloqueio de sites e aplicativos
	241	5. Paralisações de serviço
	244	6. Localização forçada de dados
250	GLOSSÁRIO	



Agradecimentos

Este Relatório foi encomendado pelo Secretariado da Rede de Políticas Internet & Jurisdição (I&JPN) e pela Comissão Econômica para a América Latina e o Caribe das Nações Unidas (CEPAL).

A produção deste Relatório foi possível graças ao apoio financeiro fornecido pela Agência Alemã de Cooperação Internacional (GIZ), agindo em nome do Ministério Federal Alemão de Cooperação Econômica e Desenvolvimento (BMZ), e pela CEPAL.

Equipe de autoria:

Autor:

Professor Carlos Affonso de Souza
Universidade do Estado do Rio de Janeiro
(UERJ)
Diretor
Instituto de Tecnologia e Sociedade
(ITS Rio)

Assistência à pesquisa:

Christian Perrone
Doutorando
Pesquisador Sênior
Instituto de Tecnologia e Sociedade
(ITS Rio)

Giovana Carneiro
Pesquisadora Júnior
Instituto de Tecnologia e Sociedade
(ITS Rio)

Coordenação do projeto (I&JPN):

Martin Hullin
Diretor de Operações e Parcerias de
Conhecimento
Secretariado da Rede de Políticas
Internet e Jurisdição

Equipe do projeto:

Bertrand de la Chapelle
Diretor Executivo
Secretariado da Rede de Políticas
Internet e Jurisdição

Paul Fehlinger
Diretor-Executivo Adjunto
Secretariado da Rede de Políticas
Internet e Jurisdição

Equipe do Projeto (CEPAL):

Edwin Fernando Rojas
Divisão da Comissão Econômica de
Produção, Produtividade e Gestão
Comissão Econômica para a América
Latina e o Caribe

Alexis Arancibia
Consultor
Comissão Econômica para a América
Latina e o Caribe

Alonso Zuniga Irigoín
Consultor
Comissão Econômica para a América
Latina e o Caribe

Produção:

Comissão Econômica para a América
Latina e o Caribe
Secretariado da Rede de Políticas
Internet e Jurisdição

Edição:

Sophie Tomlinson
Gerente, Comunicações e Divulgação
Secretariado da Rede de Políticas
Internet e Jurisdição

Design e layout do relatório original:

Comissão Econômica para a América
Latina e o Caribe

Agradecemos imensamente o tempo e a contribuição de todos os participantes e entrevistados. Sem os seus valiosos conhecimentos, este Relatório não poderia ter sido produzido.

Mauricio Agudelo

Coordenador da Agenda Digital do Banco de Desenvolvimento da América Latina (CAF)
Colômbia

Pablo Bello

Diretor para Políticas de Mensagens Privadas, LATAM
Facebook
Brasil

Daniel Cavalcanti

Coordenador
Ministério da Ciência, Tecnologia, Inovações e Comunicações
Secretaria de Governo Digital
Brasil

María Angélica Chinchilla Medina

Diretora de Telecomunicações Evolução e Mercado
Ministério da Ciência, Tecnologia e Telecomunicações (MICITT)
Costa Rica

José Clastornik

Presidente da Fundação para a Inovação Digital do Uruguai
Ex-Diretor Executivo da Agência de Governo Eletrônico e Sociedade da Informação e do Conhecimento (AGESIC)
Uruguai

Pelayo Covarrubias

Presidente
Fundação País Digital
Chile

Agustina del Campo

Diretor
Centro de Estudos sobre Liberdade de Expressão e Acesso à Informação (CELE)
Argentina

César Díaz

Engenheiro
Uruguai

Lester García

Diretor para Políticas de Conectividade LATAM
Facebook
México

Raúl Echeberría

Diretor Executivo
Associação Latino-americana de Internet (ALAI)
Uruguai

Alexandre Fernandes Barbosa

Diretor
Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (CETIC.br)
Núcleo de Informação e Coordenação do Ponto BR (NIC.br)
Brasil

Matías Fernández Díaz

Gerente Sênior (Assuntos Públicos)
Mercado Libre Argentina

Gustavo Gómez

Diretor Executivo do Observatório Latino-Americano de Regulamentação, Mídia e Convergência (OBSERVACOM)
Uruguai

José Juan Haro

Diretor para Atacado e Assuntos Públicos
Telefónica
Espanha

Héctor Huici

Ex-Secretário
Secretaria de Tecnologias da Informação e Comunicação
Argentina

Erick Iriarte

Sócio
Iriarte & Asociados (IALaw)
Peru

Juan Jung

Ex-coordenador
Centro de Pesquisa de Telecomunicações da América Latina (cet.la)
Uruguai

Yacine Khelladi

Coordenador Regional, América Latina e Caribe
Alliance for Affordable Internet (A4AI)
República Dominicana

Juan Carlos Lara

Diretor de Conteúdo
Derechos Digitales
Chile

Carolina Limbatto

Diretora para as Américas
Cullen International
Bélgica

Omar de León Boccia

Diretor Executivo
Teleconsult
Uruguai

Lilia Liu

Diretor Executivo
Lilia Liu & Associates (LLASO)
Panamá

Maryleana Méndez

Secretária-Geral
Associação Interamericana de Empresas de Telecomunicações (ASJET)
Uruguai

Oscar Messano

Presidente
Centro de Treinamento de Alta Tecnologia para a América Latina e o Caribe (CCATLAT)
Argentina

César Moliné Rodríguez

Diretor de Segurança Cibernética,
Comércio Eletrônico e Assinatura
Digital
Instituto Dominicano de
Telecomunicações (INDOTEL)
República Dominicana

Gonzalo Navarro

Diretor Executivo
Latin American Internet Association
(ALAI)
Uruguai

Rodrigo de la Parra

Vice-Presidente, Engajamento das
Partes Interessadas e Diretor-Geral
- América Latina e Caribe
Internet Corporation for Assigned
Names and Numbers (ICANN)
México

Sissi de la Peña

Gerente para Comércio Digital e
Organizações Internacionais
Associação Latino-Americana de
Internet (ALAI)
México

Eric Ramírez

Diretor
Secretaria de Inovação, Governo de
El Salvador
El Salvador

Rodrigo Ramírez Pino

Presidente
Câmara Chilena de Infraestrutura
Digital (IDICAM)
Chile

María Eunises Rivas Robleto

Secretária Executiva do Conselho
Nicaraguense de Ciência e
Tecnologia (CONICYT)
Nicarágua

Beatriz Rodríguez

Presidente
Internet Society - Capítulo do
Uruguai (ISOCUY)
Uruguai

Jorge Romo

Escritório Nacional de Coordenação
de Estratégia Digital (CEDN)
Gabinete do Presidente da
República
México

Eduardo Salido

Gerente para Assuntos Públicos e
Políticas para a América Latina
Telefónica
Espanha

Andrés Sastre

Diretor Regional da Associação
Interamericana de Empresas de
Telecomunicações do Cone Sul
(ASJET)
Uruguai

Thiago Luís Sombra

Sócio
Mattos Filho, Veiga Filho, Marrey Jr.
e Quiroga Advogados
Brasil

Paloma Szerman

Gerente Sênior de Políticas
Regulatórias
GSMA América Latina
Argentina

**Fernanda Teixeira Souza
Domingos**

Procuradora Federal
Ministério Público Federal
Brasil

Berioska Torres

Subsecretária
Escritório do Subsecretário da
Sociedade da Informação e do
Ministério das Telecomunicações
e da Sociedade da Informação
(MINTEL)
Equador

Paloma Villa Mateos

Gerente de Políticas Públicas
Telefónica
Espanha

Juan Manuel Wilches Durán

Consultor de Telecomunicações e
Transformação Digital
Colômbia

Cristina Zubillaga

Consultora Sênior
Ex-Diretora Executiva Adjunta da
Agência de Governo Eletrônico
e Sociedade da Informação e do
Conhecimento (AGESIC)
Uruguai

Prefácio

por ALICIA BÁRCENA

Secretária Executiva da Comissão Econômica para a América Latina e o Caribe (CEPAL)

A medida que a América Latina e o Caribe enfrentam a mais grave crise de saúde e humanitária em um século, restam descobertas as desigualdades que permeiam a região. Assim como a pandemia do coronavírus (COVID-19) revelou as consequências de um acesso desigual aos cuidados de saúde, a um sistema de educação de alta qualidade e a oportunidades econômicas, a acentuada desigualdade digital também se tornou mais evidente. Mais de 60% dos indivíduos da região possuem uma conexão à Internet; entretanto, existem marcadas desigualdades na conectividade em razão da renda, a área ser rural ou urbanas, por origem étnica, entre outros fatores. Em alguns países, a lacuna de conectividade entre as parcelas mais ricas e mais pobres chega a atingir 60 pontos percentuais. Para superar a crise e voltar a progredir, é essencial que sejam tomadas medidas para avançar em direção à conectividade universal e proporcionar melhor acesso às ferramentas digitais. Isso só será possível com quadros normativos fortes.

A pandemia da COVID-19 amplifica a necessidade de maior coordenação para garantir a coerência política entre os países da região em questões como transferências transfronteiriças de dados, harmonização regulatória, privacidade e segurança de dados. A implantação de tecnologias que exigem a rápida transferência de grandes quantidades de novos dados entre numerosos atores para controlar a disseminação da COVID-19 exige normas comuns e interoperabilidade jurídica. A crescente importância do trabalho remoto e das iniciativas de ensino a distância exige soluções de conectividade seguras para garantir que ninguém seja deixado para trás.

Na qualidade de Secretaria Técnica da Conferência Ministerial sobre a Sociedade da Informação na América Latina e no Caribe, a Comissão Econômica para a América Latina e o Caribe (CEPAL), há mais de 15 anos, vem trabalhando em conjunto com atores do governo e observadores representantes do meio acadêmico, da indústria, da comunidade técnica e de organizações multilaterais para preparar uma agenda digital regional, priorizando questões relacionadas ao desenvolvimento digital da nossa região. À medida que desenvolvemos a agenda digital 2020-2022 para a América Latina e o Caribe (eLAC2022), uma das iniciativas mais prioritárias é a criação de um mercado digital regional. O mercado digital regional busca fortalecer a integração digital da América Latina e do Caribe, aproveitando a proximidade geográfica e os interesses similares dos países da região.

Este Relatório pioneiro é o primeiro mapeamento abrangente de seu tipo na América Latina e no Caribe e fornece uma sólida base de evidências que apoiará o desenvolvimento da eLAC2022. O Relatório identifica e aborda as principais tendências no campo da política digital regional em rápido crescimento e traça o caminho a ser seguido. Esta contribuição é vital para o debate político e lançará luz sobre alguns dos desafios e oportunidades que podemos aproveitar para nos aproximar de um mercado digital regional mais integrado e harmonizado.

Apresentação

por BERTRAND DE LA CHAPELLE

Diretor Executivo

PAUL FEHLINGER

Diretor Executivo Adjunto

Secretariado da Rede de Políticas Internet & Jurisdição

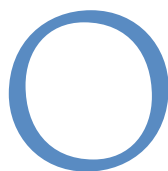
A transformação digital de economias, governos e sociedades na América Latina e no Caribe está se acelerando marcadamente em 2020, ainda mais catalisada pela pandemia de COVID-19. Com o crescimento dos serviços transfronteiriços e dos fluxos de dados, aumenta a necessidade de uma maior coordenação e interoperabilidade jurídica. A ação descoordenada de uma ampla gama de atores e iniciativas põe em risco o processo de digitalização. Para fornecer um mapeamento e análises indispensáveis do ecossistema regional na América Latina e no Caribe, a Rede de Políticas Internet & Jurisdição, em coordenação com a Comissão Econômica das Nações Unidas para a América Latina e o Caribe (CEPAL), criou este primeiro *Internet & Jurisdição e CEPAL: Relatório de Status Regional 2020*. Trata-se de uma edição regional do inovador *Internet & Jurisdição: Relatório de Status Global 2019*. O Relatório baseia-se na metodologia única da Rede de Políticas Internet & Jurisdição para compartilhar o conhecimento dos principais atores regionais de estados, empresas, operadores técnicos, organizações internacionais, academia e sociedade civil, por meio de entrevistas e pesquisas, e fazer com que suas vozes sejam ouvidas.

Uma mensagem fundamental do *Relatório de Status Regional 2020* é a necessidade de maior coerência política para a construção de um ecossistema digital regional próspero e integrado. Ao elaborar as principais tendências referentes aos desafios jurídicos no continente, o Relatório visa permitir que tomadores de decisões e formuladores de políticas aprofundem sua compreensão

sobre uma infinidade de acontecimentos em ritmo acelerado, a fim de possibilitar a inovação política baseada em evidências e promover a interoperabilidade jurídica no ciberespaço. Ao unir os campos da economia digital, segurança e direitos humanos, o Relatório lança luz sobre a mudança do cenário tecnológico e regulatório na região. Ele fornece a visão mais atualizada da pluralidade das iniciativas de política nacional e privada, bem como a jurisprudência que estabelece as regras para interações on-line, serviços digitais e fluxos de dados. O Relatório revela as últimas tendências sobre os principais tópicos, desde *start-ups*, inteligência artificial, Internet das Coisas, expressão e privacidade até o papel de intermediários. Além disso, mostra a extensão geográfica e o impacto das medidas nacionais da região, bem como a influência de medidas regulatórias públicas e privadas externos à região.

Este importante mapeamento para formuladores de políticas e tomadores de decisão foi realizado graças à forte parceria entre a Rede de Políticas Internet & Jurisdição e a CEPAL no âmbito do Memorando de Entendimento, assinado em 2019 com duração de cinco anos. O *Relatório de Status Regional 2020* é um marco importante nos esforços da Rede de Políticas Internet & Jurisdição para mapear o ecossistema jurídico transfronteiriço global, com o objetivo de ajudar no desenvolvimento de melhores políticas e soluções. Esperamos, portanto, que ele possa contribuir para fomentar a coordenação dos desafios jurídicos transfronteiriços e da cooperação digital na América Latina e no Caribe e além.

Método



O método escolhido para preparar este Relatório responde à necessidade de chegar a uma compreensão abrangente de um ecossistema altamente complexo e dinâmico, que compreende múltiplos atores, iniciativas e tendências em todos os espaços de políticas da economia digital, direitos humanos e segurança.

Isso levou à adoção de um desenho de pesquisa qualitativo e flexível que permitiu que as perguntas da pesquisa fossem exploradas em profundidade. Usando o método de pesquisa multifacetado adotado pela primeira vez para a produção do pioneiro *Relatório de Status Global 2019*, o presente relatório foi capaz de incorporar um processo sem precedentes e inovador de contribuição colaborativa e revisão em larga escala na Região da América Latina e do Caribe.

Este processo alavancou a experiência combinada dos principais atores envolvidos na Rede de Políticas Internet & Jurisdição, CEPAL e além, através de entrevistas semiestruturadas, avaliação de revisão por pares e procedimentos de coleta de dados, combinados com pesquisa documental detalhada e extensa.

Pesquisa documental

A pesquisa documental empregou métodos convencionais de pesquisa jurídica e consistiu principalmente em um estudo abrangente e análise da jurisprudência relevante, legislação e outras iniciativas regulatórias, e da literatura, incluindo livros, artigos de periódicos, artigos publicados em conferência e da indústria. Isso foi complementado com um estudo detalhado de diversos e valiosos relatórios e outros materiais de diferentes órgãos, nos últimos anos.

A pesquisa documental se beneficiou muito das publicações produzidas pela CEPAL e pela Rede de Políticas Internet & Jurisdição, e da ampla coleção de material relevante disponível na base de dados retrospectiva da Rede (I&J Retrospect Database). Esta base de dados de acesso aberto é o principal recurso

de informação da Rede de Políticas Internet & Jurisdição, documentando a evolução de políticas públicas, decisões judiciais, acordos internacionais e outros materiais que refletem tensões jurisdicionais em matéria de Internet transfronteiriça. Esta importante coleção forneceu informações atualizadas sobre as principais tendências, atitudes, progressos e iniciativas atuais. O material da base de dados retrospectiva também forneceu percepções importantes sobre abordagens legais e técnicas atuais para soluções, bem como sobre o que esse Relatório chama de “tendências abrangentes”.

Pesquisa aos atores

O primeiro método para obtenção de informações dos atores foi a utilização de um questionário on-line composto por 15 perguntas sobre uma variedade de tópicos relevantes para a pesquisa. Ao considerar a melhor forma de coletar dados para informar as questões da pesquisa, tomou-se muito cuidado para projetar perguntas que pudessem ser respondidas por qualquer um dos atores relevantes. Isso garantiu que todos os participantes da pesquisa fossem expostos ao mesmo conjunto de perguntas. O Secretariado da Rede de Políticas Internet & Jurisdição e a CEPAL identificaram participantes da pesquisa que representam todos os grupos de atores da I&JPN, nomeadamente academia, sociedade civil, governos, organizações internacionais, plataformas de Internet e comunidade técnica; os participantes foram selecionados especificamente para garantir a diversidade na região da América Latina e Caribe. Além disso, a seleção dos participantes da pesquisa foi proposital, na medida em que eles foram especificamente selecionados com base em sua expertise e conhecimentos. No total, os dados foram recebidos de mais de 40 participantes da pesquisa durante um período compreendido entre o quarto trimestre de 2019 e o segundo trimestre de 2020. Os participantes forneceram seus pontos de vista em caráter pessoal e não como representantes de qualquer organização específica e todas as contribuições para as pesquisas foram usadas sem atribuição. A contribuição de especialistas obtida com a pesquisa foi inestimável. Além de chamar a atenção para as principais tendências atuais, abordagens para soluções, metatendências abrangentes e preocupações geralmente mantidas no ecossistema, os resultados da pesquisa ajudaram a fornecer contexto

e uma compreensão diferenciada dos ambientes operacionais enfrentados pela sociedade civil, governos, organizações internacionais, plataformas de internet e a comunidade técnica. Os resultados da pesquisa são utilizados em todo o Relatório para mostrar, em números, as preocupações e atitudes do ecossistema dos atores pesquisados. Além disso, as observações dos atores foram utilizadas para destacar argumentos, observações e preocupações particularmente importantes.

Entrevistas com os atores

Entrevistas semiestruturadas foram realizadas em uma ampla gama de atores para complementar as percepções obtidas com as respostas ao questionário e a pesquisa documental. Como nas pesquisas com o questionário, tomou-se grande cuidado para garantir a inclusão e diversidade, com um leque geograficamente diversificado de atores, representando academia, sociedade civil, governos, organizações internacionais, plataformas de Internet e comunidade técnica. Esses atores foram identificados dentro e fora da Rede de Políticas Internet & Jurisdição e da CEPAL.

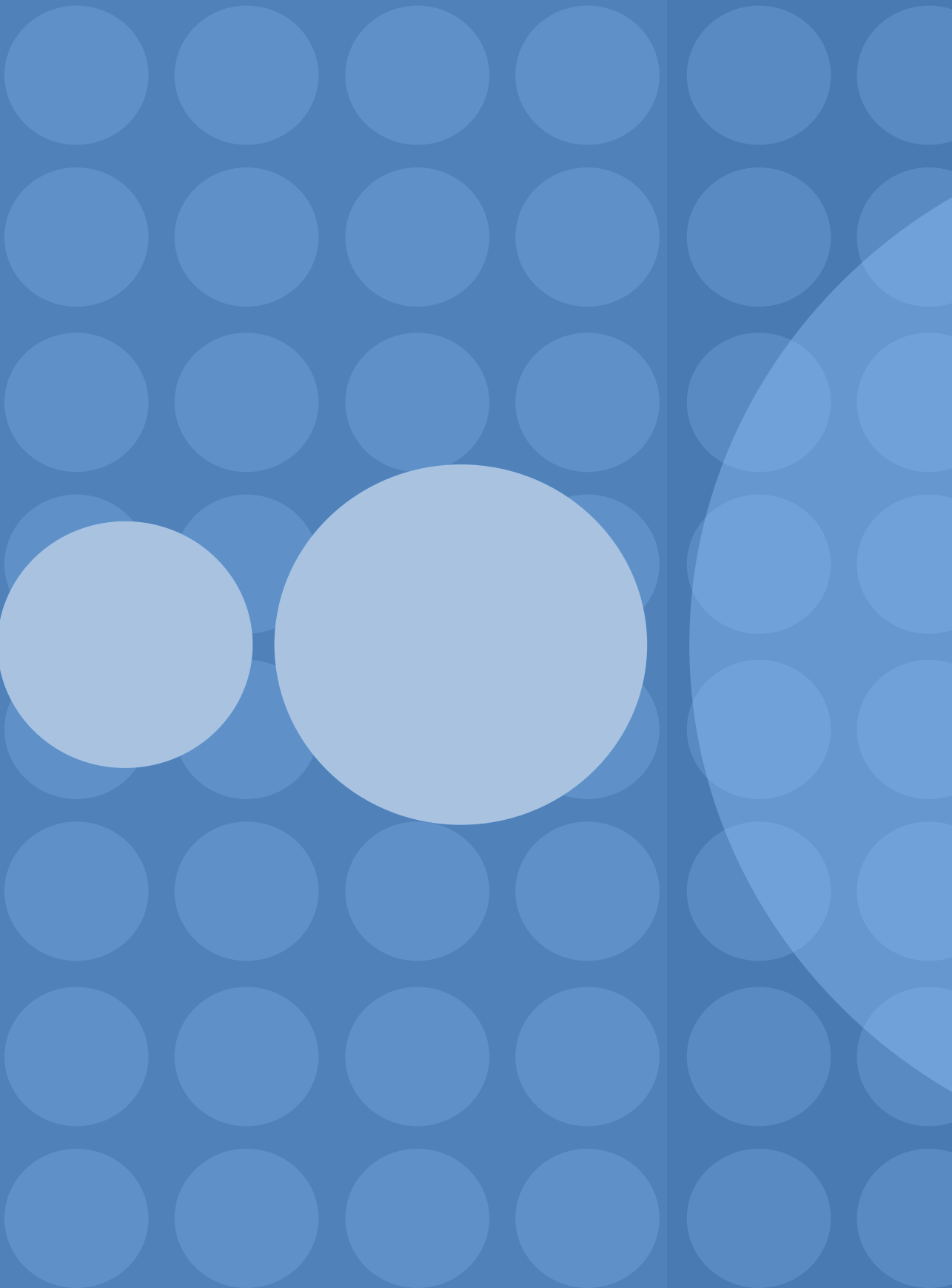
Cada entrevista durou, em média, mais de 30 minutos. As entrevistas foram realizadas em confiança e não foram gravadas. Notas detalhadas foram agrupadas, no entanto, e as observações foram documentadas de forma estruturada, facilitando referências cruzadas e análises detalhadas. As entrevistas semiestruturadas permitiram uma flexibilidade considerável e responder a perguntas suplementares com base em discussões com o entrevistado. Combinado com a garantia de confidencialidade, isso proporcionou um ambiente no qual os atores entrevistados puderam destacar assuntos que eram importantes para eles dentro dos tópicos gerais discutidos. Em muitos casos, os entrevistados também poderiam fornecer perspectivas, percepções e informações que, de outra forma, não seriam acessíveis aos pesquisadores. Dessa forma, parte do objetivo das entrevistas foi reduzir lacunas regionais e temáticas da pesquisa documental. No total, foram realizadas mais de 30 entrevistas, conduzidas do quarto trimestre de 2019 ao segundo trimestre de 2020. Como na pesquisa com questionário, os participantes forneceram seus pontos de vista em caráter pessoal e não como representantes de qualquer organização específica e todas as contribuições para as pesquisas foram usadas sem atribuição. Assim como os

comentários suscitados por meio da pesquisa com questionário, os comentários feitos pelos atores entrevistados foram vitais e utilizados ao longo do relatório para destacar argumentos, observações e preocupações particularmente importantes.

Limitações do estudo

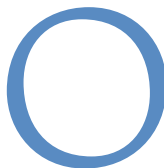
Um estudo de pesquisa desta natureza traz certas limitações. Em primeiro lugar, o escopo do Relatório é definido pelo mandato da Rede de Políticas Internet & Jurisdição e da CEPAL. Assim, não se trata de um relatório de status regional sobre a Internet em geral, mas centra-se especificamente em questões jurídicas transfronteiriças relacionadas com a Internet. Em segundo lugar, apesar das etapas descritas acima, é provável que haja lacunas. A relevância estatística da pesquisa exploratória, que se baseou em parte em um número limitado de participantes da pesquisa com questionário e de atores entrevistados, não deve ser superestimada. Além disso, a maioria das pesquisas documentais pode envolver vieses difíceis de eliminar inteiramente, independente de quaisquer esforços feitos com esse propósito.

À luz do acima exposto, este Relatório representa os melhores esforços dos compiladores para produzir uma visão geral ampla e abrangente, além de documentação das tendências passadas, atuais e emergentes dos atores relevantes e propostas de soluções para os principais desafios transfronteiriços das políticas legais que a nossa sociedade conectada enfrenta a partir de 1º de junho de 2020. Portanto, trata-se de um retrato oportuno do ambiente de políticas públicas e fornece uma primeira referência regional para futuros estudos na região da América Latina e Caribe.





Sumário Executivo



Relatório de Status Regional 2020 da Rede de Políticas Internet & Jurisdição e CEPAL é o primeiro exercício abrangente da América Latina e do Caribe de mapeamento das diferentes tendências políticas relacionadas à natureza transfronteiriça da Internet e a forma como isso afeta diferentes atores, como governos, empresas e sociedade civil.

Como as diferentes regulações regionais e nacionais podem criar barreiras ao comércio eletrônico transfronteiriço e ao investimento nos mercados digitais? Que benefícios econômicos e sociais podem ser alcançados através da harmonização das estruturas legais em toda a região? A melhor compreensão dessa situação é vital para os esforços com o intuito de fomentar a confiança dos investidores, promover a inovação e a diversificação econômica, criar maior confiança no comércio eletrônico e impulsionar um mercado de mais de 600 milhões de pessoas, enquanto abre uma série de oportunidades para os negócios, mais particularmente para as pequenas e médias empresas.

Ao mesmo tempo, a ação descoordenada de uma ampla gama de atores e iniciativas arrisca dificultar a digitalização de economias, governos e sociedades. É para ajudar os tomadores de decisões a enfrentarem os desafios que a Rede de Políticas Internet & Jurisdição, em coordenação com a Comissão Econômica para a América Latina e o Caribe (CEPAL), apresenta este Relatório.

O Relatório tem como objetivo: (i) mapear e consolidar informações relevantes para a América Latina e o Caribe e o mercado digital regional; (ii) criar e fortalecer redes regionais de colaboradores; e (iii) desenvolver capacitação sobre temas jurídicos transfronteiriços associados à transformação digital.

Em pesquisas e entrevistas realizadas para o Relatório com principais especialistas da região, 78% dos entrevistados concordaram que os desafios jurídicos transfronteiriços relacionados à Internet se tornarão cada vez mais acentuados nos próximos três anos. Ao mesmo tempo, 73,17% dos atores entrevistados concordaram ou concordaram fortemente que a coordenação era necessária para enfrentar os desafios jurídicos transfronteiriços, enquanto 60,98% consideravam que ainda não existem as instituições necessárias para enfrentar esses desafios.

INFOGRÁFICO 1

Os desafios jurídicos transfronteiriços na Internet se tornarão cada vez mais graves nos próximos três anos?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

Em um esforço para analisar tendências que são exclusivas da região, o Relatório investiga como um cenário tecnológico em câmbio está fortalecendo a ideia de atividades transnacionais como uma nova dinâmica emergente que não envolve apenas grandes empresas multinacionais, mas também está preparando o terreno para que as *start-ups* regionais cresçam rapidamente.

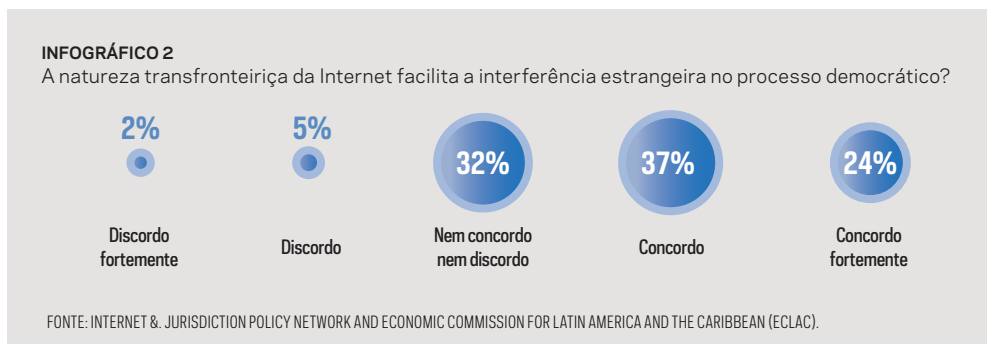
O Relatório identifica como as estruturas regulatórias regionais e nacionais podem ser inspiradas por iniciativas estrangeiras, especialmente aquelas que surgem nos Estados Unidos e na União Europeia. Esse é o caso do Regulamento Geral de Proteção de Dados da União Europeia (GDPR, na sigla em inglês), que provocou uma série de mudanças legislativas na América Latina e no Caribe. Há espaço para fertilização cruzada ou trata-se de mera transplantação?

Como as grandes empresas de Internet tentam se adaptar às expectativas cambiantes dos governos e do público em geral, envolvendo demandas crescentes por maior responsabilidade, a pluralidade de normas predispõe a região a conflitos jurisdicionais, testando os limites da aplicabilidade e o alcance das leis nacionais.

Este Relatório organiza as principais tendências atuais na América Latina e no Caribe em três grupos: expressão, segurança e economia. Não faltam tendências que são exclusivas da região, embora outras também estejam presentes em escala global.

Uma das tendências mais urgentes na área de expressão é a forma como a luta contra a desinformação e as chamadas *fake news* têm levado muitos países a adotar novas regras que podem

ter impactos que se estendem muito além de suas fronteiras. Uma maioria substancial (60,98%) dos participantes entrevistados concordou ou concordou fortemente que a natureza transfronteiriça da Internet facilitou a interferência estrangeira no processo democrático. Casos em que contas automatizadas de redes sociais criadas no exterior acabam desempenhando um papel nas eleições de um país não são incomuns na região.



A mesma demanda de cooperação entre os países para enfrentar os desafios jurisdicionais surgiu na região durante as investigações sobre escândalos de corrupção. Para garantir evidências localizadas em diferentes países, as agências de execução da lei na América Latina e no Caribe estão pressionando por mais cooperação, o que deve criar condições para a padronização das transferências transfronteiriças de dados na região.

A coordenação é crucial para se criar um mercado único digital na América Latina e no Caribe. Um tema que veio claramente à tona nas entrevistas e pesquisas realizadas para o Relatório foram os efeitos econômicos de uma abordagem regional para questões como a disseminação da tecnologia financeira (*fnotech*) na região. Os atores expressaram um apoio considerável a soluções regulatórias inovadoras, com 82,92% concordando ou concordando fortemente que a implantação de marcos inovadores, como *w* regulatórias, contribuem para fomentar o crescimento econômico.

O Relatório também destaca a forma como abordagens significativas dos dilemas transfronteiriços da Internet na América Latina e no Caribe podem vir de iniciativas legislativas ou do desenvolvimento de ferramentas tecnológicas, como o bloqueio



geográfico e a filtragem de conteúdo, levando em consideração todas as controvérsias que tais recursos poderiam trazer.

O *Relatório de Status Regional 2020* da Rede de Políticas Internet & Jurisdição e CEPAL destina-se a fornecer ferramentas para a inovação em matéria de políticas públicas baseadas em evidências e fornecer a todos os atores as informações necessárias para desenvolver marcos e padrões de políticas para a sociedade digital na América Latina e no Caribe. O Relatório contém as seguintes principais observações:

Principais aspectos transversais das tendências e soluções: tendências abrangentes

- A conectividade está em ascensão. Vários países da região estão experimentando um aumento significativo dos números dos incluídos digitalmente, mas a eliminação do abismo digital e o combate às desigualdades socioeconômicas estruturais ainda são grandes desafios para o desenvolvimento e a inovação.
- O panorama está mudando. A euforia tecnológica romantizada do passado deu lugar a um “techlash” (animosidade pública em relação às grandes empresas de tecnologia), desencadeado por preocupações sobre desinformação, discurso de ódio e cibercrime (com um período recente de intensidade tecnológica em resposta à pandemia da COVID-19 e como parte da luta contra ela). As interações transnacionais são uma nova dinâmica emergente, a influência das empresas multinacionais é forte e o ambiente empreendedor das *start-ups* regionais está crescendo.
- As iniciativas regulatórias estrangeiras influenciaram as propostas regionais e nacionais. Há um apetite crescente por regulação do ciberespaço, como atesta a proliferação de iniciativas; mas essas inspirações legislativas e judiciais são fertilização cruzada úteis ou mera transplantação?
- Estão surgindo preocupações sobre a influência externa e a crescente pluralidade normativa. As regras estão sendo definidas por – e para – grandes atores internacionais bem estabelecidos e o papel das normas das empresas está aumentando à medida que seus termos de serviço atingem status “constitucional” para os espaços digitais que controlam.
- O papel da territorialidade/soberania em uma rede global

está sendo cada vez mais questionado. As leis nacionais são cada vez mais extraterritoriais em alcance, mas isso vem gerando desafios de aplicabilidade.

- Espera-se que os intermediários desempenhem novos papéis. Os operadores privados estão sendo convidados a assumir responsabilidades crescentes; os intermediários foram convocados a fornecer um apoio significativo nas investigações administrativas e judiciais; a transparência é vital para aumentar a confiança, mas a implementação varia; há uma preocupação crescente com o devido processo nas atividades de moderação de conteúdo.

Principais tendências temáticas na América Latina e no Caribe

EXPRESSÃO:

- Notícias falsas e campanhas de desinformação estão desencadeando apelos para tomada de medidas regulatórias;
- Os governos estão impondo regras mais rigorosas para moderação e remoção de conteúdo em plataformas on-line;
- A distribuição não consensual de mídia sexualmente explícita (“pornografia de vingança”) não conhece fronteiras e pode perpetuar o dano;
- O caso Google Espanha no Tribunal de Justiça da União Europeia (TJUE) desencadeou um debate regional sobre o “direito ao esquecimento”: enquanto os especialistas reconhecem esse direito como um escopo global, a experiência regional com leis de anistia e a noção de “direito à memória” criaram uma reação contra a aplicação de um direito geral a ser esquecido;
- Os casos de difamação estão desencadeando debates sobre os efeitos transfronteiriços de proteger a reputação de uma pessoa. Além disso, a difamação é tanto uma ofensa civil quanto criminal em muitos países da região, levantando questões adicionais sobre como a proteção da reputação pode restringir a liberdade de expressão (por exemplo, para jornalistas e blogueiros).

SEGURANÇA:

- Há uma crescente necessidade e aspiração de coordenação nos esforços de cibersegurança para lidar com incidentes generalizados na região;
- Os casos de corrupção transfronteiriça na América Latina e no Caribe levaram a um debate sofisticado sobre práticas de investigação multi-jurisdicional;
- Os desafios envolvidos no acesso a provas digitais em várias jurisdições significam que é necessário rever as práticas de investigação atuais na região;
- Os atores regionais não defendem a reformulação geral do sistema de cooperação jurídica mútua (MLA), mas apoiam sua adaptação à era digital; no entanto, as agências de execução da lei da região estão buscando cada vez mais acesso aos dados do usuário fora da estrutura dos acordos de cooperação jurídica;
- Os atores regionais concordam que a Convenção de Budapeste é um passo na direção certa quando se trata de facilitar investigações transfronteiriças, mas que não resolve completamente os problemas do sistema de MLA;
- Os atores reafirmam que as *backdoors* prejudicam a confiança em sistemas criptografados;
- Os países da região ainda não adaptaram totalmente sua legislação às exigências do combate ao crime cibernético;
- O reconhecimento mútuo das identidades digitais seria um motor positivo de integração regional e econômica, principalmente para um mercado único digital.

ECONOMIA:

- Inspirados no GDPR, os países da América Latina e do Caribe estão criando ou melhorando regulamentos nacionais de proteção de dados;
- Metade dos países da região tem uma regulação específica de proteção de dados, mas há espaço para melhorias e coordenação a fim de alcançar uma estrutura verdadeiramente regional de proteção de dados;
- As iniciativas regionais estão promovendo a padronização das transferências transfronteiriças de dados;
- Há necessidade de criação de um mercado único digital na região;

- Os atores indicaram que áreas como a proteção ao consumidor e aos dados, pagamentos digitais e regimes fiscais são vitais para a criação de um mercado único digital regional;
- A região tem uma forte cultura de direitos do consumidor, proporcionando uma base útil para a criação de um mercado digital único;
- A escolha da lei aplicável e as cláusulas de escolha de foro tendem a ser malvisto no comércio eletrônico devido às normas nacionais de proteção ao consumidor;
- A Internet das Coisas (IoT) não conhece fronteiras e requer padronização, mas os atores estão divididos sobre a necessidade de regulação específica para IoT;
- Há uma série de desafios e oportunidades para cidades inteligentes na região;
- A agricultura inteligente amplia o conjunto de atores internacionais e constitui um movimento natural para a região;
- A evolução dos pagamentos digitais na região coexiste com uma população desbancarizada, baixa penetração de cartões de crédito internacionais, uma cultura de pagamento em moeda persistente e volatilidade cambial;
- As *fintechs* estão revolucionando os serviços financeiros na região, mas enfrentam tratamentos regulatórios díspares a nível nacional;
- Questões jurisdicionais transfronteiriças têm um impacto crescente nas atividades das empresas *fintech* na região;
- Os atores mostraram grande entusiasmo pela adoção de soluções regulatórias inovadoras, como *sandbox* regulatórias;
- *Blockchain* e criptomoedas são vistos como facilitadores do comércio transfronteiriço (mas também de crimes).

Principais abordagens aos dilemas transfronteiriços da Internet na América Latina e no Caribe: tendências jurídicas

- Os Estados estão recorrendo cada vez mais a uma “doutrina de efeitos” na afirmação de sua jurisdição;
- A afirmação de uma jurisdição geograficamente abrangente pode não levar à aplicação efetiva da lei;
- Até agora, os tribunais superiores da região têm se absterido de tomar decisões com alcance global;
- Os tribunais nacionais estão emitindo cada vez mais ordens de exclusão (*take-down*), manutenção da retirada

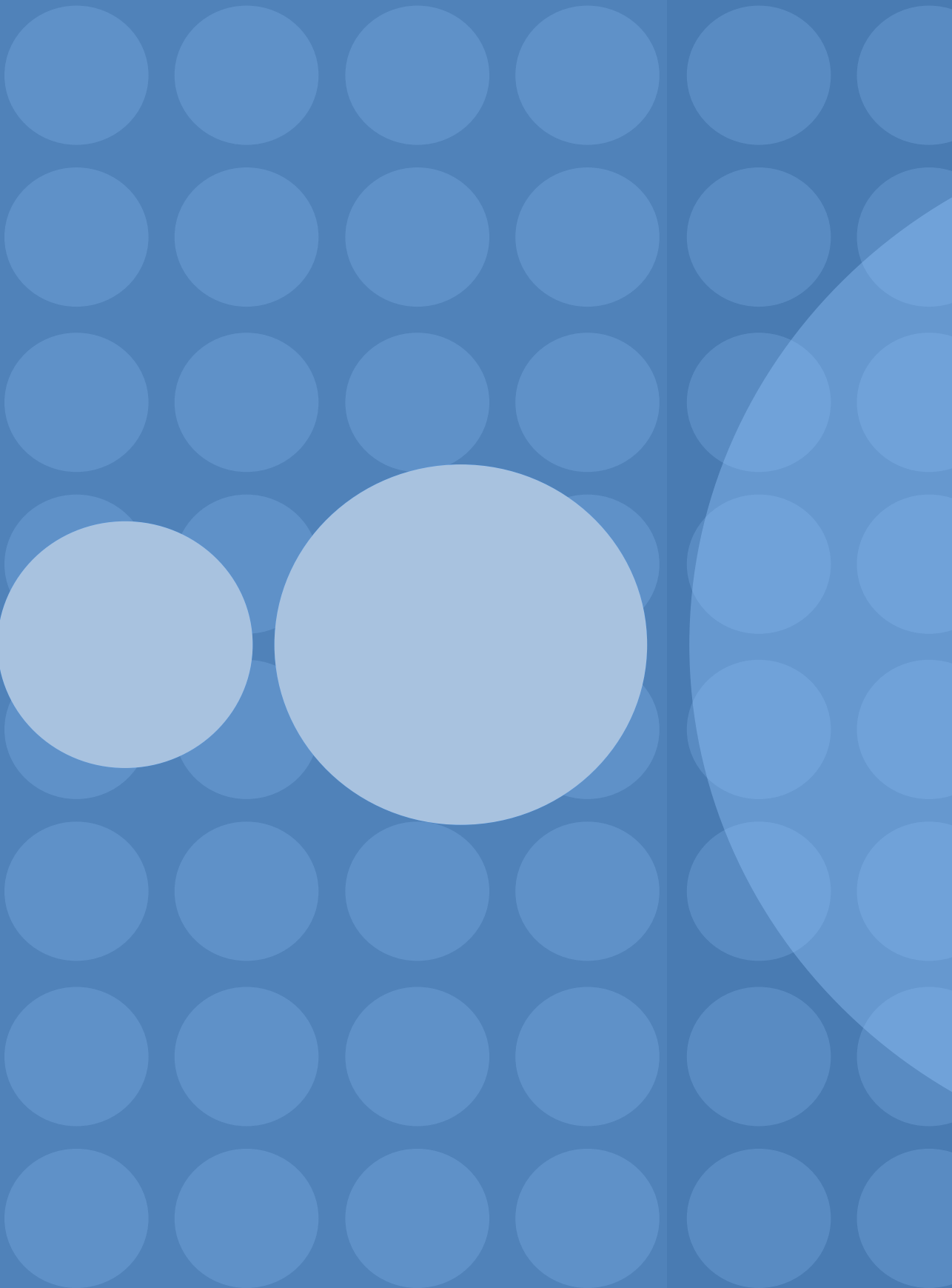


(*stay-down*) e de permanência (*stay-up*) para conteúdo publicado em plataformas on-line;

- Além da responsabilidade civil, os países recorrem cada vez mais a sanções administrativas para garantir o cumprimento de normas setoriais;
- Os termos de serviço das empresas interagem com as legislações nacionais, reforçando ou contradizendo as disposições que regulam o comportamento dos usuários;
- O impacto da controversa atualização da Diretiva Europeia sobre Direitos Autorais já está sendo sentido na região;
- Os mercados on-line (*marketplaces*) estão implantando sistemas de resolução de disputas enquanto os governos pressionam para a corregulamentação da venda de produtos falsificados;
- No interesse da defesa do consumidor, os tribunais da região tendem a não reconhecer cláusulas de escolha do foro e do direito aplicável nos termos de serviço das plataformas internacionais;

Principais abordagens para dilemas transfronteiriços na Internet na América Latina e no Caribe: ferramentas

- O uso de dados pessoais para mapear e controlar a pandemia da COVID-19 consolidará a discussão sobre tecnologias de geolocalização na região;
- O bloqueio geográfico e a geoprecificação estão aumentando as preocupações antitruste e de proteção dos consumidores e de dados;
- A filtragem de conteúdo está crescendo à medida que os países combatem discurso de ódio e desinformação;
- O bloqueio de aplicativos, que já foi um último recurso, é agora uma prática comum, com potencial para grandes impactos além das fronteiras;
- O bloqueio de DNS está sendo ordenado por alguns governos, mas não é uma prática generalizada;
- As interrupções da Internet não são comuns, mas podem acontecer em momentos de agitação social;
- A localização obrigatória de dados foi adotada em alguns países por várias razões, mas levanta sérias preocupações entre os atores.



Introdução

POR QUE UM RELATÓRIO DE STATUS REGIONAL?

Este Relatório é a primeira versão regional do pioneiro Relatório de Status Global 2019 que a Rede de Políticas Internet & Jurisdição lançou no Fórum de Governança da Internet das Nações Unidas em Berlim, em novembro de 2019, fornecendo pela primeira vez uma referência global para o ecossistema transfronteiriço de jurisdição da Internet. Este relatório regional baseia-se na metodologia comprovada do relatório global de 2019.

Os objetivos do *Relatório de Status Regional 2020* da Rede de Políticas Internet & Jurisdição CEPAL são os seguintes:

- Mapeamento e consolidação de informações relevantes para a região da América Latina e Caribe e para o mercado digital regional. O Relatório fornece, pela primeira vez, uma visão regional abrangente e uma documentação das tendências passadas, atuais e emergentes, atores significativos, além de propor soluções para os principais desafios de política jurisdicional transfronteiriça que os atores enfrentam na América Latina e no Caribe.
- Investigação das tendências e desafios político-regulatórios mais marcantes da sociedade e economia digitais. O Relatório expande, em particular, as conclusões e as questões englobadas pelos três programas da Rede de Políticas Internet & Jurisdição, a saber, acesso transfronteiriço aos dados dos usuários, restrições de conteúdo transfronteiriço e suspensões de domínio. O Relatório também examina as questões e os debates emergentes mais importantes, incluindo temas como a Internet das Coisas, comércio digital e *blockchain*, a fim de mapear esses futuros desafios regulatórios.
- Criação e fortalecimento de redes de colaboradores regionais. O Relatório fornece uma base consolidada para o desenvolvimento de capacidades através do compartilhamento de conhecimento e da facilitação da tomada de decisões bem-informadas, utilizando um processo inovador de contribuição e revisão colaborativa em larga escala para criar uma rede regional de colaboradores e alavancar a experiência combinada de atores engajados, através de entrevistas estruturadas e esforços de coleta de dados.

- Capacitação para os principais atores sobre temas jurídicos transfronteiriços associados à transformação digital. Essa visão geral e análise das tendências e iniciativas fornecem aos tomadores de decisão uma interpretação das questões fundamentais envolvidas, altamente complexas e muitas vezes técnicas, e contribui para o desenvolvimento de uma taxonomia comum tão necessária para o ecossistema de políticas públicas. O Relatório visa ajudar a atenuar conflitos jurisdicionais agudos, apoiar o desenvolvimento de soluções operacionais concretas e dotar os intervenientes políticos com as informações de que necessitam para evitar perder os benefícios da Internet transfronteiriça aberta e interoperável.

Este documento deve servir aos profissionais como um roteiro para algumas das questões mais urgentes em torno da elaboração de políticas públicas e da natureza transfronteiriças da Internet na América Latina e no Caribe.

A. A Internet: um panorama regulatório em rápida evolução

Há mais de duas décadas, tem-se discutido se e como a Internet pode ser regulada. Antes de se chegar a um acordo sobre essas questões, porém, é importante refletir sobre o que realmente significa regular a Internet. A regulação vem em muitas formas diferentes, e uma lei imposta pelo Estado não é a única forma de estimular ou desencorajar o comportamento. Lawrence Lessig sugeriu, em 1999, que o cabo de guerra regulatório poderia ser mais complexo quando o que estava em discussão é como a tecnologia afeta o comportamento humano. As regras jurídicas não são a única fonte de regulação. Em vez disso, elas têm que enfrentar forças concorrentes como o mercado e sua lógica econômica, restrições sociais e, por último, a própria tecnologia, cuja arquitetura pode permitir ou impedir um determinado tipo de comportamento.¹

O cenário retratado por Lessig revela que as mudanças na cultura, nas forças de mercado ou na arquitetura tecnológica podem ser mais eficazes do que as mudanças legislativas na formação

1 L. Lessig, "The Law of Horse; what CyberLaw might teach", Harvard Law Review, vol. 113, No. 501. Disponível em: <<https://cyber.harvard.edu/works/lessig/finalhls.pdf>>. Acesso em: 09 mai 2021.

das relações e comportamentos humanos. Para que o futuro da regulação da Internet seja compreendido, a análise deve incluir, mas não se limitar, à ação do Estado.

Os Estados desempenham inquestionavelmente um papel importante ao estabelecer as regras legais, mas também têm um papel coordenador, ao promover a inclusão e a alfabetização digitais em uma determinada sociedade e alinhar os incentivos do mercado. No entanto, o Estado sozinho não pode controlar totalmente a regulação da Internet ou os seus resultados finais.

Sobre o tema da desinformação, por exemplo, tornou-se cada vez mais claro que os incentivos econômicos dos modelos de monetização implementados pelas plataformas podem impactar os tipos de conteúdo desenvolvidos para distribuição on-line.² As características e critérios dos algoritmos de curadoria também influenciam o consumo ou não de discursos controversos, disputados ou mesmo polarizadores nas redes sociais³. A alfabetização midiática e a etiqueta social também desempenham um papel.⁴ Todos esses fatores são tão importantes para restringir a disseminação da desinformação quanto as regras legais, e às vezes até mais importante do que estas.

Para dar outro exemplo, a proteção da propriedade intelectual on-line avançou muito devido a uma mudança de mercado. O procedimento tradicional de rastrear infratores reincidentes – sejam aqueles que colocam material protegido por direitos autorais ou aqueles que constantemente acessam esse material – e depois encerrar suas contas, aplicando-lhes multas ou, em alguns casos, até mesmo prendendo-os, tem seus limites. O advento das plataformas de *streaming* para vídeo e música, no entanto, teve um grande impacto, e o consumo de conteúdo pirateado on-line despencou.⁵

-
- 2 V. Bakir e A. Mcstay, "Fake news and the economy of emotions: problems, causes, solutions", *Digital Journalism*, vol. 6, No. 2, 2018. Disponível em: <<https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1345645>>. Acesso em: 09 mai 2021.
 - 3 S. Bradshaw, "Disinformation optimized: gaming search engine algorithms to amplify junk news", *Internet Policy Review*, vol. 8, No. 4, 2019.
 - 4 F. Saurwein and C. Spencer-Smith, "Combating disinformation on social media: multilevel governance and distributed accountability in Europe", *Digital Journalism*, vol. 8, 2020.
 - 5 M. Freixo Nunes, "On-demand music streaming and its effects on music piracy", *Dissertation, International Master of Science in Management, Universidade Católica Portuguesa*, 2018.

Porém, justamente quando os consumidores começaram a adquirir novos hábitos, a multiplicidade de plataformas de *streaming* acabou criando novas restrições econômicas, tornando mais caro para os usuários acessar todo o conteúdo que desejam. Alguns veem isso como o início de uma nova fase de acesso ilegal generalizado a conteúdo on-line protegido por direitos autorais.⁶

Na América Latina e no Caribe, onde os recursos para a aplicação da lei e sua fiscalização são escassos, é ainda mais importante que as regras jurídicas levem em consideração e se beneficiem das diferentes forças em jogo na regulação da Internet. Este Relatório, portanto, baseia-se no conhecimento das tendências que envolvem as quatro áreas: regras jurídicas, incentivos econômicos, normas sociais e tecnologia. A ideia é extrair percepções da sua interação e destacar como os quatro pontos do cabo de guerra impactam a regulação transfronteiriça.

B. Interesses concorrentes são difíceis de conciliar além das fronteiras

Em um nível básico, o objetivo da regulação da Internet é combater abusos, proteger direitos individuais e salvaguardar a inovação e a economia digital, particularmente o acesso ao mercado. Do ponto de vista da região, no entanto, existem outras dimensões a serem consideradas.

Apesar da percepção de pontos comuns, a América Latina e o Caribe são muito diversos em termos de tamanho, desenvolvimento econômico e até mesmo de raízes sociais e culturais. Essa diversidade faz com que os alinhamentos de interesses sejam complicados. Existem diversas conexões e alianças nacionais, subnacionais e sub-regionais, e todas elas são influenciadas por interesses extrarregionais, sejam eles de países e regiões importantes, como os Estados Unidos, Europa ou China, ou de corporações e organizações multinacionais que exercem pressão sobre os tomadores de decisão nacionais e regionais, independentemente das rivalidades fomentadas por um ambiente mais competitivo do que cooperativo.

Tudo isto proporciona um pano de fundo difícil para a resolução de dilemas jurídicos transfronteiriços. Por um lado, existem

6 Ver: Intelligencer, "Piracy is Back", 26 Jun, 2019. Disponível em: <<https://nymag.com/intelligencer/2019/06/piracy-is-back.html>>. Acesso em: 09 mai 2021.

padrões diferentes e até contraditórios na região, alguns deles intrínsecos ao senso de identidade ou à ordem ou racionalidade jurídica de cada país. Por outro lado, a pressão de diferentes grupos de interesse pode levar ao transplante de conceitos legais e à implementação inadequada ou inapropriada de soluções legais.

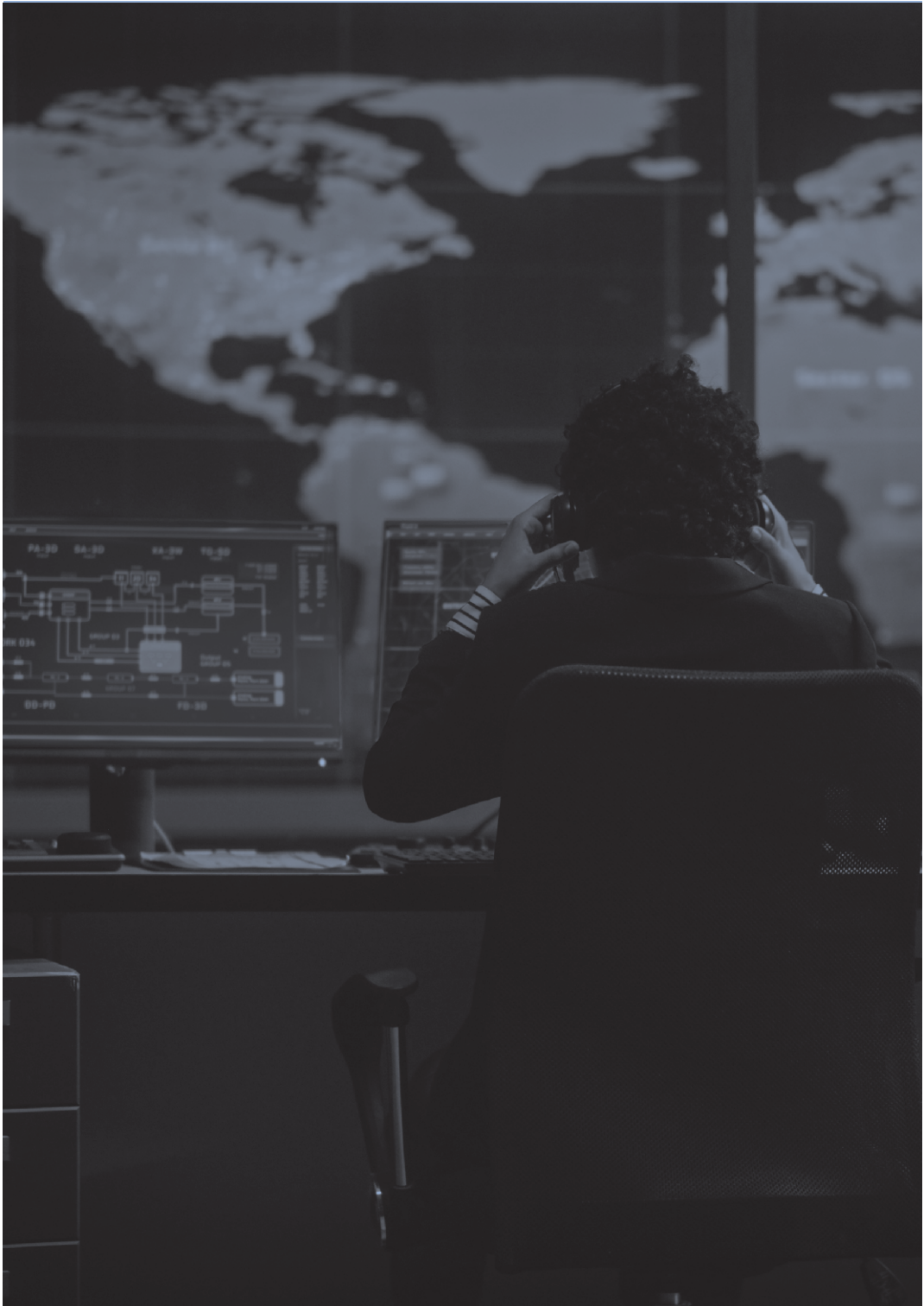
Este contexto torna-se particularmente desafiador na ausência de qualquer acordo internacional que possa fornecer orientações claras, coordenar ações e resolver contradições. Em busca de eficácia, e apesar do choque de interesses, vários Estados se encarregaram de resolver unilateralmente os problemas da Internet. Isso assume a forma de afirmações de soberania sobre o ciberespaço, aplicação extraterritorial da legislação nacional e até decisões administrativas e judiciais com alcance global (todos os tópicos explorados neste Relatório). O resultado pode aumentar o potencial para confrontos, criar mais competição entre Estados e até mesmo exacerbar as diferenças de alcance e capacidade dos Estados, a menos que esses desafios sejam enfrentados através da cooperação e coordenação.

C. Empresas, governos e indivíduos estão cada vez mais preocupados com os abusos on-line

Há uma preocupação crescente com os abusos on-line (desinformação, discurso de ódio, assédio, cibercrime, hackers, violações de privacidade e fraude, entre outros). O sentimento geral é que o rápido aumento da conectividade tem sido acompanhado por oportunidades de comportamento antiético e ilegal on-line.

Essa visão é fortalecida pela percepção de que a natureza sem fronteiras do ciberespaço torna mais difícil o policiamento, dificulta as investigações e restringe o escopo da ação governamental. A regulação estatal parece porosa e incapaz por si só de abranger ou responder adequadamente a atividades que impactam a vida e a propriedade dos cidadãos.

Os atores entrevistados observaram que havia pelo menos três dimensões diferentes para tais preocupações: (i) indivíduos agindo sozinhos ou em coordenação podem causar um grande dano sem que estejam fisicamente presentes em nenhum momento em um país, tornando mais verdadeiro do que nunca que o crime e a fraude não cessam nas fronteiras; ii) as empresas internacionais estão sob pressão para agir e nem sempre se sentem obrigadas a observar as especificidades das regulações nacionais,



especialmente quando os requisitos locais são contrários às obrigações legais do seu local de constituição; e iii) a influência estrangeira em diferentes formas e graus impacta tanto o conteúdo das respostas jurídicas locais quanto a sua capacidade de atingir seus objetivos, com desequilíbrios de poder entre os países, tornando a ação doméstica potencialmente inferior à ideal.

Além disso, escândalos internacionais como as revelações de Snowden,⁷ Cambridge Analytica⁸ e Panama Papers⁹ mostraram até que ponto as situações que surgem em um país podem impactar o próprio tecido da ordem política de outro país. Os instrumentos jurídicos disponíveis não respondem ou não podem responder plenamente aos desafios.

Alguns dos atores entrevistados apontaram que tais incidentes internacionais tinham sido frequentemente acompanhados de agitações domésticas. Um especialista observou que muitos governos capitalizaram essas respostas emocionais, recorrendo ao direito penal e à criminalização do comportamento on-line com diferentes graus de sucesso. Outro mencionou a tendência de ampliar o alcance das leis nacionais, seja através da aplicação extraterritorial ou criando uma forma de localização forçada, especialmente quando se busca acesso a dados para investigações criminais ou para fins de segurança nacional.

D. Abordar desafios jurisdicionais transfronteiriços é fundamental para construir confiança em uma rede global

A natureza global da Internet é parte integrante de como o ciberespaço tem sido arquitetado. O *world* (mundo) em “World Wide Web” (www) não está lá por acaso. A camada lógica da Internet é sem fronteiras desde a concepção (*by design*). No entanto, a ordem mundial internacional está estruturada sobre

-
- 7 Ver: L. M. Austin, “Lawful Illegality: What Snowden Has Taught us about the Legal Infrastructure of the Surveillance State”, abril 2014. Disponível em: <<https://ssrn.com/abstract=2524653>>. Acesso em: 09 mai 2021.
 - 8 Ver F. González and others, “Global Reactions to the Cambridge Analytica Scandal: A Cross-Language Social Media Study”, 2019. Disponível em: <https://www.researchgate.net/publication/333066944_Global_Reactions_to_the_Cambridge_Analytica_Scandal_A_Cross-Language_Social_Media_Study>. Acesso em: 09 mai 2021.
 - 9 Ver: L. J. Trautman, “Following the Money: Lessons from the Panama Papers, Part 1: Tip of the Iceberg”, Penn State Law Review, vol. 807, 12 de maio de 2017. Disponível em: <<https://ssrn.com/abstract=2783503>>. Acesso em: 09 mai 2021.

um princípio muito diferente, com a igualdade soberana dos Estados tornando o Estado-nação e seu território geográfico como o principal centro de regulação.¹⁰ Diferentes abordagens e até mesmo prioridades são de se esperar. A regulação tende, então, a não ser nem constante, nem uniforme.

Lidar com a coexistência de leis e métodos regulatórios tão heterogêneos que se aplicam à Internet transfronteiriça é um dos maiores desafios do século XXI. Soluções regulatórias escaláveis e coerentes não podem ser desenvolvidas sem uma compreensão abrangente deste ecossistema altamente complexo e dinâmico, composto por vários atores, iniciativas e tendências em todos os espaços de políticas da economia digital, direitos humanos e segurança.

Este paradoxo da regulação primária local e do espaço global (ciberespaço), juntamente com a multiplicidade de atores, tende naturalmente a levar à fragmentação. Dois fenômenos podem ter impacto na Internet como ela é atualmente. O primeiro é a tendência de que ela se fragmente, recriando as fronteiras do mundo físico no ciberespaço. O segundo são os esforços das instituições nacionais para exercer influência extraterritorial na tentativa de regular a Internet global de um ponto de vista nacional unilateral. Ambas as dinâmicas minam a utilidade e a confiança na Internet global.

A história da região da América Latina e do Caribe de luta contra a colonização e o surgimento do princípio internacional da não-intervenção tendem a reforçar ambos os fenômenos: fragmentação e esforços para ampliar o alcance da legislação nacional extraterritorialmente. No entanto, diferenças de dimensão, poder e eficiência administrativa significam diferentes graus de sucesso.

Em qualquer caso, os especialistas consultados observaram a tendência dos países da região para regular a Internet e afirmar sua soberania sobre o ciberespaço. Isso parece ser particularmente verdadeiro quando se trata de dados, com reivindicações de soberania e localização de dados (como discutido na seção V.B.6) e com aplicações extraterritoriais da legislação de proteção de dados (como analisado na seção IV.C.6).

10 M.Kettman, *The Normative Order of the Internet: A Theory of Rule and Regulation Online*, Oxford University Press, 2020. Disponível em: <https://www.ssoar.info/ssoar/bitstream/handle/document/69191/ssoar-2020-kettemann-The_Normative_Order_of_the.pdf?sequence=2&isAllowed=y&lnkname=ssoar-2020-kettemann-The_Normative_Order_of_the.pdf>. Acesso em: 09 mai 2021.

Para fazer avançar o debate regional sobre a concepção e aplicação da legislação on-line e para catalisar o desenvolvimento de uma estrutura compartilhada, é importante que os atores se envolvam em diálogos contínuos que ajudem a identificar os desafios e promovam a coordenação de diferentes iniciativas e propostas regulatórias. A obtenção de informações de alta qualidade através de pesquisas e documentação relevantes é vital para apoiar os processos de tomada de decisão e estimular a inovação política baseada em evidências. Este Relatório apresenta o estado atual da discussão e as tendências em curso, fornecendo a base para uma reflexão necessária sobre a forma de abordar adequadamente o aspecto de coordenação da jurisdição e das preocupações transfronteiriças.

Do ponto de vista da região, a integração digital é, sem dúvida, uma oportunidade. É parte indispensável do esforço para diversificar as economias regionais. Há evidências do enorme potencial do comércio intrarregional para avançar na direção de uma cesta de exportação mais intensiva em termos de conhecimento. Em 2018, 54% das exportações intrarregionais por valor consistiam em manufaturas de alta, média e baixa tecnologia.¹¹ Ao mesmo tempo, o rápido crescimento do comércio eletrônico internacional proporciona grandes oportunidades de comércio internacional para as pequenas e médias empresas (PMEs).

Estima-se que 155,5 milhões de pessoas na América Latina compraram produtos e serviços on-line em 2019, um aumento substancial de 22% em relação aos 126,8 milhões que o fizeram em 2016. No entanto, o número médio anual de transações on-line per capita na América Latina em 2016 foi o menor do mundo, com apenas 9,2 ao ano.¹²

A região fez progressos significativos com a legislação relativa à Internet. Em 2017, mais de 80% dos países da América Latina e do Caribe tinham algum tipo de legislação sobre transações eletrônicas e assinaturas eletrônicas e 90% tinham regulações sobre propriedade intelectual.

11 Economic Commission for Latin America and the Caribbean (ECLAC), International Trade Outlook for Latin America and the Caribbean, 2018 (LC/PUB.2018/20-P), Santiago, 2018.

12 Statista, E-commerce in Latin America. Disponível em: <<https://www.statista.com/study/14764/e-commerce-in-latin-america-statista-dossier/>>

Estes números destacam a importância de promover uma estrutura legal e regulatória harmonizada para ajudar a eliminar as barreiras ao comércio eletrônico transfronteiriço e ao investimento em mercados digitais. A harmonização das estruturas regulatórias em toda a região poderia criar benefícios econômicos e sociais significativos, potencialmente levando ao aumento da confiança dos investidores e a mais investimento estrangeiro direto, à promoção da inovação e à diversificação econômica. Também poderia fomentar a confiança no comércio eletrônico e impulsionar um mercado de mais de 600 milhões de pessoas, ao mesmo tempo em que abriria uma série de oportunidades para as empresas, incluindo as pequenas e médias empresas.

E. A coordenação necessária para enfrentar este desafio é negligenciada

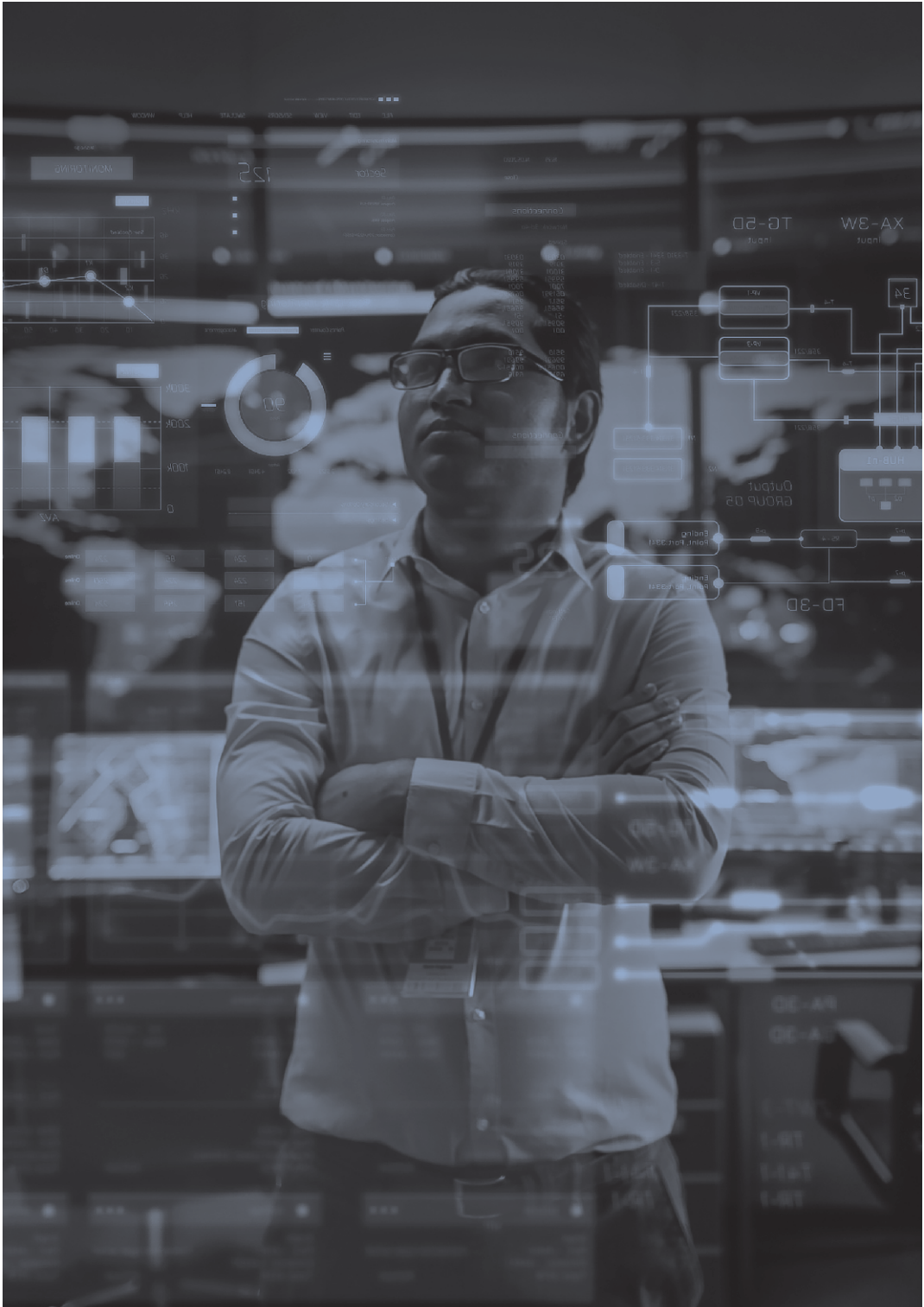
Os países da região estão cada vez mais conscientes da dimensão internacional dos desafios trazidos pela Internet. Ficou claro que a natureza global da rede mundial é uma fonte tanto de força, proporcionando muitas oportunidades sociais e econômicas, quanto de uma série de dificuldades associadas a ela, particularmente a interação entre a ação local e o impacto internacional e vice-versa.

As estruturas governamentais nacionais, no entanto, parecem insuficientes por si só para lidar com muitas das questões trazidas pela Internet. Com a eficácia da ação do Estado assim desafiada, noções de soberania e não-interferência parecem assumir conotações diferentes.

Essa percepção é reforçada pelo poder relativo e impacto potencial dos países da América Latina e do Caribe. Os entrevistados falaram da impressão de que nem todos os Estados podem ter a mesma influência na forma como a Internet é regulada ou na forma como eles e seus cidadãos são afetados por sua estrutura e arranjos de governança.

1. NECESSIDADE DE DIÁLOGO ENTRE OS DIVERSOS ATORES DA REGIÃO

A comunidade internacional há muito reconhece a necessidade do diálogo entre os diversos atores para discutir a governança da Internet. O Fórum de Governança da Internet (IGF) é a plataforma predominante para esse diálogo. No entanto, o



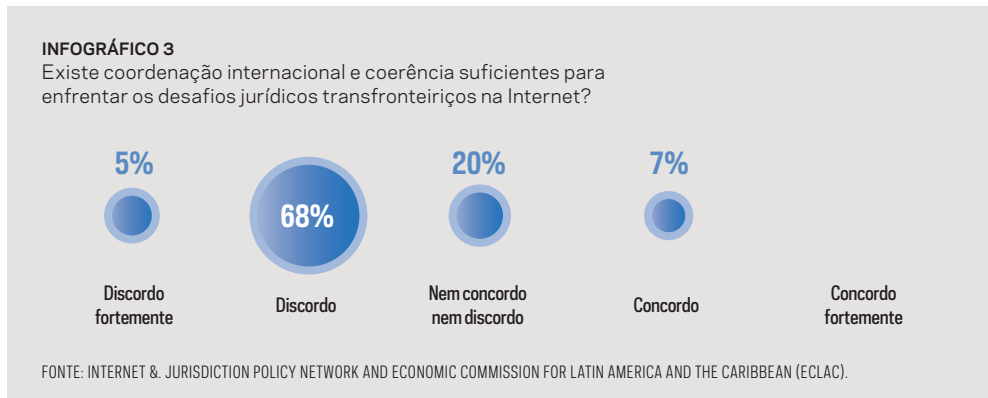
Relatório do Painel de Alto Nível sobre Cooperação Digital do Secretário-Geral das Nações Unidas de 2020 identificou desafios e lacunas nos acordos de cooperação digital existentes e propôs três possíveis arquiteturas para essa cooperação em escala global.¹³ Os atuais mecanismos de tomada de decisão sobre a governança da Internet estão, portanto, passando por melhorias.

O primeiro Fórum de Governança da Internet da América Latina e Caribe (LACIGF, na sigla em inglês) foi realizado em 2008 por iniciativa da Associação para o Progresso das Comunicações (APC, na sigla em inglês), do Registro de Endereços de Internet da América Latina e do Caribe (LACNIC, na sigla em inglês) e da Rede de Informação para o Terceiro Setor (RITS). Entre maio de 2019 e julho de 2020, o Comitê do Programa LACIGF realizou uma revisão do LACIGF com o objetivo de elaborar propostas concretas para o desenvolvimento e avaliação de pontos de ação para melhorar os fóruns.¹⁴ Os atores mencionaram o LACIGF como uma importante oportunidade para o mapeamento coletivo de problemas e o desenvolvimento de políticas públicas comuns, mesmo na ausência de decisões vinculativas. Também é importante garantir que esses mecanismos de coordenação garantam a diversidade e incluam jovens, mulheres e povos indígenas, ao mesmo tempo em que aumentam a representação sub-regional da América Latina e do Caribe. Em nível nacional, nem todos os países da América Latina e do Caribe têm uma agenda ativa para temas relacionados à governança da Internet. Tomando as iniciativas nacionais do IGF (iniciativas nacionais e regionais do IGF (NRIs, na sigla em inglês) como ponto de partida para análise, o primeiro evento nacional de governança da

13 United Nations, *The Age of Digital Interdependence. Report of the UN Secretary-Generals High-level Panel on Digital Cooperation, 2020*, pp. 22-29. Disponível em: <<https://www.un.org/en/pdfs/DigitalCooperation-report-for%20web.pdf>> [A Era da Interdependência Digital: Relatório do Painel de Alto Nível sobre Cooperação Digital do Secretário-Geral da ONU, 2020. Disponível em: <https://cgi.br/media/docs/publicacoes/1/20200901150023/CadernoCGIbr_A_era_da_interdependencia_digital.pdf>]. Acesso em: 09 mai 2021.

14 LACIGF, "Proposed first consultation for the review of LACIGF", 2020. Disponível em: <<https://lacigf.org/en/proposed-first-consultation-for-the-review-of-lacigf/>>. Acesso em: 09 mai 2021. Para mais informações, ver: R. Echeberria, *Review of the Latin American and Caribbean Internet Governance Forum (LACIGF), Public Consultation Process, Report and Conclusions, 2020*. Disponível em: <<https://lacigf.org/en/revision-del-lacigf/>>. Acesso em: 09 mai 2021.

Internet foi realizado no Brasil em 2011. No momento da redação deste Relatório, eventos nacionais do IGF na região da América Latina e Caribe são realizados na Argentina, Barbados, República Bolivariana da Venezuela, Brasil, Colômbia, Costa Rica, República Dominicana, Equador, El Salvador, Guatemala, Haiti, Honduras, México, Panamá, Paraguai, Peru, Estado Plurinacional da Bolívia, São Vicente e Granadinas, Trinidad e Tobago e Uruguai.¹⁵



Como mostra a rápida difusão dessa iniciativa, o debate sobre a governança da Internet vem ganhando ritmo na região. Isso demonstra como as iniciativas de alguns países podem servir de inspiração e incentivar outros países da América Latina e do Caribe a fortalecer o debate nacional sobre temas da Internet. Embora esse não seja um passo necessário para a coordenação regional, os desenvolvimentos em nível nacional também são importantes porque aumentam o capital humano e a capacidade dos formuladores de políticas públicas para trabalhar nas escalas regional e global. A CEPAL foi citada pelos atores como um pioneiro e importante órgão de governança com a infraestrutura necessária não só para promover iniciativas de capacitação em países onde essas questões ainda não foram muito trabalhadas,

15 IGF, Latin American and Caribbean Regional Group (GRULAC). Disponível em: <<https://www.intgovforum.org/multilingual/content/latin-american-and-caribbean-regional-group-grulac>>. Acesso em: 09 mai 2021; ver também: C. Aguerre and others, Mapping National Internet Governance Initiatives in Latin America, University of Pennsylvania, 2018]. Disponível em: <http://globalnetpolicy.org/wp-content/uploads/2018/06/Latin-AmericanReport_IPO_final.pdf>. Acesso em: 09 mai 2021.

mas também para desempenhar um papel ativo na catalisação da transformação de forma mais ampla.

Os atores mencionaram entidades regionais que poderiam abordar algumas das questões apresentadas neste Relatório, como a Comissão Interamericana de Telecomunicações (CITEL) e o Fórum Latino-Americano de Reguladores de Telecomunicações (REGULATEL), mas observaram que a cooperação regional genuína e a harmonização significativa ainda estão muito distantes. Há um problema de continuidade nas políticas implementadas, o que sugere a necessidade de políticas de médio e longo prazo na região.

2. UMA CRESCENTE ASPIRAÇÃO DE COOPERAÇÃO E COORDENAÇÃO

A cooperação e a coordenação tornaram-se metas significativas e talvez necessárias para enfrentar os desafios transfronteiriços. O argumento para a ação coordenada parece forte à luz dos ganhos potenciais para a economia (em termos de escala, acesso a mercados e tecnologia) e para a segurança (segurança cibernética e proteção de serviços básicos e de infraestruturas críticas). A cooperação e a coordenação também têm um papel importante a desempenhar na luta contra desafios sociais significativos, como a desinformação e a cibercriminalidade.

A ação descoordenada de uma ampla gama de atores e iniciativas pode dificultar a digitalização de economias, governos e sociedades. Entre os atores entrevistados, 73,17% concordaram ou concordaram fortemente que havia necessidade de coordenação para enfrentar os desafios jurídicos transfronteiriços.

Só esse número é suficiente para definir a direção deste Relatório, que é apresentado pela Rede de Políticas Internet & Jurisdição em coordenação com a Comissão Econômica das Nações Unidas para a América Latina e o Caribe (CEPAL) para fornecer mapeamento e análise indispensáveis do ecossistema na América Latina e no Caribe.

Com a região da América Latina e do Caribe visando desenvolver um mercado único digital, os atores que responderam ao questionário para este Relatório enviaram uma mensagem forte, com 78,04% tendo concordado que seria necessário um esforço significativo de harmonizar as normas para que esse objetivo fosse alcançado. Como enfatizou um dos atores pesquisados:



Creio que os países do MERCOSUL e da América Latina devem encontrar uma maneira de se envolver em uma ampla regulação transfronteiriça que possa fomentar a economia digital na região. Atualmente, o arcabouço jurídico é muito escasso, sem pontos em comum. Essa disparidade está comprometendo o desenvolvimento da região.

Em um mundo em transição para uma nova década, aos países da América Latina e do Caribe tem sido apresentada a oportunidade de promover a integração regional em um momento em que os países precisam reinventar seus papéis no cenário global do despertar da pandemia do COVID-19. As repercussões sociais e econômicas serão grandes e entender como diferentes decisões políticas sobre a Internet (e tecnologia em geral) podem afetar outros países será crucial para os novos quadros que possam surgir da crise.





01. **Tendências gerais**

A combinação de estudos detalhados e contribuições dos atores — através de pesquisas e das entrevistas — chamou a atenção para várias tendências globais que são centrais para qualquer discussão sobre os desafios jurídicos transfronteiriços na Internet. Algumas dessas tendências refletem claramente aquelas descritas no Relatório de Status Global 2019¹⁶ da Rede de Políticas Internet & Jurisdição, e o presente Relatório destaca como elas vêm se desenvolvendo especificamente na região da América Latina e Caribe. Essas tendências abrangentes estão moldando as tendências atuais (seção IV) e, em certa medida, estabelecem os parâmetros dentro dos quais as abordagens jurídicas e técnicas podem ser exploradas (seção V).

A. O aumento da conectividade é necessário, mas pode reforçar as desigualdades socioeconômicas

Embora várias implicações jurisdicionais decorrentes da natureza transfronteiriça da Internet tenham consequências semelhantes em todo o mundo, o número de casos, seu impacto e a viabilidade de possíveis soluções variam de acordo com o grau de inclusão digital em um país específico. Na América Latina e no Caribe, 67% da população é usuária da Internet, com diferenças regionais e nacionais que variam de acordo com o nível socioeconômico e a localização geográfica.¹⁷

Os esforços de inclusão digital e desenvolvimento tecnológico devem levar em conta certas desigualdades, especialmente as relacionadas com renda, gênero, diferenças entre áreas urbanas e rurais, a forma como as comunidades indígenas acessam a Internet e a forma como os recursos on-line são acessíveis e compreensíveis para a população idosa.¹⁸

O grau em que as estratégias nacionais de desenvolvimento digital consideram cada um desses fatores varia. Por exemplo, em uma

16 Ver: <<https://www.Internetjurisdiction.net/news/release-of-worlds-first-Internet-jurisdiction-global-status-report>> [Versão em português: <<https://cgi.br/publicacao/cadernos-cgi-br-internet-jurisdicao-6-1/>>]

17 Development Bank of Latin America (CAF) and others, Las oportunidades de la digitalización en América Latina frente al COVID-19, Santiago, 2020, p. 9.

18 Ver: R. Martínez, A. Palma and A. Velasquez, "Revolución tecnológica e inclusión social: reflexiones sobre desafíos y oportunidades para la política social en América Latina", Social Policy series, No. 233 (lc/ts.2020/88), Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), 2020.

comparação entre 14 estratégias nacionais na região, em apenas quatro foram encontradas prioridades de aumento do acesso às populações de nível socioeconômico mais baixo, o que significa que existe a necessidade de uma agenda política adicional focada na redução das desigualdades no acesso à Internet.¹⁹ Ao mesmo tempo, pelo menos 12 países consideram o fosso digital (“digital gap”) a partir de três perspectivas importantes: (i) o desenvolvimento de uma infraestrutura robusta para conectividade digital de alta qualidade, (ii) a promoção do uso de tecnologias da informação e comunicação (TICs) na vida diária e (iii) o desenvolvimento econômico com o uso de plataformas e serviços digitais.²⁰

Quando a Internet se revelou a principal forma de trabalho, estudo e acesso dos cidadãos aos serviços básicos durante a crise da COVID-19, diferentes atores regionais reconheceram que um ecossistema digital desenvolvido estava intrinsecamente relacionado ao desenvolvimento social e econômico e que a Internet era uma ferramenta necessária para várias atividades diárias, como trabalho, estudo, comércio e comunicação. Os países com um fosso digital maior sofreram consequências mais negativas do que aqueles com menor desigualdade. Entre 2004 e 2018, o ecossistema digital na América Latina e no Caribe se desenvolveu menos do que em qualquer outra região em desenvolvimento, exceto os Estados Árabes.²¹ Em geral, a penetração da Internet cresceu consideravelmente nos países da América Latina e do Caribe, mas continuam a existir diferenças entre eles. No Equador, 60,67% da população tinha acesso à Internet em 2018, aumentando para 68,09% em 2020. Em Honduras, o número aumentou de 34,06% em 2018 para 39,33% em 2020.²²

19 Ibid., p. 57.

20 Ibid., p. 55.

21 Ásia e Pacífico: 9,39%; África: 8,27%; Europa Oriental: 6,89%; América Latina e Caribe: 6,21% (Banco de Desenvolvimento da América Latina (CAF) e outros, *Las oportunidades de la digitalización en América Latina frente al COVID-19*, Santiago, 2020, p. 5. Disponível em: <<https://www.cepal.org/es/publicaciones/45360-oportunidades-la-digitalizacion-america-latina-frente-al-covid-19>>. Acesso em: 09 mai 2021.

22 Telecom Advisory Services, *El estado de la digitalización de América Latina frente a la pandemia del COVID-19*, Banco de Desenvolvimento da América Latina (CAF), abril 2020, p. 18. Disponível em: <https://scioteca.caf.com/bitstream/handle/123456789/1540/El_estado_de_la_digitalizacion_de_America_Latina_frente_a_la_pandemia_del_COVID-19.pdf?sequence=1>. Acesso em: 09 mai 2020.

Também é importante observar que a inclusão digital é um conceito que vai além do acesso à Internet em si. Um estudo do Banco de Desenvolvimento da América Latina (CAF) constatou que as ferramentas de comunicação e as mídias sociais são responsáveis pela maior parte do uso da Internet na região.²³ Isto indica a necessidade de um maior desenvolvimento para liberar todo o potencial da inclusão digital em seus aspectos sociais e econômicos.

Em qualquer caso, disponibilizar a Internet a todos os cidadãos é uma preocupação importante e também faz parte da Agenda 2030 para o Desenvolvimento Sustentável. O objetivo 9.c consiste em “aumentar significativamente o acesso às tecnologias de informação e comunicação e empenhar-se para procurar ao máximo oferecer acesso universal e a preços acessíveis à internet nos países menos desenvolvidos, até 2020”. De acordo com um estudo da CEPAL de 2020 sobre cenários e projeções considerando a pandemia da COVID-19, esta meta é “passível de ser alcançada na tendência atual” na região.²⁴

Um quadro digital e conectado também tem um papel a desempenhar no desenvolvimento de outras tecnologias particularmente importantes na região, como a agricultura inteligente (*smart farming*). Quanto mais desconectada for uma área rural, mais distante é a perspectiva de uma agricultura conectada e eficiente. Desenvolvimento já pode ser visto em iniciativas de inclusão digital voltadas para cadeias de suprimentos logísticos e agroindustriais.²⁵

Além disso, à medida que os países desenvolvem suas estratégias governamentais digitais e oferecem cada vez mais serviços públicos parcial ou totalmente pela Internet (por exemplo,

23 Ibidem., pp. 4, 18-21.

24 Economic Commission for Latin America and the Caribbean (ECLAC), The 2030 Agenda for Sustainable Development in the new global and regional context: scenarios and projections in the current crisis (lc/PUB.2020/5), Santiago, 2020.

25 Ver, por exemplo, o exemplo do Peru no Banco de Desenvolvimento da América Latina (CAF), “Sector público y privado comprometido en hoja de ruta para la digitalización de la cadena agroexportadora en región Ica”, 24 de janeiro de 2020. Disponível em: <<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>>. Acesso em: 09 mai 2020. Ver também: G. Pérez, “Rural roads: key routes for production, connectivity and territorial development”, FAL Bulletin, No. 377, Santiago, Economic Commission for Latin America and the Caribbean (ECLAC), julho 2020.

solicitações de benefícios sociais, registros fiscais e bancos de dados de registro), ser incluído digitalmente significa cada vez mais gozar dos direitos básicos do cidadão. A expansão das iniciativas de identidade digital é também um bom exemplo dessa tendência.

Estudos comparativos recentes sobre países latino-americanos e caribenhos reconheceram a importância das políticas públicas para reduzir o fosso digital na região.²⁶ Tais políticas geralmente incluem não apenas o acesso à própria rede, mas também disposições relativas à infraestrutura, fabricação de dispositivos e desenvolvimento de competências digitais. Os desenvolvimentos diferem na região, mas alguns destaques são mencionados abaixo.

- Em agosto de 2020, a Argentina emitiu o Decreto nº 690/2020 que declara os serviços de tecnologia da informação e comunicação (TIC) como serviços públicos sujeitos a regras administrativas mais rígidas.²⁷ O decreto também previa que não deveria haver aumento nos preços desses serviços, incluindo rádio e telefonia (telefonia móvel ou fixa residencial), até 31 de dezembro de 2020.
- No Peru, a Telefonica, Facebook, Grupo BID e o Banco de Desenvolvimento da América Latina (CAF) se associaram para criar o projeto Internet para Todos (IpT). A partir de 2020, o projeto conectou mais de 1,5 milhão de peruanos em áreas rurais com tecnologia 4G. Para 2021, o objetivo é fornecer acesso à Internet a 30.000 comunidades rurais.²⁸ Outro objetivo é expandir o projeto para outros países da América Latina e do Caribe.²⁹ Isso

26 L. Robinson and others, "Digital inclusion across the Americas and the Caribbean", *Social Inclusion*, vol. 8, No. 2, 2020.

27 Argentina, "Decreto 690/2020", *Boletín Oficial de la República Argentina*, 21 de agosto de 2020. Disponível em: <<https://www.boletinoficial.gob.ar/detalleaviso/primera/233932/20200822>>. Disponível em: 09 mai 2021.

28 Banco de Desenvolvimento da 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 maio de 2020: Disponível em: <<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/>>. Acesso em: 09 mai 2021.

29 Banco Interamericano de Desenvolvimento (BID), "Internet para Todos: helping Latin America log on", 2020. Disponível em: <<https://www.iadb.org/en/improvinglives/internet-para-todos-helping-latin-america-log>>. Acesso em: 09 mai 2021.

demonstra o potencial das parcerias público-privadas para o desenvolvimento da Internet na região.

- O programa de inclusão digital do Estado Plurinacional da Bolívia inclui a participação de cidadãos voluntários em apoio às atividades em andamento nas comunidades locais.³⁰
- Em 2015, o Brasil lançou o projeto “Amazônia Conectada”, com o objetivo de expandir a tecnologia de banda larga na Amazônia. Embora tenham sido feitos progressos com a infraestrutura da Internet, o projeto foi alvo de críticas consideráveis e foi avaliado negativamente pelo Tribunal de Contas da União (TCU) devido a falhas técnicas e de implementação.³¹
- Em 2019, o Setor de Desenvolvimento de Telecomunicações das Nações Unidas (ITU-D) envolveu 75 líderes indígenas em toda a Argentina, República Bolivariana da Venezuela, Chile, Colômbia, Costa Rica, Equador, El Salvador, Guatemala, Honduras, México, Nicarágua, Panamá, Paraguai, Peru e Estado Plurinacional da Bolívia no desenvolvimento de capacidades com foco em ferramentas inovadoras.³²

A inclusão digital ainda é um grande desafio na América Latina e no Caribe e uma prioridade quando se discute a regulação da Internet. Deverá ser dada especial atenção à camada de infraestruturas da Internet, onde a natureza transfronteiriça da rede se depara com as necessidades básicas de desenvolvimento local. Mas poderia haver margem para uma maior cooperação para desenvolver soluções e formas inovadoras de combater o fosso digital? Uma maior integração na região tem o potencial de fomentar o desenvolvimento e o compartilhamento de boas

30 Estado Plurinacional da Bolívia, “Bolívia: Decreto Supremo nº 3900, 8 de mayo de 2019”, maio 2019. Disponível em: <<https://www.lexivox.org/norms/BO-DS-N3900.html>>. Acesso em: 09 mai 2021. Ver também: Electronic Government and Information and Communications Technologies Agency (AGETIC), ‘Decreto Supremo N° 3900’, 10 de junho de 2019. Disponível em: <<https://digital.gob.bo/2019/06/contenido-libre/>>. Acesso em: 09 mai 2021.

31 A. B. Gomes, F. Duarte e P. Rocillo, Inclusão digital como política pública: Brasil e América do Sul em perspectiva, Belo Horizonte, Instituto de Pesquisa em Internet & Sociedade (IRIS), 2020. Disponível em: <<https://irisbh.com.br/publicacoes/inclusao-digital-como-politica-publica-brasil-e-america-do-sul-em-perspectiva/>>. Acesso em: 09 mai 2021.

32 International Telecommunication Union (ITU), “Indicadores de nuestros programas de capacitación para el fortalecimiento de los pueblos indígenas”. Disponível em: <<https://www.itu.int/en/ITU-D/Digital-Inclusion/Indigenous-Peoples/Pages/Indicadores.aspx>>. Acesso em: 09 mai 2021.

práticas na superação da desigualdade digital, bem como de conectar mais pessoas a uma única Internet global.

B. Um cenário tecnológico em mudança

As percepções de como a Internet afetou quase tudo, desde as atividades cotidianas triviais até os blocos de construção das relações internacionais, mudaram drasticamente nas últimas décadas. A América Latina e o Caribe têm sua própria parcela de peculiaridades que convidam a uma análise mais aprofundada de como os países da região integraram o componente digital em suas estratégias nacionais e internacionais. Quanto o acesso à Internet mudou a vida dos cidadãos nos países da América Latina e do Caribe? Quem são os atores que moldam as políticas digitais na região e como eles afetam governos, empresas e indivíduos através das fronteiras nacionais?

1. MUDANÇAS NAS PERCEPÇÕES: DA EUFORIA TECNOLÓGICA AO TECHLASH

Para que a Internet nos conectasse a todos, alguns argumentaram que nenhuma regulação deveria ser permitida no ciberespaço. Em 1996, o conhecido documento *Uma Declaração da Independência do Ciberespaço*, de John Perry Barlow, traçou uma linha entre os Estados como “gigantes cansados de carne e aço” e o ciberespaço como “a nova casa da Mente”.³³ Proclamando as virtudes decorrentes da existência de um espaço virtual para o livre fluxo de informação, Barlow instou os Estados a não interferirem no desenvolvimento da rede através de normas de qualquer espécie.

O debate sobre a regulação da Internet mudou desde o final da década de 1990. Em termos gerais, a euforia tecnológica da época de Barlow deu lugar a uma percepção mais dura de como a Internet pode ser usada para cometer crimes e espalhar desinformação, afetando enormemente o exercício dos direitos fundamentais e corroendo o discurso político. Aquilo que começou como euforia se transformou em *techlash*, envolvendo esforços regulatórios significativos.

33 J. P. Barlow, “A Declaration of the Independence of Cyberspace”, 8 Fev 1996. Disponível em: <<https://www.eff.org/pt-br/cyberspace-independence>>. [Versão em português: <<https://www.nic.br/publicacao/uma-declaracao-de-independencia-do-ciberespaco/>>]. Acesso em: 09 mai 2021.

O início da década de 2020, no entanto, trouxe um marco importante. À medida que a luta contra a COVID-19 forçou os países a fechar fronteiras e impor bloqueios, foi a Internet que serviu de tábua de salvação, permitindo que famílias, empresas e governos continuassem a se comunicar durante tempos difíceis. Não podemos voltar ao período de euforia, mas o pêndulo parece estar balançando novamente e a percepção pública do papel que a Internet desempenha na vida das pessoas pode passar por outra transformação.³⁴

Por mais paradoxal que possa parecer, o fechamento de fronteiras para conter o vírus foi acompanhado por um aumento do nível de atividade on-line de indivíduos, empresas e autoridades. Milhares de serviços públicos e privados foram forçados a entrar no digital, a fim de continuar atendendo ao público em geral.

Muitos países recorreram à prestação de serviços on-line, desde benefícios emergenciais até ações públicas básicas do dia a dia. Mesmo as legislaturas e os magistrados de muitos países transferiram suas atividades para a Internet. No setor privado, muitas empresas têm oferecido seus serviços on-line para sobreviver, transferindo todos os funcionários cujas atividades podem ser realizadas fora de suas instalações físicas para o trabalho remoto. De repente, milhões de pessoas e milhares de empresas tiveram que se adaptar à era digital.

A Internet ganhou relevância e importância, mostrando seus aspectos positivos e muitas de suas complexidades. Por um lado, as pessoas conseguiram manter algum grau de relações interpessoais por causa disso. Por outro, elas se tornaram mais vulneráveis à desinformação, fraude e crimes cibernéticos, também devido ao fato de que a Internet se tornou a única opção de acesso a uma série de serviços tradicionalmente prestados off-line.

2. O TRANSNACIONALISMO É UMA NOVA DINÂMICA EMERGENTE

Outro aspecto que a pandemia deixou bem claro é que as fronteiras são uma construção. Elas também são porosas. A globalização,

34 A Rede de Políticas Internet & Jurisdição preparou três documentos de definição de escopo abordando, respectivamente, acesso a dados de usuários, desafios de moderação de conteúdo e abusos no nível do sistema de nomes de domínios, no contexto da pandemia de COVID-19. Ver: <<https://www.internetjurisdiction.net/publications>>. Acesso em: 09 mai 2021.

que em muitos aspectos depende da forma como a humanidade lida com a geografia, tem sido apresentada sob uma luz diferente, através de um constante fluxo internacional de informações e serviços.³⁵ Apesar das fronteiras reais estarem fechadas, a Internet permite que as comunicações e os dados entrem e saiam. Nossas experiências compartilhadas durante este tempo reafirmaram, assim, uma conclusão que pode parecer evidente: a Internet transformou o transnacionalismo em uma nova dinâmica emergente.

A América Latina e o Caribe abraçaram, em muitos aspectos, tal fenômeno. A natureza sem fronteiras da Internet criou um ambiente perfeito para as ideias alcançarem um público mais amplo. Também para os negócios, os países da região têm servido como campo de prova para numerosas soluções inventivas para os mais diversos desafios. Para grandes multinacionais e *start-ups* promissoras, a região continua a oferecer muitas oportunidades.

No entanto, a viabilidade dessas oportunidades depende, por vezes, da estrutura regulatória nacional e regional. Decidir como misturar inspiração estrangeira com inovação regional é o primeiro passo para entender como abordar as políticas para a Internet na América Latina e no Caribe.

3. MULTINACIONAIS ESTRANGEIRAS SÃO INFLUENTES NA REGIÃO

Empresas multinacionais de muitos países estão competindo pela atenção dos cidadãos da América Latina e do Caribe e fazem parte de todas as camadas do mercado, desde a infraestrutura até os serviços de mídia de última geração. O aumento da conectividade (discutido na seção III.A) fez da América Latina e do Caribe um dos maiores mercados do mundo. A conectividade móvel tem aumentado a disponibilidade dos serviços de Internet para uma crescente maioria de seus cidadãos.³⁶

Empresas com uma presença global têm se envolvido tanto no desenvolvimento do próprio mercado quanto na exploração das oportunidades que a América Latina e o Caribe têm a oferecer. Isso trouxe problemas próprios pois as questões transfronteiriças

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

36 Internet Live Stats, "Internet users by country (2016)". Disponível em: <<https://www.internetlivestats.com/internet-users-by-country/>>. Acesso em: 09 mai 2021.

acabam se tornando uma ocorrência cada vez mais normal. Enquanto no mercado físico uma empresa precisaria de uma presença robusta no território para fornecer bens e serviços, as atividades on-line não necessariamente exigem isso. Certos serviços podem ser disponibilizados sem que o provedor tenha qualquer presença na região. As empresas estrangeiras podem até mesmo não ter representação legal, menos ainda uma sede ou incorporação em qualquer um dos países da região. No entanto, essas empresas ainda podem ter um efeito sobre os mercados ou consumidores da América Latina e do Caribe, com o que é mais difícil lidar.

Os consumidores, acostumados a exigir seus direitos nos tribunais dos seus próprios países, acabam por perceber o quanto isso pode ser desafiador quando há um componente internacional para as suas reivindicações. A necessidade de cooperação jurídica internacional aumenta porque os serviços diplomáticos podem estar envolvidos e diferentes padrões de procedimentos legais e de proteção podem ser destacados.

Na outra ponta do espectro, as empresas estrangeiras podem não saber necessariamente em que países seus clientes vivem ou podem não ter as ferramentas para verificar isso (ver seção V.B.1 para mais informações sobre tecnologias de geolocalização). Como consequência, a não-observância é uma possibilidade com várias consequências práticas.

Do ponto de vista da administração pública, se as empresas quiserem participar do mercado da região, terão que cumprir suas leis e estar disponíveis para adjudicação local. Nem as expectativas da empresa que presta serviços de Internet nem a conveniência (ou não) do local de jurisdição são geralmente levadas em consideração.

Além disso, as empresas multinacionais são frequentemente confrontadas com a situação de ter que cumprir obrigações legais contraditórias. O alcance extraterritorial ou global de certas leis nacionais, ordens judiciais ou pedidos administrativos pode conduzir a tais conflitos. As empresas são, então, colocadas em uma posição em que têm de escolher qual obrigação legal cumprirão.³⁷

Na América Latina e no Caribe, esse fenômeno manifestou-se particularmente em matéria de acesso a dados armazenados no

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

exterior. As empresas multinacionais, particularmente aquelas que prestam ou utilizam serviços em nuvem, armazenam dados fora do território onde prestam serviços, e, assim, potencialmente submetem os dados a pelo menos duas jurisdições. Sempre que o país onde os dados estão localizados tem o que é chamado de regra de bloqueio, que só permite o acesso a dados em condições particulares, a possibilidade de conflito entre leis das jurisdições onde os serviços são prestados (ou os dados recolhidos) aumenta.

Tais confrontos levaram a casos em que empresas multinacionais se recusaram a cumprir ordens válidas emitidas sob as leis internas de países da América Latina e do Caribe. Isso levou à aplicação de instrumentos legais que vão desde a cobrança de grandes multas às empresas-mãe e contra ativos no país até acusações criminais contra funcionários de corporações multinacionais.

Os atores entrevistados apontaram para a harmonização das leis, a coordenação dos esforços e a cooperação entre os Estados como formas de lidar com esses desafios. Padrões harmonizados levam a resultados previsíveis, tornando as empresas mais preparadas para cumprir as regulações. Da mesma forma, mediante a coordenação e cooperação, os Estados podem obter melhores resultados e nutrir um ambiente de conformidade geral.

4. O AMBIENTE DE NEGÓCIOS PARA START-UPS NA REGIÃO É VARIÁVEL

O outro lado da moeda é que várias empresas na América Latina e no Caribe estão aproveitando a oportunidade para se expandir para outros mercados, tanto dentro quanto fora da região. Há uma mistura crescente de oportunidades emergentes para que as empresas estabelecidas e *start-ups* se beneficiem das características transnacionais da Internet. Um especialista entrevistado mencionou a existência de pontos em comum inexplorados na região que poderiam permitir a rápida expansão dos mercados, tais como traços culturais ibéricos comuns e parentesco linguístico.

Há, portanto, uma tendência dos produtores regionais de bens e serviços a participarem da economia de plataforma, beneficiando-se dos mercados internacionais (plataformas de comércio eletrônico) que proporcionam acesso aos clientes no

exterior. Dessa forma, mesmo as pequenas e médias empresas podem tornar-se exportadoras e encontrar novos clientes fora de seus mercados habituais.³⁸

Não só o ambiente empresarial doméstico está se expandindo em muitos dos países da região, particularmente no que diz respeito às *start-ups* tecnológicas, mas várias empresas estão se expandindo em toda a região e até internacionalmente. Um especialista observou que várias *start-ups* financeiras e projetos relacionados à *blockchain* estão se expandindo rapidamente e enfrentando as dificuldades iniciais que isso traz (ver seção IV.C.4 para mais informações sobre tecnologia financeira (*fintech*)).

Entretanto, a maioria dos especialistas pesquisados (60,97%) considerou que os desafios legais são uma barreira para as empresas transfronteiriças da Internet, particularmente as pequenas e médias empresas (PMEs). Eles mencionaram que essas empresas regionais enfrentam vários desafios ao procurarem expandir, incluindo: (i) diferentes regulações e padrões, (ii) serem submetidas a tribunais em jurisdições inesperadas, (iii) obstáculos regulatórios, (iv) incoerência fiscal e (v) encargos logísticos e administrativos.

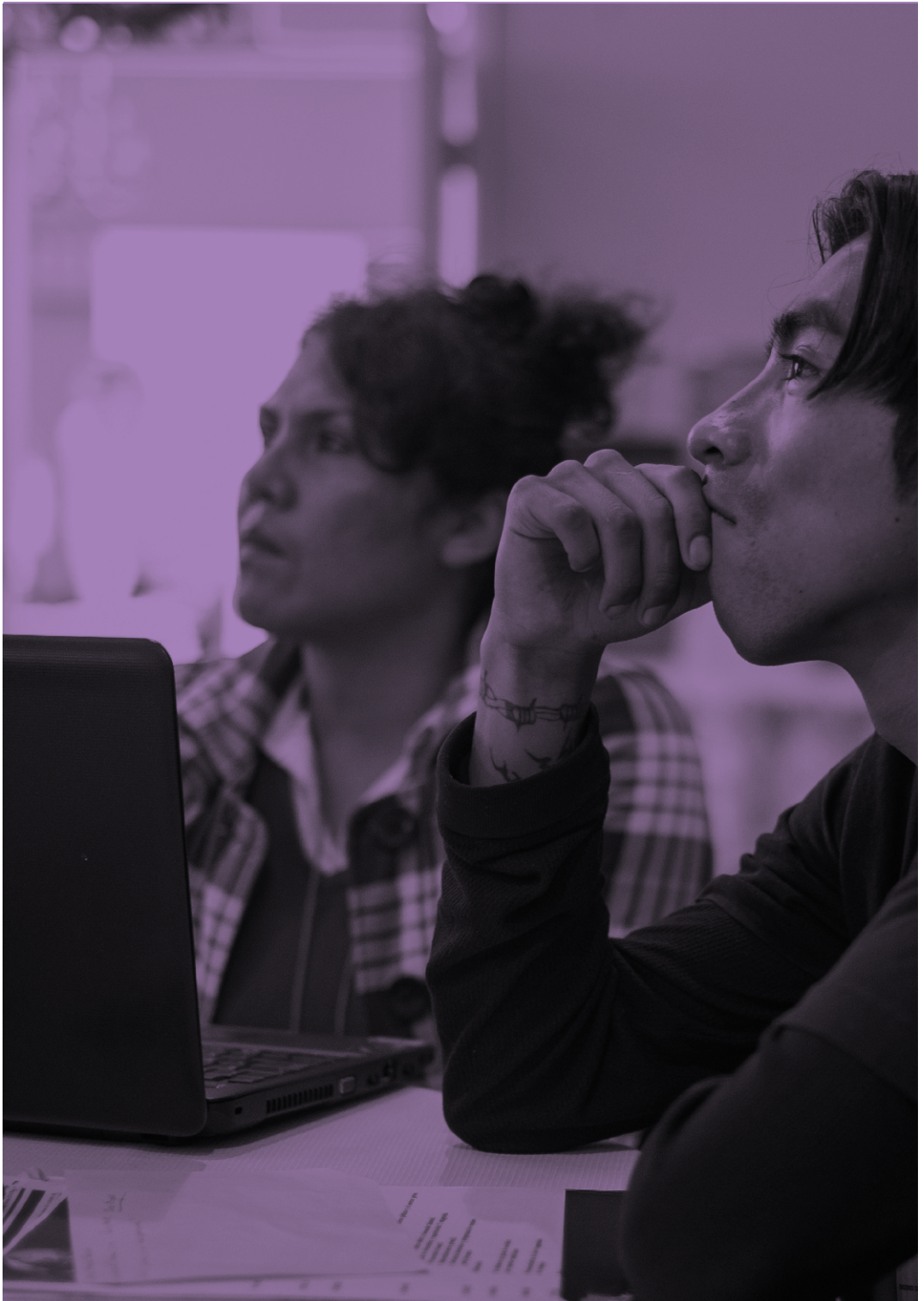
INFOGRÁFICO 4

Os desafios jurídicos transfronteiriços que afetam a Internet constituem um obstáculo para as pequenas e médias empresas (PME) na região.



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

38 Ver: S. Lund and J. Manyika, How Digital Trade is Transforming Globalisation, E15 Initiative, Geneva, International Centre for Trade and Sustainable Development (ICTSD)/World Economic Forum, 2016. Para obter dados específicos, ver: eBay "The State of Small Online Businesses: Worldwide Results from eBay's 5-Year Study". Disponível em: <<https://www.ebaymainstreet.com/policy-papers/state-small-online-businesses-worldwide-results-ebay%E2%80%99s-5-year-study>>. Acesso em: 09 mai 2021.



Ao discutir o novo papel que as empresas da região estão desempenhando e as oportunidades que elas têm on-line, é importante observar que os desafios legais transfronteiriços podem ou não ser um obstáculo competitivo. A região tem uma grande oportunidade de facilitar essa tendência expansionista através de maior cooperação e integração, que pode assumir a forma de um mercado único digital (tratado mais detalhadamente na seção IV.C.1).

C. Iniciativas regulatórias estrangeiras estão inspirando propostas regionais e nacionais

Embora a Internet não tenha sido projetada com as fronteiras dos países em mente, a regulação da rede tem um impacto que vai muito além das fronteiras de qualquer Estado. Esse impacto transfronteiriço pode surgir porque o âmbito da aplicação das políticas internas engloba frequentemente atividades que ocorrem além das fronteiras territoriais. As leis de um país também podem servir como modelos ou fontes de inspiração para outros.³⁹

A esmagadora maioria dos atores pesquisados disse que abordagens regulatórias estrangeiras impactaram os esforços internos na América Latina. Em números, 80,5% dos atores indicaram que as iniciativas regulatórias nacionais foram “enormemente” ou “muito” inspiradas, 17% que foram inspiradas “até certo ponto” e apenas 2,5% que foram “apenas ligeiramente” inspiradas por iniciativas estrangeiras. Nenhum dos atores afirmou no questionário que as iniciativas estrangeiras não eram uma fonte de inspiração. Em seus comentários, os atores observaram que as iniciativas originárias dos Estados Unidos e da Europa tiveram o maior efeito no desenvolvimento e na aplicação dos arcaouços jurídicos nacionais dos países da América Latina e do Caribe.

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

INFOGRÁFICO 4

Até que ponto as abordagens regulatórias em países e regiões estrangeiras, como a União Europeia ou os Estados Unidos, inspiram iniciativas nacionais sobre governança e regulamentação da Internet na América Latina e no Caribe?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

Os atores identificaram cinco razões para essa influência: (i) a afinidade social e cultural entre os Estados Unidos, Europa e América Latina e Caribe e as semelhanças entre seus sistemas jurídicos, tornando os tomadores de decisão mais dispostos a buscar inspiração nessas fontes; (ii) a natureza global da Internet, que cria pressão para a harmonização e torna importante olhar para abordagens fora da região; (iii) as obrigações dos tratados internacionais, que incentivam a consideração de soluções globais; (iv) a crença de que os países fora da região são mais experientes em tecnologias digitais e mais familiarizados com os problemas que elas podem trazer; e (v) o fato de que nem todos os países têm a capacidade técnica para desenvolver e implementar tais regulações, o que os torna receptivos aos mecanismos de cooperação técnica internacional através dos quais as iniciativas e abordagens internacionais podem operar, ajudando na implementação. Assim, a tendência geral é que as iniciativas internas de governança e regulação da Internet na América Latina e no Caribe sejam inspiradas por abordagens estrangeiras.

Como mencionado por um dos entrevistados: “Há sempre modas e a necessidade de seguir tendências”. Existe hoje uma grande consciência sobre temas como segurança cibernética, dados pessoais e privacidade, por exemplo. No entanto, nem tudo é sempre copiado da legislação de outros lugares. Houve esforços bilaterais: México-União Europeia, Argentina-União Europeia. A Lei de Neutralidade da Rede Chilena foi pioneira. O Marco Civil da Internet no Brasil também foi pioneiro. De qualquer forma, o debate é global.

1. AS INICIATIVAS DE POLÍTICAS TÊM PROLIFERADO À MEDIDA QUE AUMENTA O APETITE PARA REGULAR O CIBERESPAÇO

Existe atualmente um consenso de que é necessária alguma regulação para a Internet. No entanto, há menos consenso quando se trata dos tipos de complexidades que a regulação pode trazer. Como aponta o *Relatório de Status Global 2019* da Rede de Políticas Internet & Jurisdição, a questão não é tanto se a Internet deve ser regulada, mas como e por quem. Globalmente, houve um aumento nas formas de regulação, que podem incluir tratados internacionais, leis nacionais, regulações administrativas, decisões judiciais, códigos de conduta, diretrizes nacionais ou internacionais, declarações, normas técnicas, convenções, políticas da empresa e comunidade e obrigações contratuais. Estas iniciativas criaram uma intrincada colcha de retalhos de estruturas normativas, algumas das quais carecem de legitimidade, mas não deixam de ter impacto no panorama de políticas.

Os países da região da América Latina e do Caribe estão tendo que lutar com esta multiplicidade de iniciativas, nem todas de sua própria autoria. Três fenômenos importantes podem ser identificados entre as respostas dos atores.

Em primeiro lugar, há os desafios de conformidade que as empresas enfrentam quando se esforçam para compreender o quadro jurídico aplicável. Por conseguinte, a primeira questão que deve ser respondida é: qual é a legislação nacional aplicável a um caso específico?

Em segundo lugar, as regulações podem criar incerteza jurídica apenas por serem complexas e com várias camadas. Mesmo uma vez identificada a legislação nacional aplicável, uma infinidade de instrumentos legais tais como leis, decretos, portarias, decisões judiciais e outras fontes legais pode dificultar a navegação no arcabouço jurídico do país.

Em terceiro lugar, as ações regulatórias podem ter consequências não intencionais. Essas consequências podem surgir porque o equilíbrio entre diferentes regras e direitos não tem necessariamente um resultado predeterminado. É o caso das solicitações de provas eletrônicas de um provedor de serviços de nuvem, pois os dados podem ser cobertos por diferentes leis, dependendo de onde eles são armazenados. Pode também acontecer que um pedido infrinja algumas regras nacionais e os efeitos da sanção da empresa responsável pela infração sejam

sentidos muito além das fronteiras de um país. O bloqueio do aplicativo de mensagens WhatsApp no Brasil, que afetou usuários na Argentina e no Chile, é um exemplo disso (o bloqueio de aplicativos é discutido na seção V.B.4).

A profusão de regulações pode resolver alguns problemas, mas por si só é uma fonte de outros problemas. A maioria dos atores parece ser da opinião de que deve haver mais coordenação e cooperação em torno da formulação de políticas públicas para a Internet na América Latina e no Caribe e que certos tópicos são mais regulados do que outros.

2. INSPIRAÇÃO LEGISLATIVA E JUDICIAL: FERTILIZAÇÃO CRUZADA OU IMITAÇÃO?

A profusão de iniciativas regulatórias nacionais pode ocultar até que ponto a legislação estrangeira e as decisões judiciais promovem debates nacionais e regionais na América Latina e no Caribe. Os esforços internos podem mimetizar, imitar ou copiar diretamente abordagens e racionalidades originárias do exterior. A revisão da literatura e as contribuições dos atores pesquisados sugerem que existe uma linha tênue entre a fertilização cruzada e a imitação.

Essa tendência global de imitação é exemplificada por muitos casos em diferentes áreas da regulação da Internet, onde um esforço externo resultou em iniciativas nacionais ou regionais.

- Esse tem sido o caso da discussão sobre a neutralidade da rede nos Estados Unidos, com a abordagem da Comissão Federal de Comunicações (FCC) fornecendo a base para o debate sobre o assunto em toda a América Latina e o Caribe.⁴⁰
- O acórdão do Tribunal de Justiça da União Europeia no caso Costeja afirmando um “direito ao esquecimento” dividiu especialistas, países e tribunais da América Latina e do Caribe (ver seção IV.A.5 para mais informações sobre este tema).

40 Intervezes - Coletivo Brasil de Comunicação Social/Derechos Digitales, Neutralidad de red en América Latina: reglamentación, aplicación de la ley y perspectivas. Los casos de Chile, Colômbia, Brasil y México, São Paulo/Santiago, 2017. [Versão em português do relatório: Neutralidade de rede na América Latina: regulamentação, aplicação da lei e perspectivas – os casos do Chile, Colômbia, Brasil e México, 2017. Disponível em: <<https://intervezes.org.br/arquivos/interliv011nral2017.pdf>>]

- A aprovação e posterior entrada em vigor do Regulamento Geral de Proteção de Dados da União Europeia (GDPR, na singla em inglês) levaram muitos países a adotar nova legislação ou a embarcar em uma reforma do seu regime de proteção de dados. Não menos que quatro leis sobre proteção de dados foram aprovadas desde 2016 (o ano em que entrou em vigor do GDPR, e países como Argentina, Chile, Colômbia e Uruguai iniciaram revisões ou reformaram sua legislação de proteção de dados. Alguns países também decidiram introduzir nova legislação geral de proteção de dados, incluindo Barbados, El Salvador e Jamaica, para citar apenas alguns.

A recente adoção da nova Diretiva da União Europeia sobre Direitos Autorais estimulou a discussão sobre regimes de responsabilidade de plataformas por violações de direitos autorais de terceiros (ver seção IV.C.2), com impactos já sendo sentidos na América Latina e no Caribe.

Essa influência está tendo consequências positivas e negativas na região. Por um lado, os atores salientaram que elas servem como um instrumento de harmonização: ao fazer, em um país, iniciativas semelhantes às de outros lugares, passam a ter um efeito coordenador. Curiosamente, iniciativas nos países da América Latina e do Caribe também podem estar influenciando outros dentro da região, aumentando a consonância entre diferentes países.

No entanto, os atores manifestaram a preocupação de que, em algumas circunstâncias, soluções estrangeiras não seriam adequadas ao contexto social, econômico e cultural da região. Um mencionou que, mesmo que as soluções fossem sólidas, elas podem não ser aplicadas no nível ideal. As instituições encarregadas podem não possuir recursos ou autoridade para atingir os objetivos das políticas a que se destinavam.

Uma consideração final é que, se a lógica subjacente à iniciativa estrangeira for controversa ou invasiva, sua adoção na região pode ter um efeito semelhante, potencialmente levando a conflitos.

D. Preocupações com a influência internacional e pluralidade normativa

Em muitas áreas do direito, a legislação nacional continua a ser a principal forma de regulação. Para a Internet, no entanto, dificilmente pode-se dizer que este é o único elemento que

regula e orienta a conduta on-line. Outros fatores como acordos internacionais, iniciativas regulatórias estrangeiras (com e sem efeitos extraterritoriais), normas técnicas e específicas do setor, diretrizes nacionais e internacionais, termos de uso e serviço das empresas, diretrizes de comunidade e decisões arquiteturais (codificação) também pesam significativamente no ambiente on-line.

O ciberespaço como rede é influenciado e impactado por seus múltiplos elementos. A circulação rápida (“viralidade”) não é apenas uma característica associada a vídeos, imagens e informações. Uma pluralidade de iniciativas normativas pode causar um “efeito borboleta” na regulação da Internet, impactando a conduta on-line em todo lugar.

Como mencionado no *Relatório de Status Global 2019* da Rede de Políticas Internet & Jurisdição, um modelo regulatório de tipo piramidal⁴¹, com regulamentos rígidos emitidos pelo Estado, não pode explicar a profusão de iniciativas normativas e seu impacto relativo. Na região da América Latina e do Caribe, os países são atraídos e céticos em relação às iniciativas estrangeiras. O que não pode ser negado é que uma pluralidade de esforços, não confinados aos Estados ou à própria região, está influenciando e governando a conduta on-line.

1. AS REGRAS SÃO DEFINIDAS PARA (E POR) ATORES INTERNACIONAIS GRANDES E BEM ESTABELECIDOS

Os atores entrevistados e que responderam ao questionário apontaram que nem todas as iniciativas tiveram o mesmo impacto e nem todos os atores tiveram a mesma posição no processo de tomada de decisão. Eles enfatizaram que, em muitas circunstâncias, Estados e empresas maiores tinham mais voz e maior influência na definição de regras para a Internet do que as menores.

As iniciativas normativas parecem sofrer de uma atração gravitacional por atores maiores. Quanto maior o ator, mais fortemente as regras são moldadas às suas ambições. As normas parecem ser concebidas para satisfazer os interesses das nações e das empresas maiores e estão menos adaptadas às circunstâncias das PMEs ou das empresas em países menores ou menos desenvolvidos.

A maioria dos atores considera esta tendência um obstáculo

41. F. Ost e M. van de Kerchove, *De la pyramide au réseau?: pour une théorie dialectique du droit*, Bruxelles, Université Saint-Louis - Bruxelles, 2002.

às PMEs e às empresas dos Estados menores competindo internacionalmente. Alguns entrevistados mencionaram que a maioria das nações e empresas de menor porte não possuíam recursos ou capital humano necessários para cumprir complexos conjuntos de regulações.⁴²

Quanto às transações transfronteiriças e iniciativas internacionais, apesar de alguns sucessos recentes, as empresas da região ainda são substancialmente afetadas pela falta de harmonização e coordenação de esforços. As empresas latino-americanas e caribenhas que atuam transnacionalmente tendem a ser financiadas por capital de risco estrangeiro ou adquiridas por empresas estrangeiras com maior capitalização.

Essa situação se reflete na pesquisa, sendo que a maioria dos atores considera que os desafios legais transfronteiriços que afetam a Internet são uma barreira para as PMEs da região.

2. O PAPEL CRESCENTE DAS NORMAS DA EMPRESA: O STATUS "CONSTITUCIONAL" DOS TERMOS DE SERVIÇO

As empresas, especialmente as plataformas, estabelecem suas próprias regras para regular o comportamento on-line. Reconhece-se amplamente que a escolha da arquitetura (código) impacta e regula a conduta dos atores on-line e pode afetar o que é possível na atividade on-line. Sem um botão "curtir", os usuários não podem expressar sua satisfação ou falta dela com algum comentário on-line, foto ou vídeo.⁴³ Se uma mensagem só pode ser enviada a uma pessoa em vez de a cinco ou vinte, trata-se de um desincentivo para divulgar informações (e desinformação).⁴⁴ Esses são apenas dois exemplos de como o código pode afetar a conduta on-line.

No entanto, o código é apenas uma das dimensões em que as

42 S. Hubbard, "Fake news is a real antitrust problem", *Antitrust Chronicle*, vol. 1, No. 3, dezembro de 2017.

43 Ver, por exemplo: SPIEGEL International, "'Like' button battle: Facebook agrees to voluntary privacy code", 8 Set 2011. Disponível em: <<https://www.spiegel.de/international/germany/like-button-battle-facebook-agrees-to-voluntary-privacy-code-a-785190.html>>. Acesso em: 09 mai 2021.

44 Esta é uma referência às mudanças que o WhatsApp Messenger fez em sua arquitetura para limitar as oportunidades de reenvio de mensagens que já foram encaminhadas muitas vezes. Ver: The Guardian, "WhatsApp to impose new limit on forwarding to fight fake news", 7 Abr 2020. Disponível em: <<https://www.theguardian.com/technology/2020/apr/07/whatsapp-to-impose-new-limit-on-forwarding-to-fight-fake-news>>. Acesso em: 09 mai 2021.

plataformas influenciam o comportamento. Os termos de serviço e os padrões de comunidade fornecem uma base normativa para que os provedores de serviços de Internet atuem como reguladores e policiem o ciberespaço. Dependendo da plataforma, eles podem ser sofisticados o suficiente para criar instituições que se assemelham às de um Estado.⁴⁵ O Facebook instituiu recentemente um órgão quase-judicial paralelo chamado Comitê de Supervisão, que funcionará como órgão de apelação para as suas decisões de moderação de conteúdo.⁴⁶ As plataformas de comércio eletrônico possuem mecanismos de resolução de litígios, estendendo-se à proteção de direitos autorais.⁴⁷ O Reddit permite que as comunidades elaborem seu próprio conjunto de regras e aconselha-as a ter moderadores ativos e procedimentos de recursos.⁴⁸ A lista de plataformas e suas ações semelhantes às das instituições estatais está crescendo.

As iniciativas supracitadas deram origem a termos de serviço que se assemelham a constituições. Apesar de serem normas da empresa, elas parecem ser a primeira camada normativa aplicável. Se a conduta on-line for considerada ofensiva ou prejudicial, espera-se que plataformas atuem, ações tais que se baseiam principalmente em seus termos de serviço. Ao mesmo tempo, as plataformas estão cada vez mais afirmando os direitos de seus usuários de forma quase “constitucional”.

Essas tendências têm uma série de consequências abrangentes. A primeira (discutida na seção IV. A abaixo) é que as plataformas estão sendo conclamadas a assumir mais responsabilidade pelo que acontece dentro de seus domínios. A segunda é que as plataformas são capazes de agir através das jurisdições, já que as regras de conduta não são limitadas pelas fronteiras dos Estados e uma empresa pode alterar os termos de todas as suas plataformas em todos os países ou em uma seleção deles.

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

46 Ver on-line: <<https://about.fb.com/news/2020/05/welcoming-the-oversight-board/>>. Acesso em: 09 mai 2021.

47 Ver on-line: <<https://www.mercadolivre.com.br/brandprotection/enforcement>>. Acesso em: 09 mai 2021.

48 Ver: <<https://www.redditinc.com/policies/moderator-guidelines-for-healthy-communities>>. Acesso em: 09 mai 2021.

A terceira é que as empresas podem acordar entre si normas particulares comuns e implementá-las de forma coordenada, sem a necessidade de coordenação do Estado.⁴⁹

Há outro conjunto de implicações: essas normas de empresas carecem de qualquer processo de aprovação pública ou democrática e podem potencialmente entrar em conflito com as regulações nacionais. Na América Latina e no Caribe, houve mais de um desses confrontos. O caso que tem atraído a atenção internacional tem sido o que diz respeito às ordens de permanência (*stay-up*), decisões judiciais que requerem que as plataformas mantenham o conteúdo on-line, mesmo que ele alegadamente viole os termos de serviço.⁵⁰ No lado positivo, essas normas de empresa podem facilitar a harmonização das normas internacionais. Sua aplicação transnacional conduz ao debate internacional e pode levar a uma resposta coordenada ou harmonizada. No entanto, os atores pesquisados chamaram a atenção para a falta de transparência e clareza na definição desses termos. Nos comentários, um ator observou que o DNA global de tais termos de serviço – estabelecidos principalmente por plataformas multinacionais – pode não estar bem preparado ou não ser suficientemente flexível para abranger a diversidade e as idiossincrasias presentes nas realidades locais, particularmente em nações menores e em desenvolvimento, como as da América Latina e do Caribe. Poder-se-ia dizer que existe o risco de que as “constituições” das plataformas globais não sejam suficientemente inclusivas para as realidades locais dos países menores.

E. O papel da territorialidade e o exercício

49 Isto foi feito recentemente através de uma declaração conjunta contra a propagação da desinformação em relação à pandemia da COVID-19. Ver: <<https://techcrunch.com/2020/03/16/facebook-reddit-google-linkedin-microsoft-twitter-and-youtube-issue-joint-statement-on-misinformation/>>. Acesso em: 09 mai 2021.

50 Ver: Waqas, "Brazil will sue Facebook for blocking picture of indigenous woman", HackRead, 20 de abril de 2015. Disponível em: <<https://www.hackread.com/facebook-blocking-brazil-indigenous-picture/>>. Acesso em: 09 mai 2021. Para uma análise das decisões de manutenção de conteúdo (*stay-up*), ver: D. Keller, *Dolphins in the Net: Internet Content Filters and the Advocate Generals Glawischig-Piesczek v. Facebook Ireland Opinion*, Stanford Center for Internet and Society, 2019.

da soberania são diferentes em uma rede global

O conceito de territorialidade tem sido difícil de conciliar com algumas das características do ciberespaço. A territorialidade deve cumprir a função de princípio orientador, tanto para fornecer motivos para que um Estado exerça o poder quanto para definir a extensão geográfica desse poder, colocando um limite topográfico à soberania do Estado.

A Internet, por outro lado, foi desenvolvida para ser sem fronteiras, ou pelo menos neutra, de modo que as informações possam fluir apesar das barreiras geográficas. Assim, uma jurisdição territorial perde seu significado preciso em um ciberespaço que não deveria espelhar as divisões políticas subjacentes do Estado no mundo físico. Os países não podem, no entanto, ignorar o fato de que certas ações on-line impactam tanto a propriedade quanto as pessoas localizadas no mundo físico e dentro do seu próprio território. O aumento da interconexão dos mundos físico e virtual dissipou os contornos entre ambos, levando a regulações estatais geograficamente mais extensas.

Os Estados têm procurado utilizar a localização de pessoas, dispositivos ou servidores como pontos de ancoragem territorial para justificar o exercício da jurisdição on-line. Em certa medida, a jurisdição está vinculada em relação a atos que podem estar legalmente ligados a mais de um território e potencialmente a mais de uma jurisdição. A consequência é que, em alguns casos, os Estados têm ou um alcance excessivo, estabelecendo jurisdição onde existe apenas uma tênue ligação, ou um alcance insuficiente, o que significa que certas vítimas ficam sem recurso.

A América Latina e o Caribe têm uma relação única com o conceito jurídico de territorialidade, sendo considerado o berço do princípio de não-intervenção.⁵¹ Não é por acaso que a definição mais famosa de “Estado” vem de uma convenção elaborada na região, a Convenção sobre Direitos e Deveres dos Estados de 1933. A Convenção define o território como um dos seus

51 Para uma visão geral do desenvolvimento do princípio, ver: J. P. Scarfi and A. Tillman (eds.), *Cooperation and Hegemony in US-Latin American Relations*, New York, Palgrave Macmillan, 2016. Para uma das primeiras declarações sobre o assunto, ver: A. Alvarez, “Latin America and international law”, *American Journal of International Law*, vol. 3, No. 2, abril de 1909.

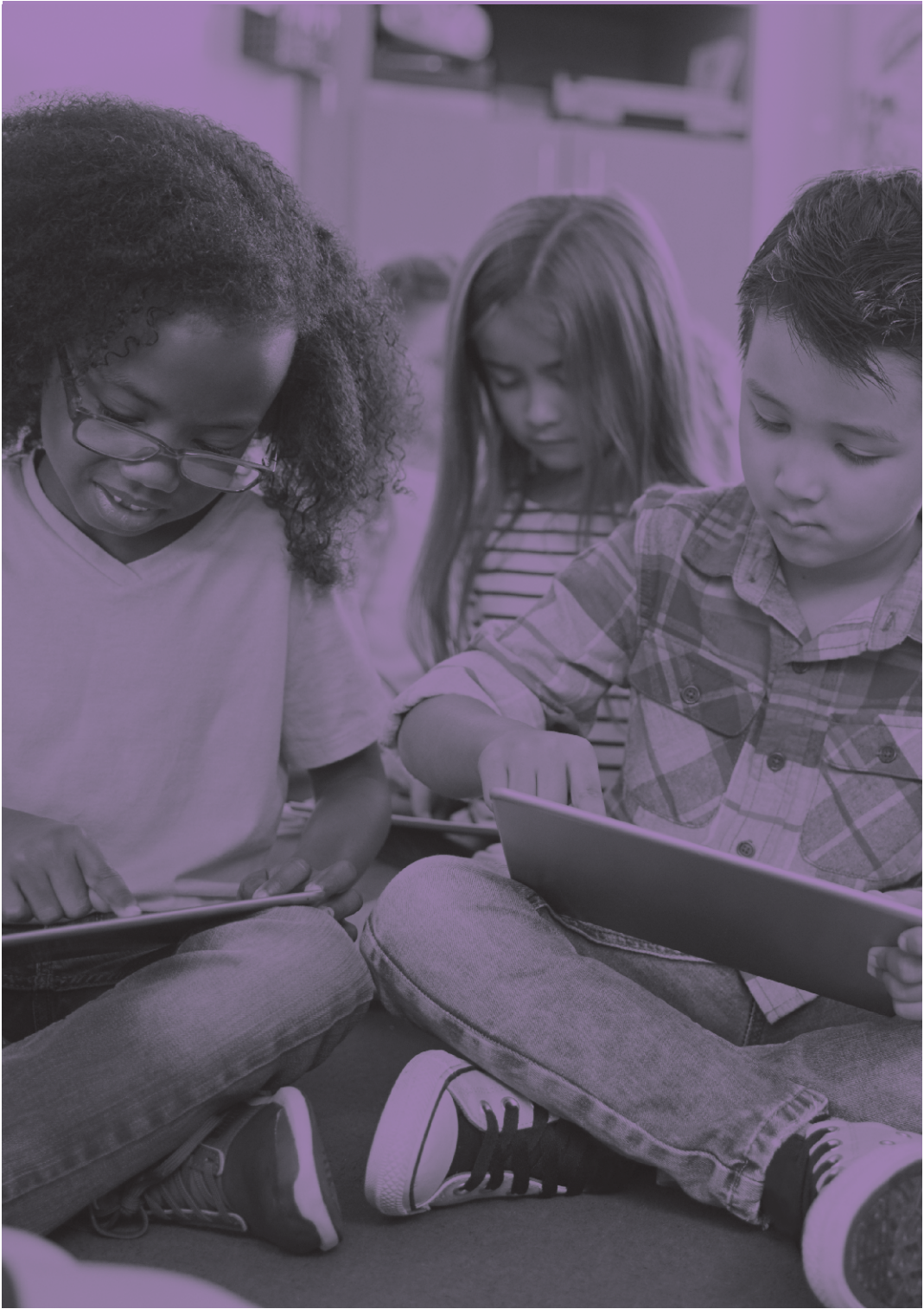
elementos constituintes.⁵² Esse contexto tem implicações para a compreensão de certos tipos de questões temáticas como sendo abrangidos pela jurisdição interna de um Estado. É contra esse pano de fundo que os Estados da região conceituam a jurisdição territorial, incluindo a jurisdição on-line.

O fato de que a América Latina e o Caribe serem o berço do princípio da não-intervenção dá o tom ao entendimento de jurisdição aqui. A abordagem da região é ilustrada pelo tratamento de empresas estrangeiras que parecem não seguir as leis nacionais. A escalada para o bloqueio de aplicativos ou a detenção de executivos de empresas parece ser uma consequência desta noção: a lei de um Estado tem de ser respeitada dentro do seu território. Da mesma forma, com as provas eletrônicas (*e-evidence*), parece que as agências nacionais de execução da lei ficam perplexas quando não têm acesso a dados sobre crimes cometidos dentro de suas fronteiras.

Em algumas circunstâncias, a lógica da jurisdição é territorialmente dependente e independente ao mesmo tempo. Há um apetite para regular o que acontece ou impacta no território da América Latina e Caribe, mas a jurisdição pode ser posteriormente estendida além da região, sendo exemplos a aplicação extraterritorial de regulações de proteção de dados e condições para transferências transfronteiriças de dados pessoais. Em casos de difamação e moderação de conteúdo, as ordens de exclusão (*take-down*) geralmente se concentram na remoção do conteúdo ou até mesmo no fechamento de contas, com um alcance global e não apenas local.

Há uma tendência abrangente para a jurisdição se concentrar mais na localização do comportamento ou da conduta do que no local onde os dados são armazenados. No entanto, a localização e o movimento dos dados ainda são, por vezes, fatores relevantes a serem considerados.

52 Ver: <<https://treaties.un.org/doc/Publication/UNTS/LON/Volume%20165/v165.pdf>>. Acesso em: 09 mai 2021.



1. O ALCANCE CRESCENTE EXTRATERRITORIAL DAS LEIS NACIONAIS

Os Estados estão cada vez mais insatisfeitos com a forma como a fluidez do ambiente on-line, no qual não existem barreiras claras à interação transfronteiriça, é explorada para contornar a legislação nacional. Compreensivelmente, eles querem uma regulação que desencoraje tal comportamento. A lógica é que as leis devem ser respeitadas tanto no ambiente on-line quanto no mundo off-line. Cada Estado se considera habilitado a governar o que acontece e o que está disponível on-line. Existe a percepção de que se o comportamento tem impacto ou efeito sobre o território de um Estado, então ele deve estar dentro da jurisdição desse Estado.

Na ausência de instrumentos internacionais ou regionais vinculativos, muitos Estados, inclusive Estados da região, acabam reivindicando ampla jurisdição, seja através de novas leis, seja através da interpretação expansionista das leis existentes. Na América Latina e no Caribe, esta tendência global é particularmente visível nas áreas de proteção de dados (seção IV. 3) e acesso às provas eletrônicas pelas agências de execução da lei (seção IV.2).

Na opinião dos atores que responderam ao questionário, essa abordagem da regulação (aumentando o alcance geográfico das leis nacionais) pode levar à execução arbitrária ou à frustração. Esta última surge porque a execução real pode ser difícil ou quase impossível em certos casos. Com relação à primeira, as pessoas podem se surpreender de serem processadas em um país distante por violar uma lei local de forma inconsciente. Outro aspecto é que o escopo da regulação pode ser tão amplo que pode ser desafiador determinar quais comportamentos serão abrangidos, caso em que a execução pode parecer discricionária.

Uma tendência global paralela detectada pelos países da América Latina e do Caribe é a promulgação de regulações com multas elevadas por não conformidade. As ameaças de sanções são usadas para incentivar o cumprimento. A preocupação expressa pelos Estados latino-americanos e caribenhos é que, com sanções menos proibitivas, suas leis passarão a um segundo plano e poderão ser ignoradas pelos atores internacionais. A dificuldade com essa lógica parece ser que ela motiva outros países a fazerem o mesmo e a competirem para impor as maiores multas e as sanções mais severas, impedindo o fluxo de dados e negócios.

2. EXTRATERRITORIALIDADE TRAZ DESAFIOS DE EXECUÇÃO

Demandas por jurisdições mais amplas podem ser difíceis de serem cumpridas, e quanto mais amplas forem, mais difícil será a sua execução. Reivindicar jurisdição não é o mesmo que ser capaz de executá-la. Um Estado que aplica suas leis com base em um vínculo ténue – aquele entre a conduta e o próprio Estado – pode achar difícil que suas ações sejam aceitas como legítimas. Da mesma forma, afirmar a jurisdição sem poder executá-la pode ser prejudicial às percepções da eficácia da norma e contrariar o objetivo de incentivar o cumprimento.

Afirmações amplas de jurisdição podem, no entanto, serem uma estratégia em si mesmas. Pode deixar claro que uma determinada questão afeta um importante valor social, ou seja, que o Estado se preocupa com ela. Essa estratégia pode ser concebida como uma forma de estabelecer linhas jurisdicionais e articular um ponto de vista sobre a extensão dos interesses de um Estado.

Um Estado também pode se ver na necessidade de confiar na cooperação com outro Estado. Os ativos tangíveis ou dados podem estar noutro país e, portanto, fora do alcance do país de execução ou não realisticamente acessíveis a ele. Isso cria o potencial para conflitos regulatórios, constituindo tanto um desafio para a cooperação interestatal como uma oportunidade para encontrar soluções mutuamente aceitáveis.

Isso é reforçado pelo fato de que, uma vez que a jurisdição é afirmada, o país tem que estar disposto a vê-la retribuída: outros Estados podem reivindicar uma jurisdição igualmente ampla. A América Latina e o Caribe têm uma tradição de reciprocidade internacional. Assim, as afirmações estrangeiras de jurisdição provavelmente serão correspondidas pelos países da região.

Vários atores assinalaram que nem todos os países da América Latina e do Caribe tinham a mesma capacidade de estender sua jurisdição para além de suas fronteiras. Eles observaram as diferenças de tamanho, peso econômico e poder entre os países da região e destacaram os potenciais obstáculos aos esforços para corresponder à ação externa. Assim, uma afirmação de jurisdição extraterritorial ou ampla por um país da América Latina ou do Caribe pode ser considerada insatisfatória quando se trata de execução da lei.

Isso também funciona do outro lado. Alguns dos atores no questionário mencionaram que nações menores poderiam ficar

sem poder quando nações maiores flexionassem seus músculos legais. O caso do jogo de azar on-line apresentado por Antígua e Barbuda perante a Organização Mundial do Comércio (OMC) é um exemplo ilustrativo.⁵³ Embora a disputa tenha sido finalmente decidida pelo Órgão de Apelação em favor dos Estados Unidos, teria sido um desafio para a nação caribenha afirmar seus direitos e salvaguardar seus negócios frente a uma norma norte-americana com efeito transfronteiriço.⁵⁴ Na realidade, mesmo que legal do ponto de vista da OMC, o resultado acabou sendo uma “medida destruidora de mercado”⁵⁵ e o serviço não pôde mais continuar.

F. Espera-se que os intermediários desempenhem novos papéis

Os intermediários são muito diversos: mecanismos de busca, redes de mídia social, plataformas de comércio eletrônico ou *streaming*, mecanismos de pagamento digital e muitos outros atores que facilitam as atividades mais conhecidas on-line. À medida que a Internet se tornou mais popular, os intermediários ganharam importância, tornando-se integrados na rotina dos usuários da Internet. Eles se tornaram os condutores que conectam diferentes pessoas e empresas e facilitam as transações. O resultado foi uma mudança na morfologia do ciberespaço: outrora uma “região selvagem” largamente auto-organizada, tornou-se uma multiplicidade de “jardins” organizados e mais ou menos murados.

O grau de dependência dos intermediários da Internet é contestado. É claro, porém, que eles representam uma parte significativa do tráfego e, do ponto de vista do usuário, simplificam o uso da Internet. Com esta centralidade recentemente alcançada, surgiu uma discussão sobre os papéis destes atores e sua responsabilidade pelo que acontece no ciberespaço, a opinião sendo de que os intermediários deveriam compartilhar mais o fardo de supervisionar o que acontece on-line.

53 Ver: <https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm> Acesso em: 09 mai 2021.

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

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

1. UMA RESPONSABILIDADE CADA VEZ MAIOR ESTÁ SENDO COLOCADA SOBRE OS OPERADORES PRIVADOS

Tradicionalmente, os países consideram que os intermediários da Internet merecem proteção legal devido à sua importante função como encruzilhada, passagens ou locais de encontro para os usuários da Internet. No entanto, uma série de situações envolvendo pornografia infantil, violência explícita, terrorismo, divulgação de imagens privadas (“pornografia de vingança”), campanhas de desinformação (*fake news*) e infrações de direitos autorais em larga escala, entre outras, têm exposto as deficiências dessa abordagem se forem seguidas sem salvaguardas.⁵⁶

Países de toda a América Latina e do Caribe têm se movimentado no sentido de atribuir um papel maior na governança da Internet a operadores privados. A questão tornou-se mais importante para os países da região, particularmente nos campos de discurso de ódio e conteúdo nocivo, desinformação (principalmente no contexto das eleições), violações de direitos autorais, venda de produtos falsificados, privacidade e proteção de dados.

Os intermediários acabam desempenhando funções quase estatais, por exemplo, em seu papel quase judicial de decidir quando retirar conteúdo e suspender ou encerrar as contas dos infratores de direitos autorais reincidentes. São eles que são chamados a decidir sobre a legalidade do conteúdo, se é sátira política (permitido) ou conteúdo difamatório (não permitido), por exemplo. Eles podem tomar tais ações voluntariamente, de acordo com seus termos de serviço, ou sob a coação de normas nacionais e decisões judiciais.

Os regimes legais que até recentemente protegiam os intermediários de processos judiciais deram lugar a abordagens mais matizadas.⁵⁷ Na América Latina e no Caribe, as estratégias têm variado de país para país. A República Bolivariana da Venezuela e Cuba parecem estar entre os mais rigorosos, tendo promulgado legislação que cria obrigações para os provedores de serviços de

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

57 Como exemplo, o Marco Civil da Internet brasileiro (Lei nº 12.965 de 2014) consagra uma disposição de “porto seguro” (*safe harbour*). A Lei chilena nº 20430 de 2010 reformou a legislação de direitos autorais do país para fornecer um “porto seguro” contra a responsabilidade de terceiros em relação aos direitos autorais da Internet.

Internet (PSIs) monitorar e “regular” discursos. Eles também conferem amplos poderes aos órgãos públicos, que podem até mesmo fechar intermediários que desrespeitem sua autoridade.⁵⁸ Outros países têm procurado regular áreas específicas como o discurso do ódio, tornando os intermediários responsáveis se não removerem um conteúdo considerado ilegal. Outras abordagens têm sido a emissão de códigos de conduta ou a celebração de acordos administrativos com intermediários.

Alguns dos entrevistados salientaram que esta tendência poderia ter implicações transfronteiriças. Isso é particularmente grave nos casos em que as empresas não têm outra escolha senão cumprir a regulação de um Estado (incluindo ordens judiciais) sob o risco de violar o regime legal de outro, se houver um conflito de leis. As consequências podem não ser fáceis de prever, especialmente para um país latino-americano ou caribenho. As empresas podem implementar uma abordagem de denominador comum mais rigorosa, limitando potencialmente a liberdade de expressão na região, ou, quando pressionadas, podem optar por não implementar leis locais, o que poderia impactar a legitimidade jurídica interna.

Os atores observaram que exigir que as plataformas desempenhem esse papel como guardiões da Internet poderia corroer a legitimidade e a confiança nas instituições do Estado e o senso de justiça, enquanto em situações eleitorais poderia impactar o processo democrático. Isso significa que as empresas são encarregadas de definir quais informações podem circular e como. No entanto, a desinformação também pode ter um efeito prejudicial nas eleições democráticas.

2. OS INTERMEDIÁRIOS SÃO CADA VEZ MAIS SOLICITADOS A FORNECER DADOS PARA APOIAR INVESTIGAÇÕES

Quando os telefones se tornaram um importante meio de comunicação, as escutas telefônicas se tornaram um valioso recurso de investigação para os agentes da lei, dando-lhes acesso de fato às comunicações dos suspeitos de crimes e fornecendo

58 Ver: <<http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf>>. Acesso em: 09 mai 2021.; e "Office of the Special Rapporteur for Freedom of Expression, Special Report on the Situation of Freedom of Expression in Cuba", Organization of American States (OAS), 2018.

uma maneira de aprender como os crimes eram planejados, quando aconteceriam ou como tinham sido discutidos. Mesmo a “*mens rea*” poderia ser melhor determinada, através da escuta de conversas que teriam sido privadas se não fossem pistas que as ligassem a investigações criminais.

A Internet mudou a situação. Uma miríade de serviços diferentes desempenha a mesma função, permitindo que as informações sobre conduta ilegal sejam compartilhadas, quer ocorram on-line ou off-line. As técnicas da era do telefone não podem ser facilmente transferidas para a Internet. O apoio às funções investigativas passou dos intermediários que fornecem a infraestrutura para aqueles que fornecem diretamente certas aplicações muito populares da Internet. Esses intermediários da Internet são aqueles capazes de fornecer acesso à informação. Isso levanta pelo menos quatro questões principais: acesso a dados armazenados; acesso a dados em massa (dados gerais ou bases de dados); o uso de criptografia; e as categorias de serviços de dados que as empresas podem ser obrigadas a coletar e fornecer.

Como muitos intermediários estão ampliando seu alcance global, todas essas questões tendem a ter um componente transfronteiriço. Quanto ao acesso aos dados, diferentes regras internas regem quando e como os agentes de execução da lei podem receber esses dados. Se forem armazenadas no exterior, os desafios tendem a ser ainda maiores. Para contornar as complexidades da cooperação judiciária internacional, os países da região estão contemplando a ideia de impor obrigações aos intermediários da Internet. Tais obrigações incluem: (i) localização de dados; (ii) uma presença física no país ou nomeação de um representante; e (iii) a obrigação de fornecer acesso a dados, remoto ou não. Os dois últimos pontos são objeto do artigo 32 do projeto de Lei das Fake News aprovada pelo Senado brasileiro, por exemplo.⁵⁹

59 O projeto também continha uma obrigação de localização de dados, mas isso foi retirado antes da votação no Senado. Ver: <<https://www.bloomberg.com/news/articles/2020-07-01/brazil-s-senate-approves-draft-bill-to-rein-in-on-fake-news>>. Acesso em: 09 mai 2021. Para o texto original do projeto de lei (em português) e discussão sobre ele, ver: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/141944.%20%20F>>. Acesso em: 07 mai 2021. Para uma discussão sobre o impacto do art. 32, ver: C. A. Souza e C. Perrone, " 'Fake news' e acesso a dados armazenados no exterior", JOTA, 2020. Disponível em: <<https://www.jota.info/coberturas-especiais/liberdade-de-expressao/fake-news-e-acesso-a-dados-armazenados-no-exterior-30062020>>. Acesso em: 09 mai 2021.

Os intermediários também estão sendo obrigados a fornecer acesso não apenas a dados específicos, mas a grandes volumes de dados. Em muitas circunstâncias, eles estão sendo solicitados a disponibilizar um palheiro inteiro na busca de uma agulha mal definida. Tais solicitações foram feitas, sem sucesso, em relação aos dados de localização de torres de telefonia móvel nos Estados Unidos, por exemplo.⁶⁰ Na América Latina e no Caribe, no entanto, houve casos de tribunais superiores que concederam solicitações muito amplas, mesmo que esta não seja a resposta padrão.⁶¹ A pandemia da COVID-19 ampliou o escopo de tais solicitações do campo de investigações criminais para a aplicação de políticas públicas (pelo menos durante a pandemia).⁶²

As obrigações impostas aos intermediários em apoio às investigações criaram outro dilema difícil. Vários intermediários usaram ou pretendem usar mais técnicas de preservação da privacidade envolvendo diferentes tipos de criptografia, inclusive a criptografia de ponta-a-ponta [*end-to-end encryption* ou E2EE]. Assim, poderia se tornar mais difícil (ou às vezes até mesmo tecnicamente impossível) cumprir tal papel, pois as informações podem não ser acessíveis.

Nessas circunstâncias, os países da América Latina e do Caribe, como muitos de seus pares internacionais, estão tentando obrigar os intermediários a não usar técnicas criptográficas ou a fornecer uma chave. Eles estão até mesmo encontrando outras formas de obter acesso à informação, como o uso de um intruso não identificado. Isso é semelhante ao que aconteceria numa situação de escuta telefônica, mas com consequências potencialmente muito mais amplas, uma vez que todas as conversas poderiam ser ouvidas, não apenas as específicas, e isso poderia ser feito por qualquer pessoa capaz de acessá-las, e não apenas pelos agentes da lei.

60 Supremo Tribunal dos Estados Unidos, *Carpenter v. Estados Unidos*. Disponível em: <<https://www.scotusblog.com/case-files/cases/carpenter-v-united-states-2/>>. Acesso em: 09 mai 2021.

61 Ver: <<https://www.telesurenglish.net/news/Google-Must-Share-Data-Related-To-Marielle-Franco-Murder-Case-20200827-0004.html>>. Acesso em: 09 mai 2021.

62 M. P. Canales, *La herejía tecno-optimista florece en pandemia: un repaso crítico a las tecnologías disponibles*, *Derechos Digitales*, 2020. Disponível em: <<https://www.derechosdigitales.org/wp-content/uploads/herejia-tecno-optimista.pdf>>. Acesso em: 09 mai 2021.

Outra estratégia proposta na região tem sido a de que os serviços de mensagens colem mais informações para que isso seja acessível em futuras investigações. Dois formatos foram sugeridos: solicitando a identificação de indivíduos, restringindo, assim, o anonimato on-line, ou exigindo que intermediários rastreiem certas categorias de mensagens, particularmente aquelas com conteúdo amplamente distribuído.⁶³

Todas essas novas funções exigem disposições substanciais para equilibrar os direitos e podem ter um impacto significativo nas ações dos intermediários da Internet, especialmente quando prestam serviços globalmente. Especialistas entrevistados apontaram a necessidade de harmonizar as necessidades legítimas da execução da lei com a organização da Internet, os direitos dos usuários e o alcance global dos provedores de serviços de Internet.

3. A TRANSPARÊNCIA É ESSENCIAL PARA AUMENTAR A CONFIANÇA, MAS A IMPLEMENTAÇÃO VARIA

As maiores funções atribuídas aos intermediários da Internet também aumentaram as demandas por mais transparência em relação aos seus procedimentos, decisões e ações. A necessidade de uma maior moderação do conteúdo ou do comportamento pelas plataformas também cria incentivos para que elas confiem em algoritmos automatizados de tomada de decisão, a fim de atender às expectativas de que o conteúdo e o comportamento controversos serão analisados. Trata-se de um cenário em que a discussão da transparência nos procedimentos, critérios e justificativas para as decisões se torna mais importante.

A questão foi agora abordada, em certa medida, em relação à proteção de dados e à discussão sobre o direito a uma explicação quando ocorre a moderação automatizada. Muitas empresas emitem os próprios relatórios de transparência e estabelecem alguns de seus procedimentos em seus termos de uso ou regras de comunidade.⁶⁴

63 Ver: <<https://www.eff.org/deeplinks/2020/06/5-serious-flaws-new-brazilian-fake-news-bill-will-undermine-human-rights>>. Acesso em: 09 mai 2021. Ver também: <<https://blog.mozilla.org/netpolicy/2020/06/29/brazils-fake-news-law-harms-privacy-security-and-free-expression/>>. Acesso em: 09 mai 2021.

64 Ver: <<https://rankingdigitalrights.org/>>. Acesso em: 09 mai 2021.

A questão de saber se isso deve ser tratado através de regulações vinculativas ou através de códigos de conduta, correção ou autorregulação ainda está aberta para discussão. Na América Latina e no Caribe, várias organizações da sociedade civil são da opinião que mais transparência é essencial. Os países abordaram esta questão propondo regras vinculativas,⁶⁵ mas estas têm de ser cuidadosamente elaboradas, uma vez que podem ter um impacto prejudicial no desenvolvimento de novas soluções e impor um fardo de altos custos e burocracia às empresas nascentes e às *start-ups*.

Como princípio, a transparência é importante para o desenvolvimento de uma boa governança da Internet na América Latina e no Caribe. No entanto, se for imposta aos intermediários da Internet, é necessário ter em conta as diferentes variáveis em funcionamento na região, a capacidade dos intermediários para lidar com ela e os efeitos no desenvolvimento da inovação e de *start-ups*.

4. CRESCENTE ATENÇÃO TEM SIDO DADA AO DEVIDO PROCESSO NAS ATIVIDADES DE MODERAÇÃO DE CONTEÚDO

Outro aspecto significativo da mudança do papel dos intermediários é a importância de proporcionar oportunidades para que as decisões de moderação de conteúdo sejam contestadas. A rapidez e a generalização dos serviços de Internet significam que a revisão subsequente pelo Judiciário pode ser inacessível aos usuários ou causar dificuldades ou danos significativos. Tornar os atores privados, ou seja, os intermediários da Internet, responsáveis por suas ações ou fornecer uma forma de os usuários protestarem, apelarem ou se defenderem pode se mostrar crucial para a preservação de valores sociais e direitos fundamentais importantes (abordados na seção V.A.5).

É certamente o caso que, assim como a transparência, impor legalmente procedimentos desafiadores pode levar a situações difíceis, nas quais nem todos os intermediários serão capazes de lidar com as exigências que lhes são impostas. É importante,

65 O projeto da Lei das *Fake News* proposto no Brasil contém disposições sobre transparência para redes sociais e serviços de mensagens. Para o texto do projeto de lei, ver: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>>

no entanto, que certo nível de revisão esteja disponível em princípio, particularmente do ponto de vista da proteção dos cidadãos na América Latina e no Caribe. Um dos especialistas pesquisados observou que a região tende a consumir tecnologias desenvolvidas fora dela e que estas não estão adaptadas às circunstâncias dos cidadãos latino-americanos e caribenhos. Fornecer um espaço para que os resultados sejam contestados e revistos é, portanto, uma forma de tornar os serviços mais sólidos, mais compatíveis com as necessidades dos indivíduos e mais consistentes com seus direitos e com o contexto em que vivem. Isso deve ser visto como uma oportunidade de adaptação.

As consequências de tais novas funções para os intermediários, sejam elas mudanças na responsabilidade civil, regulação adicional ou a imposição de novas obrigações, levantam, por sua vez, novas questões transnacionais, inclusive sobre como melhor preservar os direitos humanos e a natureza global da Internet, com as oportunidades de inovação que ela proporciona. Os países da América Latina e do Caribe, como outros Estados ao redor do mundo, devem equilibrar as vantagens e desvantagens dos novos papéis dos intermediários da Internet com os métodos usados para mitigar os riscos.





02 . **Principais tendências da atualidade na América Latina e no Caribe**

A. Expressão

1. FAKE NEWS E DESINFORMAÇÃO

1.1. A ação regulatória está aumentando

A Internet diminuiu as barreiras para os cidadãos que desejam se informar e se expressar. Ao mesmo tempo, a desinformação – disseminação em massa de informações falsas, fora de contexto ou destinadas a causar danos – também se tornou mais prevalente.

A velocidade, o volume e a “viralidade” dos fluxos de informação os tornam difíceis de controlar. O uso de dados pessoais nas campanhas de microdirecionamento⁶⁶ e o efeito que alguns algoritmos têm de criar filtros bolha⁶⁷ ou câmaras de eco, com as pessoas apenas vendo, ouvindo e compreendendo o que querem ou esperam, aumentam a necessidade de acesso a informações confiáveis. A capacidade das pessoas de formar seus pensamentos, ideias e opiniões sem serem indevidamente influenciadas está em risco.

Essa situação é particularmente aguda durante eleições. Os atores pesquisados repetiram muitas das preocupações que os atores internacionais têm transmitido. A desinformação pode levar à polarização,⁶⁸ silos de informação, supressão eleitoral⁶⁹ e manipulação da agenda política, entre outros impactos negativos.⁷⁰ Um dos atores mencionou que ataques e manipulação eram o trabalho de atores tanto estrangeiros quanto domésticos que utilizam a rede para semear intencionalmente a divisão e a polarização.

Como afirmou um ator entrevistado:

-
- 66 Ver: <https://datasociety.net/wp-content/uploads/2018/10/DS_Digital_Influence_Machine.pdf>. Acesso em: 09 mai 2021.
- 67 E. Pariser, *The Filter Bubble: What the Internet Is Hiding from You*, New 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, No. 2, 2018. Disponível em: <<https://www.tandfonline.com/doi/full/10.1080/21670811.2017.1345645>>. Acesso em: 09 mai 2021.
- 70 Organization of American States (OAS), *Guide to Guarantee Freedom of Expression Regarding Deliberate Disinformation in Electoral Contexts*, 2019. Disponível em: <https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf>. Acesso em: 09 mai 2021.



A interferência eleitoral é uma grande ameaça ao direito universal das pessoas de participarem no processo democrático. Essa é uma questão que tanto governos quanto empresas de tecnologia estão enfrentando para fazer face aos desafios das últimas táticas e tecnologias de interferência eleitoral. Vale ressaltar que os ataques e a manipulação coordenada não são mais provenientes de potências estrangeiras malignas sozinhas. Cada vez mais, a interferência nos processos eleitorais é usada pelos atores domésticos como forma de semear divisão e polarização em contextos autoritários e democráticos.

Os países da América Latina e do Caribe responderam a essas tendências de várias maneiras. A maioria deles tem seguido a tendência de produzir regulações que ou criminalizam a disseminação da desinformação, geralmente sob o título de *fake news*, ou impõem um dever para que as plataformas de Internet sejam mais proativas em seu monitoramento do conteúdo, muitas vezes transferindo o ônus da responsabilidade para os intermediários de Internet.

A ameaça de criminalização tem sido a estratégia utilizada no Peru, por exemplo, onde o Ministério da Justiça e dos Direitos Humanos afirmou que o conteúdo que manipula os cidadãos, a fim de obter um benefício ou perturbar a ordem pública deve ser punido como crime.⁷¹ Outros países, entre eles, Argentina, Colômbia, Costa Rica, México e Uruguai, iniciaram discussões públicas sobre o assunto, a fim de orientar as plataformas para integrar iniciativas de verificação de fatos em sua arquitetura.⁷²

-
- 71 Peru, Gestión, "Personas que difundan noticias falsas podrían recibir hasta 6 años de prisión", 8 de abril de 2020. Disponível em: <<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-nndc-noticia/?ref=gesr>>. Acesso em: 09 mai 2021.
- 72 A plataforma pública de checagem de fatos "Confiar", da Argentina, é um exemplo. Ver: <www.argentina.gob.ar/noticias/confiar-la-plataforma-oficial-para-combatir-la-infodemia>. Acesso em: 09 mai 2021. Além disso, a organização de checagem de fatos "Chequeado", criada na Argentina, coordenou a coalizão LatamChequea com 35 organizações em toda a América Latina. Ver: <<https://chequeado.com/latamcoronavirus/>>. Acesso em: 09 mai 2021.

O Brasil ampliou o leque de táticas implementadas, com o STF⁷³ e o Congresso⁷⁴ iniciando separadamente investigações sobre indivíduos e redes coordenadas que supostamente disseminavam discurso de ódio e desinformação. Além disso, um longo projeto de lei que pretende regular as *fake news* foi aprovado pelo Senado Federal em 30 de junho de 2020.⁷⁵ Na verdade, o projeto de lei regula uma grande variedade de assuntos, revendo substancialmente o papel desempenhado pelas plataformas de mídia social e serviços de mensageria. Elas agora seriam obrigadas a rastrear mensagens amplamente distribuídas (virais), exigir a identificação adequada sob certas circunstâncias, moderar o conteúdo, estabelecer um procedimento de defesa e recurso muito detalhado, e fornecer acesso aos dados, não importando sua origem ou seu armazenamento. O projeto de lei também propõe a criação de um órgão consultivo e cria sanções severas para a não observância das disposições (ver seção V.A.4 para mais informações sobre essa tendência).

Há pouca dúvida de que a luta contra a desinformação tem impactos transfronteiriços: as empresas que oferecem bens e serviços transfronteiriços terão de adaptar suas políticas para lidar com estas novas responsabilidades.

1.2 Bots automatizaram notícias falsas e desinformação

O comportamento orgânico e autêntico pode levar a uma ampla difusão da informação, mas quando ela é acoplada a ferramentas automatizadas ou *bots*, contas criadas artificialmente que são parcial ou completamente controladas por software de automação, o potencial para atingir um público muito mais amplo aumenta.⁷⁶

73 Supremo Tribunal Federal do Brasil, "Inquérito 4781". Disponível em: <<http://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=444198&ori=1>>. Acesso em: 09 mai 2021.

74 Senado Federal do Brasil, "Comissão Parlamentar Mista de Inquérito - Fake News": Disponível em: <<https://legis.senado.leg.br/comissoes/comissao?0&codcol=2292>>. Acesso em: 09 mai 2021.

75 Ver: <<https://www.bloomberg.com/news/articles/2020-07-01/brazil-senate-approves-draft-bill-to-rein-in-on-fake-news>>. Acesso em: 09 mai 2021. Para o texto original do projeto de lei e discussão sobre ele, ver: <<https://www25.senado.leg.br/web/atividade/materias/-/materia/141944>>. Acesso em: 09 mai 2021.

76 C. Shao and others, "The spread of low-credibility content by social bots", *Nature Communications*, vol. 9, 2018. Disponível em: <<https://www.nature.com/articles/s41467-018-06930-7>>. Acesso em: 09 maio 2021.

Essas ferramentas também direcionam o tráfego (e a atenção das pessoas) para questões e tipos particulares de informação e podem fomentar uma sensação artificial de popularidade e relevância.⁷⁷ Assim, a automação acrescenta mais “aceleração” à névoa de difusão viral de informações e, portanto, à desinformação.

Por um lado, o uso de tais ferramentas de automação pode ter um impacto positivo ao empurrar ideias e vozes importantes, porém marginalizadas, para frente do debate público. Por outro lado, entretanto, esta mesma função pode ser usada para manipular informações, ampliar seu alcance, criar uma sensação de apoio ou consenso onde não há nenhum e obscurecer fatos importantes.⁷⁸ Em outras palavras, estas ferramentas podem ser amplificadores de desinformação.⁷⁹

O uso de *bots* e automação em plataformas globais levanta uma série de outras questões transfronteiriças. Do ponto de vista da origem, tais ferramentas podem ser estrangeiras. *Bots* podem ser desenvolvidos em países estrangeiros, ou podem funcionar fora do país-alvo, talvez dentro de uma rede internacional coordenada.

Na América Latina e no Caribe,⁸⁰ por exemplo, houve relatos de *bots* usando o *script* cirílico durante as eleições brasileiras, o que parece indicar uma origem russa.⁸¹ Em outro caso, des-

77 J. Bayer and others, “Disinformation and propaganda - Impact on the functioning of the Rule of Law in the EU and its Member States”, HEC Paris Research Paper, 2019. Disponível em: <<http://dx.doi.org/10.2139/ssrn.3409279>>. Acesso em: 09 mai 2021.

78 P. Howard, *How Political Campaigns Weaponize Social Media Bots*, 2018. Disponível em: <<https://spectrum.ieee.org/computing/software/how-political-campaigns-weaponize-social-media-bots>>. Acesso em: 09 mai 2021. Ver também: 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 e P. Howard “Troops, trolls and troublemakers: a global inventory of organized social media manipulation”, Oxford Computational Propaganda Research Propaganda Project, 2017. Disponível em: <<http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/07/Troops-Trolls-and-Troublemakers.pdf>>. Acesso em: 09 mai 2021.

80 Para um relatório geral, ver: Atlantic Council, *Disinformation in Democracies: Strengthening Digital Resilience in Latin America*, 2019. Disponível em: <<https://www.atlanticcouncil.org/wp-content/uploads/2019/09/Disinformation-in-Democracies.pdf>>. Acesso em: 09 mai 2021.

81 Ver: <<http://dapp.fgv.br/pesquisa-da-fgv-dapp-revela-vinculos-entre-robos-e-campanhas-da-eleicao-presidencial-de-2014/>>. Acesso em: 09 mai 2021.

cobriu-se que *bots* brasileiros foram usados em uma eleição presidencial mexicana.⁸²

As plataformas globais também descobriram redes de contas automatizadas envolvendo o que é chamado de “comportamento não autêntico coordenado”. Em casos significativos, o comportamento originou-se num país, mas teve o seu foco noutra.⁸³

Uma segunda questão diz respeito às investigações sobre esse uso estrangeiro de ferramentas automatizadas ou *bots*. Em muitos casos, eles podem violar as leis eleitorais e até mesmo penais sobre a divulgação de desinformação. Informações importantes podem ser mantidas por plataformas estrangeiras que podem ou não ter um representante legal no país em questão. Os dados também podem não estar prontamente disponíveis ou podem ser armazenados em servidores no exterior.

Embora a atenção tenha sido voltada para como lidar com essas técnicas nacionalmente, os aspectos internacionais podem ter um grande impacto em futuras regulações para refrear notícias falsas e desinformação. Elas destacam a necessidade de cooperação e coordenação, a fim de encontrar soluções para campanhas de desinformação on-line.

Nas eleições municipais do Rio de Janeiro de 2016, foi utilizada uma mistura de ferramentas automatizadas e comportamento autêntico coordenado. Um recurso chamado “doe um like” foi implementado pela campanha oficial de um candidato. Consistiu em um pedido para que as pessoas apoiassem o candidato doando a capacidade de “curtir” e compartilhar conteúdo por um período de três meses. Uma vez aceito, uma ferramenta capturaria o perfil e a senha do usuário e seria usada para divulgar o conteúdo do candidato. Assim, as contas reais pertencentes a pessoas reais seguiriam e, sob um regime automatizado coordenado, participariam da campanha de um candidato.⁸⁴

82 Ver: <https://horizontal.mx/bots-su-deteccion-y-la-participacion-en-las-campanas-electorales-en-mexico/#_edn1>. Acesso em: 09 mai 2021.

83 Ver: <<https://about.fb.com/news/2020/07/removing-political-coordinated-inauthentic-behavior/>> Acesso em: 09 mai 2021. Ver também: <<https://www.theverge.com/2018/10/25/18021456/twitter-q3-2018-earnings-9-million-mau-decline>>. Acesso em: 09 mai 2021.

84 D. Arnaudo, “Computational propaganda in Brazil: social bots during elections”, Oxford Computational Propaganda Research Project, 2017. Disponível em: <<https://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Brazil-1.pdf>>. Acesso em: 09 mai 2021.

INFOGRÁFICO 5

A natureza transfronteiriça da Internet facilita a interferência externa no processo democrático?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

2. DIFAMAÇÃO

2.1. Os desafios transfronteiriços estão aumentando

Respeito e proteção à honra pessoal e reputação são encontrados nas leis de uma infinidade de países com diversos antecedentes culturais. Como um valor central compartilhado, a difamação é ilegal tanto off-line quanto on-line. A implementação, interpretação e alcance do conceito, no entanto, variam consideravelmente. A Internet aumentou a importância dessas diferenças legais e criou mais potencial para conflitos entre jurisdições.

Os desafios transfronteiriços surgem especialmente em três circunstâncias: (i) quando o conteúdo publicado em um país tem impacto em outro; (ii) quando o meio empregado para publicação está fora do país onde a pessoa ofendida normalmente vive ou trabalha, seja porque a empresa que presta o serviço está estabelecida em outro país ou porque os servidores estão em outro país; e (iii) quando o dano à honra ou reputação de uma pessoa ocorre em mais de uma jurisdição.

O *Relatório de Status Global 2019* apontou que isso não é algo novo. Devido ao alcance geográfico potencialmente global da Internet, a difamação transfronteiriça tem sido uma ocorrência comum on-line. No caso *Dow Jones v. Gutnick*, por exemplo, o Supremo Tribunal da Austrália teve que decidir se a publicação tinha ocorrido onde o artigo foi postado on-line ou onde foi baixado.⁸⁵ Esse tribunal foi um dos primeiros a entender que uma publicação on-line pode difamar alguém além das fronteiras.

85 Ver: High Court of Australia, *Dow Jones and Company Inc v. Gutnick* [2002] HCA 56: <<http://eresources.hcourt.gov.au/showCase/2002/HCA/56>>. Acesso em: 09 mai 2021.

A questão dos danos não foi de todo resolvida, uma vez que o demandante limitou sua reivindicação aos danos sofridos no local onde o processo foi ajuizado, a Austrália, que também era o país onde ele estava principalmente preocupado em proteger sua reputação. Entretanto, a porta foi deixada aberta para uma discussão muito mais ampla sobre se ele poderia potencialmente processar em mais de uma jurisdição, procurando os tribunais mais favoráveis, e se ele poderia reclamar por danos que poderiam ter ocorrido globalmente em qualquer ou em todas as jurisdições. De certa forma, a questão é saber se uma reputação pode ser internacional e os danos devem também ter em conta uma potencial dimensão extraterritorial. As decisões sobre o assunto podem interferir potencialmente em disposições legais de outros países e os direitos dos seus cidadãos. Se um tribunal decidir conceder indenizações globalmente, pode levar em consideração países onde esse conteúdo não seria considerado difamatório, restringindo indiretamente a liberdade de expressão.

Essa questão pode ter mais implicações transfronteiriças. Por exemplo, na América Latina e no Caribe, os pedidos de indenização em casos de difamação têm sido frequentemente acompanhados de pedidos de remoção ou retificação do conteúdo considerado difamatório. Os demandantes frequentemente procuram intermediários na Internet, que posteriormente são colocados na posição de terem de cumprir ordens judiciais e decidir o seu âmbito territorial.

Esse foi o caso do serviço blogger.com do Google. Os tribunais colombianos⁸⁶ e mexicanos⁸⁷ instruíram o Google a remover posts considerados difamatórios. No Brasil, foi ordenado ao Facebook que removesse o conteúdo e retirasse todo um perfil considerado difamatório para um candidato político.⁸⁸ Cada um desses casos

86 O Tribunal Constitucional colombiano decidiu que o Google deveria excluir um blog "blogger.com" que continha declarações difamatórias. Ver: I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publicationsretrospect#article-6369_2017-10>. Acesso em: 09 mai 2021.

87 Rede de Políticas Internet & Jurisdição, Dezembro de 2017. Mexican Supreme Court rejects Google's argument that Mexican courts do not have jurisdiction over the platform. I&J Retrospect Database. Disponível em: <<https://www.internetjurisdiction.net/publications/retrospect#eyJ0b3Yl6lJlWmJAtMDMifQ==>>. Acesso em: 09 mai 2021.

88 Ver: <<https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24horas/62909>>. Acesso em: 09 mai 2021.

contribuiu para um entendimento de que tal conteúdo pode ser afetado mundialmente por decisões judiciais domésticas.

O debate também surgiu no Tribunal de Justiça da União Europeia no caso *Glawischnig-Piesczek contra o Facebook Irlanda*.⁸⁹ A questão era se a Diretiva da União Europeia (UE) relativa ao comércio eletrônico regulamentou o alcance da jurisdição, autorizando os tribunais nacionais a ordenarem ao Facebook a remover conteúdos alegadamente difamatórios sobre um político austríaco com efeito global, ou impedindo isso. A resposta do tribunal não foi definitiva. Ele declarou que a diretiva da UE não regulamentava o escopo da jurisdição quanto aos “remédios” disponíveis e que isso cabia aos tribunais nacionais decidir, levando em consideração suas próprias leis nacionais e internacionais (veja a seção 5.A.2 para mais informações sobre o escopo geográfico da jurisdição reparativa).

Uma série de outras questões relativas à difamação também surgiram. Na região, houve casos que tratam das técnicas de preenchimento automático⁹⁰ utilizadas em diferentes serviços de Internet, particularmente buscadores.⁹¹ Outra questão que ganhou destaque é a responsabilidade potencial das pessoas apenas por apoiar (por exemplo, por “curtir”) conteúdo considerado difamatório ou prejudicial⁹² ou compartilhar esse

89 Tribunal de Justiça da União Europeia, “Processo C-18/18 Glawischnig-Piesczek”, 2019.

90 Para uma análise interessante dos desafios das técnicas de preenchimento automático, ver: Paul Baker e 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, pp. 187-204.

91 No Brasil, houve algumas decisões sobre o assunto. Ver: <<https://www.migalhas.com.br/arquivos/2014/9/art20140917-05.pdf>>. Acesso em: 09 mai 2021. O Tribunal Constitucional da Colômbia também decidiu que os motores de busca não são responsáveis quando links para conteúdo considerado difamatório aparecem entre seus resultados. Colômbia, Tribunal Constitucional, “Sentencia T-040/13”, 28 Jan 2013. Disponível em: <<http://bit.ly/1FylMlk>>. Acesso em: 09 mai 2021.; Tribunal Constitucional, “Sentencia T-453/13”, 15 Jul 2013: Disponível em: <<http://bit.ly/1R6lHaO>>. Acesso em: 09 mai 2021.; Tribunal Constitucional, “Sentencia T-634/13”, 13 set 2013. Disponível em: <<http://bit.ly/1OyMApE>>. Acesso em: 09 mai 2021.

92 No que diz respeito à situação internacional, ver: <<https://blog.oup.com/2017/09/traps-of-social-media/>>. Acesso em: 09 mai 2021. Ver também: <<https://www.internationallawoffice.com/Newsletters/Litigation/Switzerland/Lenz-Staehelin/Liking-or-sharing-defamatory-Facebook-posts-can-be-unlawful>>. Acesso em: 09 mai 2021.

conteúdo.⁹³ Por fim, outra questão é em que medida os administradores de grupos de redes sociais ou comunidades como as do serviço de mensagens do WhatsApp devem ser responsáveis por moderar o conteúdo dentro desse grupo ou comunidade.⁹⁴

2.2. A difamação ainda é uma ofensa criminal em certos países da região

Em muitos países da América Latina e do Caribe, a difamação não é apenas uma questão civil, mas também uma questão criminal.⁹⁵ A criminalização de conteúdo que viola a reputação de uma pessoa ainda é uma tradição jurídica difundida na região, embora o Sistema Interamericano de Direitos Humanos a tenha condenado como uma restrição indevida à liberdade de expressão.⁹⁶ A difamação on-line também pode ter repercussões criminais, o que pode ser ainda mais preocupante no caso de conteúdo disponibilizado durante eleições, quando o remédio sugerido deve ser de preferência a retificação ou o direito de resposta.⁹⁷

-
- 93 Em um caso brasileiro, foi decidido que a pessoa poderia ser responsabilizada. Ver: <<https://www.conjur.com.br/2017-nov-10/limite-penal-curtir-compartilhar-publicacoes-ofensivas-redes-sociais-crime>>. Acesso em: 09 mai 2021.
- 94 Ver: <<https://www.uol.com.br/tilt/noticias/redacao/2018/07/17/justica-pode-mirar-administrador-de-grupo-no-whatsapp-em-que-houve-crime.htm>>. Acesso em: 09 mai 2021.
- 95 Como exemplo, ver o estudo geral realizado pelo Comitê de Proteção de Jornalistas sobre leis de difamação criminal sul-americana. Disponível em: <<https://cpj.org/reports/2016/03/south-america.php>>. Acesso em: 09 mai 2021. Ver também o estudo do International Press Institute sobre leis de difamação criminal no Caribe. Disponível em: <<https://ipi.media/ipi-adds-caribbean-defamation-laws-to-online-database/>>. Acesso em: 09 mai 2021.
- 96 Corte Interamericana de Direitos Humanos, "Caso de Herrera Ulloa v. Costa Rica. Objecões Preliminares, Méritos, Reparações e Custos. Acórdão de 2 de julho de 2004", Série C, nº 107; "Caso de Ricardo Canese v. Paraguai. Méritos, Reparações e Custos, Acórdão de 31 de agosto de 2004", Série C, nº 111; "Caso de Kimel v. Argentina. Méritos, Reparações e Custos. Acórdão de 2 de maio de 2008", Série C, nº 177; "Caso de Tristán Donoso v. Panamá. Objecões Preliminares, Méritos, Reparações e Custos. Acórdão de 27 de janeiro de 2009". Série C, nº 193; "Caso de González Medina e Família v. República Dominicana, Julgamento de 27 de fevereiro de 2012"; "Caso de Vélez Restrepo v. Colômbia, Julgamento de 3 de setembro de 2012"; e "Caso de Fontevicchia e D'Amico v. Argentina, Acórdão de 29 de novembro de 2011".
- 97 Ver: <https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf>. Acesso em: 09 mai 2021.

A criminalização de conteúdo nocivo à reputação de uma pessoa também tem um efeito assustador (*chilling effect*) sobre as atividades de jornalistas profissionais, cidadãos e blogueiros, especialmente em pequenas cidades da América Latina e do Caribe. É fácil para as autoridades locais restringir severamente o conteúdo se alguém divulgar notícias ou produzir relatórios que possam desagradá-los, arriscando sua liberdade ao fazê-lo.

3. BULLYING ON-LINE

Diferentes tipos de *cyberbullying* emergem à medida que a tecnologia se desenvolve.⁹⁸ O bullying é tradicionalmente reconhecido por ocorrer quando há um ofensor e uma vítima submetida a assédio emocional ou físico. O bullying realizado por meio de tecnologias eletrônicas, especialmente a Internet, inclui mensagens privadas, a criação de sites focados em provocar algum tipo de mal a outra pessoa, a publicação on-line de fotos pouco lisonjeiras ou inapropriadas sem autorização e o tratamento danoso ou desagradável via telefones celulares ou on-line.⁹⁹

O *cyberbullying* afeta uma em cada 10 crianças.¹⁰⁰ De acordo com as *Diretrizes para a Proteção de Crianças On-line*, de 2020, da União Internacional de Telecomunicações (UIT), a maioria é capaz de distinguir o *cyberbullying* de brincadeiras ou provocações on-line, reconhecendo que o *cyberbullying* tem a intenção de prejudicar.¹⁰¹ As *Diretrizes para os formuladores de políticas para a Proteção de Crianças On-line* recomendam o desenvolvimento de legislação nacional apropriada e afirmam que a harmonização e coordenação em nível internacional é um passo fundamental para a proteção das crianças on-line. Isso porque leis e regras processuais harmonizadas de crimes cibernéticos sobre o assunto

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

99 United Nations Educational, Scientific and Cultural Organization (UNESCO), Behind the Numbers: Ending School Violence and Bullying, 2019, p. 14. Disponível em: <<https://unesdoc.unesco.org/ark:/48223/pf0000366483?posInSet=8&queryId=a84f5b5a-3828-462f-b63c-d45eae258884>>. Acesso em: 09 mai 2021.

100 Ibidem., p. 7.

101 União Internacional de Telecomunicações (UIT), "Guidelines on Child on-line Protection", 2020. Disponível em: <<https://www.itu-cop-guidelines.com/>>. Acesso em: 09 mai 2021.

permitiriam mais efetivamente prever as sanções penais necessárias para lidar com os danos on-line às crianças.¹⁰²

Quando o perpetrador do *cyberbullying* é anônimo ou usa uma conta falsa, a execução das normas contra este tipo de prática é um desafio e pode levar a decisões mais fortes por parte dos formuladores de políticas. Por exemplo, o aplicativo Secret foi indisponibilizado na App Store brasileira após uma série de relatos de *cyberbullying* supostamente ocorrido na forma de “segredos” anônimos publicados no aplicativo.¹⁰³ O mesmo aplicativo foi fortemente criticado no México, também por supostamente permitir práticas de *cyberbullying*.¹⁰⁴

A Global Kids Online é uma iniciativa importante para fornecer uma base de provas internacionais para o uso da Internet pelas crianças e conectar atores. Os países da região que disponibilizam resultados de pesquisa são: Argentina, Brasil, Chile e Uruguai.¹⁰⁵

Em abril de 2020, a SaferNet Brasil e o Fundo das Nações Unidas para a Infância (UNICEF) lançaram conjuntamente uma campanha para combater o *cyberbullying*, #ÉDaMinhaConta. A campanha oferece instruções sobre como agir em situações de bullying, como identificar se alguém é um alvo ou está praticando bullying.

Pesquisas conduzidas pela Fundación Paniamor na Costa Rica, envolvendo 1.008 crianças e adolescentes entre nove e 17 anos de idade, produziram descobertas importantes sobre o uso da Internet pelas crianças e adolescentes e os riscos relacionados à violência e à discriminação. De uma amostra de

102 Ver União Internacional de Telecomunicações (ITU), Guidelines for policy-makers on ChildOnline Protection, 2020, pp. 28-29. Disponível em: <<https://www.itu-cop-guidelines.com/policymakers>>. Acesso em 09 mai 2021.

103 UOL, "Aplicativo Secret cria polêmica ao permitir postagem anônima de 'segredos'", 2014. Disponível em: <<https://www.uol.com.br/tilt/noticias/redacao/2014/08/13/secret-cria-polemica-ao-prometer-anonimato-acao-visa-proibir-o-aplicativo.htm>>. Acesso em: 09 mai 2021. Ver também: GI, "Secret é retirado de loja de aplicativos da Apple no Brasil", 2014. Disponível em: <<http://g1.globo.com/tecnologia/noticia/2014/08/secret-e-retirado-de-loja-de-aplicativos-da-apple-no-brasil.html>>. Acesso em: 09 mai 2021.

104 Milenio, "Secret, la 'app' preferida de los jóvenes para 'cyberbullying'", 2014. Disponível em: <<https://www.milenio.com/cultura/secret-la-app-preferida-de-los-jovenes-para-ciberbullying>>. Acesso em: 09 mai 2021.

105 Ver Global Kids Online: <<http://globalkidsonline.net/about/>>. Acesso em: 09 mai 2021.

crianças entre nove e 12 anos de idade, 5,9% disseram ter sido discriminadas ou abusadas através da Internet, e 2,5% disseram não saber.¹⁰⁶ Entre os adolescentes com idade entre 13 e 17 anos, 3,2% disseram ter certeza e 2,8% não tinham certeza.¹⁰⁷

No Brasil, o *cyberbullying* e as ofensas diretas são os motivos mais comuns para entrar em contato com a linha de ajuda da SaferNet, superando os problemas relacionados à proteção de dados, fraude ou discurso de ódio.¹⁰⁸ No total, o *cyberbullying* é responsável pelo maior número de notificações, respondendo por 2.310 dos 25.184 casos desde 2007.

4. DISTRIBUIÇÃO NÃO CONSENSUAL DE MÍDIA SEXUALMENTE EXPLÍCITA

A distribuição não consensual da mídia sexualmente explícita pode assumir formas diferentes. Pode ser realizada por estranhos que publicam intencionalmente mídia sexualmente explícita on-line ou por alguém que teve uma relação íntima com a pessoa e publica o que é comumente conhecido como pornografia de vingança (no termo em inglês, *revenge porn*).

Países da América Latina e do Caribe têm adotado diferentes abordagens sobre o assunto. Em alguns casos, a distribuição de mídia sexualmente explícita não consensual pode ser tratada como difamação, enquanto em outros é adotada uma abordagem mais direcionada, com legislação penal emendada para tratar a prática como um novo tipo de conduta criminosa.

Entre meados de 2008 e 2020, 17 estados no México aprovaram a Lei Olímpica reformando a Lei Geral de Acesso das Mulheres a uma Vida Livre de Violência e os Códigos Criminais para reconhecer a violência digital como crime, impondo penas que podem variar até oito anos de prisão (em Michoacán) e multas.¹⁰⁹

106 Ver Relatório sobre a primeira pesquisa Kids on-line na Costa Rica, Niñas, niños y adolescentes en la Internet, abril 2019, figura 32. Disponível em: <<http://globalkidsonline.net/wp-content/uploads/2019/07/Kids-Online-Costa-Rica-1-Julio.pdf>>. Acesso em: 09 mai 2021.

107 Ibidem.

108 SaferNet, Helpline: <<https://helpline.org.br/indicadores/>>. Acesso em: 09 mai 2021.

109 México, "Ley Olimpia". Disponível em: <<http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf>>. Acesso em: 09 mai 2021.

O Brasil tem regras específicas tanto no direito penal quanto no direito civil. A transmissão, publicação, distribuição ou disponibilização de pornografia, mídia sexualmente explícita ou imagens de nudez, com ou sem o consentimento da vítima, é um crime punível com pena de prisão de um a cinco anos.¹¹⁰ O artigo 21 do Marco Civil da Internet, por sua vez, prevê um regime específico de remoção de imagens, vídeos ou outros materiais que representem nudez ou atos sexuais de natureza privada: o provedor de aplicações da Internet deve remover o conteúdo ao receber uma notificação extrajudicial, ou seja, uma denúncia ou comunicação do usuário.¹¹¹

No Uruguai, a distribuição não consensual de mídia sexualmente explícita é um crime e as plataformas da Internet estão sujeitas a sanções se não retirarem imediatamente o conteúdo.¹¹² Outros países, como Chile¹¹³ e Peru¹¹⁴, estão discutindo projetos de lei para abordar especificamente a distribuição não-consensual de mídia sexualmente explícita.

Embora em alguns casos possa ser difícil para tecnologias automatizadas reconhecer o propósito de uma publicação com conteúdo sexualmente explícito (uma questão abordada pela campanha *#WeTheNipple*¹¹⁵), plataformas intermediárias têm tomado cada vez mais medidas para responder à violência

-
- 110 Brasil, Código Penal, artigo 218-C. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 09 mai 2021.
- 111 Chiara A. S. de Teffe, "What is revenge porn and how can I protect myself?" Carta de Direitos da Internet do Brasil: Um olhar mais atento, Carlos Affonso Souza, Mario Viola e Ronaldo Lemos (eds), 2017, p. 137. Disponível em: <https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa_pages_miole_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf>. Acesso em: 09 mai 2021.
- 112 Uruguai, Lei nº 19580 de 2018, artigo 92. Disponível em: <<https://www.impo.com.uy/bases/leyes/19580-2017>>. Acesso em: 09 mai 2021.
- 113 Chile, Boletines, nº 11923-25 e 12164-07. Disponível em: <<https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmlD=12444&prmBol etin=11923-25>>. Acesso em: 09 mai 2021.
- 114 Peru, Projetos de Lei 01669/2016-CR e 2460/2019, ambos tornando criminalmente responsáveis. Ver: <http://www.leyes.congreso.gob.pe/Documentos/2016_2021/Proyectos_de_Ley_y_de_Resoluciones_Legislativas/PL0166920170717.pdf> and <<http://www.congreso.gob.pe/comisiones2016/Justicia/ProyectosLey/>>. Acesso em: 09 mai 2021.
- 115 A campanha pede ao Facebook e Instagram que façam uma exceção às suas restrições de nudez para permitir a arte no meio da fotografia. É apoiada por representantes em diferentes países ao redor do mundo, inclusive Brasil, Chile, Colômbia e República Dominicana.

baseada em gênero.¹¹⁶ Primeiro, a distribuição não consensual de mídia sexualmente explícita viola os padrões de comunidade de todas as principais plataformas, conforme descrito no *Relatório de Status Global 2019* da Rede de Políticas.¹¹⁷ Além disso, as plataformas estão implantando aprendizado de máquina e inteligência artificial para detectar imagens ou vídeos que estão sendo compartilhados de forma não consensual e também lançaram *hubs* de suporte a vítimas.¹¹⁸

Mesmo assim, as organizações da sociedade civil estão cada vez mais exigindo uma resposta mais proativa das plataformas, para que estas forneçam uma resposta mais rápida às notificações e sejam mais transparentes sobre dados de violência baseada em gênero.¹¹⁹

Além do acima exposto, é importante considerar que as vítimas da distribuição não consensual da mídia sexualmente explícita tendem a pertencer a grupos que são vulneráveis e frequentemente discriminados. As mulheres, por exemplo, são geralmente as vítimas, enquanto os homens são os autores.¹²⁰ Esse tipo de abuso, no entanto, não é o único enfrentado on-line por mulheres.

Ativistas mexicanos descreveram pelo menos 13 possíveis manifestações de violência on-line baseada em gênero: acesso não autorizado e controle de acesso; controle e manipulação de

-
- 116 Juliana Pacetta Ruiz, Mariana Girogetti Valente and Natalia Neris, "Between the perpetrator and the victim: the role of Internet intermediaries on violations against women", *Sociologia y Tecnociencia*, vol. 9, No. 1, 2019, pp. 14-17. Ver Disponível em: <<https://revistas.uva.es/index.php/sociotecn/article/view/2240/1779>>. Acesso em: 09 mai 2021.
- 117 Rede de Políticas Internet & Jurisdição, *Internet & jurisdição: relatório de status global 2019*, p. 166.
- 118 Facebook, "Detecting Non-Consensual Intimate Images and Supporting Victims", Março de 2019. Ver: <<https://about.fb.com/news/2019/03/detecting-non-consensual-intimate-images/>>. Acesso em: 09 mai 2021.
- 119 México, "Internet é nuestra MX. Llamado a las plataformas digitales a agilizar procesos de denuncia tras agresiones que mujeres reciben en el marco de protesta #NoMeCuidanMeViolan", 2019. Ver: Disponível em: <<https://internetesnuestra.mx/post/187169630893/llamado-a-las-plataformas-digitales-a-agilizar>>. Acesso em: 09 mai 2021.
- 120 Clare McGlynn, Erika Rackley and Ruth Houghton, "Beyond 'revenge porn: the continuum of image-based sexual abuse", 2017 Disponível em: <<https://link.springer.com/content/pdf/10.1007/s10691-017-9343-2.pdf>>. Acesso em: 09 mai 2021; Abby Whitmarsh, "Analysis of 28 days of data scraped from a revenge pornography Website", 2015. Disponível em: <<https://everlastingstudent.wordpress.com/2015/04/13/analysis-of-28-days-of-data-scraped-from-a-revenge-pornography-website/>>.

informações; personificação e roubo de identidade; vigilância e perseguição; conteúdo discriminatório; assédio; ameaças; compartilhamento não consensual de informações privadas; extorsão; difamação; abuso e exploração sexual relacionados à tecnologia; ataques aos canais de comunicação; e excessos por parte de agentes reguladores.¹²¹

Esse tipo de abuso direcionado é particularmente predominante em uma região onde pelo menos 12 mulheres morrem todos os dias devido a incidentes relacionados ao simples fato de serem mulheres,¹²² e onde a igualdade de gênero ainda está longe de ser uma realidade.¹²³ Sendo assim, a violência off-line e on-line devem ser vistas como interconectadas e não devem ser tratadas separadamente.¹²⁴ Não significa que certo tipo de abuso comece e termine on-line. Em vez disso, a violência pode ocorrer tanto off-line, quanto, de forma reiterada (e contínua), on-line.¹²⁵ Exemplos são quando o abuso sexual é filmado e disseminado nas mídias sociais ou quando ativistas de direitos das mulheres recebem ameaças on-line seguidas de ataques nas ruas.

Dificuldades em executar tal remoção de conteúdo, às vezes por causa de questões jurisdicionais, também podem ter

-
- 121 GenterIT.org, "13 manifestations of gender-based violence online" (2018). Disponível em: <<https://www.genderit.org/resources/13-manifestations-gender-based-violence-using-technology>>. Acesso em: 09 mai 2021.
- 122 Economic Commission for Latin America and the Caribbean (ECLAC), "Feminicídio", Infografias, 24 Out 2016. Disponível em: <<https://www.cepal.org/es/infografias/feminicidio>>. Acesso em: 09 mai 2021. Em 2018, os países latino-americanos com as maiores taxas de femicídio por 100.000 mulheres foram El Salvador (6,8), Honduras (5.1), o Estado Plurinacional da Bolívia (2.3), Guatemala (2.0) e República Dominicana (1,9). No Caribe, Santa Lúcia (4.4) e Trinidad e Tobago (3.4) apresentaram as taxas mais altas. Ver: ECLAC, "Femicide or feminicide". Disponível em: <<https://oig.cepal.org/en/indicators/femicide-or-feminicide>>. Acesso em: 09 mai 2021.
- 123 Ver "Indicadores". Disponível em: <<https://oig.cepal.org/en/indicators>>. Acesso em: 09 mai 2021. E CEPAL, "Planos de igualdade de gênero na América Latina e no Caribe: mapas para o desenvolvimento", Observatório de Igualdade de Gênero para a América Latina e o Caribe. Estudos, nº 1 (LC/pub.2017/1-p/rev.1), Santiago, 2019.
- 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, p. 15. Disponível em: <https://www.internetlab.org.br/wp-content/uploads/2017/11/Relatorio_ViolenciaGenero_UNU.pdf>. Acesso em: 09 mai 2021.
- 125 Swedish International Development Cooperation Agency (Sida), "Gender-based violence online", 2019. Ver: <https://www.sida.se/contentassets/97224704b4f643cba3b4fca3d931e576/brief_gender-based_violence_online_sep-2019_webb.pdf>. Acesso em: 09 mai 2021.

consequências que alteram a vida das mulheres. Na Colômbia, por exemplo, não foi possível identificar uma pessoa que enviava ameaças a uma mulher, porque as ameaças foram enviadas de um lugar público (um cibercafé). Em outro caso, o autor não pôde ser identificado porque o endereço era um local nos Estados Unidos.¹²⁶

Tais casos têm um efeito que se estende para além da vítima, visando as mulheres de forma mais ampla. Como observou a Relatora Especial das Nações Unidas sobre a violência contra as mulheres, “apesar dos benefícios e potencialidades de capacitação da Internet e das TIC, as mulheres e as meninas em todo o mundo manifestaram cada vez mais a sua preocupação com conteúdos e comportamentos on-line nocivos, sexistas, misóginos e violentos. Portanto, é importante reconhecer que a Internet está sendo utilizada num ambiente mais amplo de discriminação estrutural generalizada e sistêmica e de violência baseada no gênero contra mulheres e meninas”¹²⁷.

Em resumo, diferentes tipos de abusos que poderiam prejudicar a todos também devem ser vistos através das lentes específicas dos grupos visados, sejam eles mulheres, minorias étnicas, povos indígenas, imigrantes ou LGBTQ. O outro lado desta perspectiva é a forma como a Internet também deu voz a grupos socialmente marginalizados e os ajudou a construir redes para combater ameaças on-line, combater a violência baseada em gênero e dar apoio às vítimas, por exemplo, as iniciativas Take Back the Tech¹²⁸ (mundial) e Vita Activa¹²⁹ (México).

126 Case Study Number 1, Colombia, (Ramírez Cardona (2014), citado em Association for Progressive Communications (apc), From Impunity to Justice: Domestic Legal Remedies for Cases of Technology-Related Violence against Women, “End violence: Women’s rights and safety online” project (p. 22). Disponível em: <https://www.genderit.org/sites/default/files/flow_domestic_legal_remedies_0.pdf>. Acesso em: 09 mai 2021.

127 Nações Unidas, Relatório da Relatora Especial das Nações Unidas sobre a violência contra as mulheres, suas causas e consequências sobre a violência on-line contra mulheres e meninas a partir de uma perspectiva de direitos humanos (A/HCR/38/47), 2018. Disponível em: <<https://undocs.org/en/A/HRC/38/47>>. Acesso em: 09 mai 2021.

128 Ver: <<https://www.takebackthetech.net/>>. Acesso em: 09 mai 2021.

129 Ver: <<https://vita-activa.org/>>. Acesso em: 09 mai 2021

5. O “DIREITO AO ESQUECIMENTO” SE DEPARA COM AS CARACTERÍSTICAS PARTICULARES DA REGIÃO

Conforme explorado em maior profundidade na seção IV.C.6, vários países da região adotaram uma lei geral de proteção de dados, mais ou menos inspirada no Regulamento Geral Europeu de Proteção de Dados (GDPR). Também influente foi uma decisão de 2014 do Tribunal de Justiça da União Europeia no caso Google Espanha¹³⁰, que decidiu que um cidadão espanhol poderia exercer seu “direito ao esquecimento” contra os mecanismos de busca on-line, obrigando as empresas em questão a removerem alguns resultados de busca alegadamente prejudiciais.

Essa decisão desencadeou uma discussão regional, centrada na situação normativa em muitos países que agora reconheceram o direito a ser esquecido e a questão de se é prudente, ou mesmo desejável, instituir tal direito. O debate é mais apropriadamente entendido como um direito de solicitar o “desreferenciamento” (*de-listing*) ou a “desindexação” (*de-indexing*). Na Espanha, como o julgamento não estabeleceu tal exigência, o conteúdo em si não é apagado. Em vez disso, os mecanismos de busca como Google, Bing e outros só são instruídos a remover os resultados das pesquisas com base no nome do indivíduo e outros marcadores pessoais identificáveis ligados a informações consideradas irrelevantes, desatualizadas ou sem valor atual.

O caso do Google Espanha provocou uma série de reivindicações afirmando esse direito no contexto da região. As diferenças nas regulações de proteção de dados (ou a falta delas) não impediram que alguns tribunais nacionais reconhecessem a existência de “um direito ao esquecimento” e ordenassem aos mecanismos de busca, e às vezes aos veículos de notícias, que procedessem ao desreferenciamento das informações.¹³¹ Na maioria das vezes, os parâmetros desse direito foram deixados pouco claros, de modo que seu escopo e até mesmo a questão

130 Tribunal de Justiça da União Europeia, processo C-131/12, Google Spain SL e Google Inc. V. Agencia Española de Protección de Datos (AEPD) e Mario Costeja González, 2014.

131 Ver: <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>. Acesso em: 09 mai 2021.

de quem é responsável pelo desreferenciamento e sob quais condições são deixados em aberto.¹³²

Outros tribunais rejeitaram ou qualificaram o direito.¹³³ A história da proteção da liberdade de expressão na região tende a atuar como contrapeso ao desreferenciamento, particularmente sem uma ordem judicial.¹³⁴

5.1. O “direito ao esquecimento” é amplamente percebido como um conceito global

Os participantes da pesquisa responderam se o direito ao esquecimento havia atingido o status global ou se era aplicável à América Latina e ao Caribe como um todo. Um dos atores disse que a expressão “direito ao esquecimento” tinha sido usada na América Latina e no Caribe como um termo guarda-chuva, incluindo todas as instâncias em que os usuários pediram a Provedores de Serviços de Internet (PSIs) para remover, desindexar, desreferenciar ou ocultar conteúdo. Outros argumentaram que o conceito por trás do direito está ganhando terreno e que certos tribunais e países estão reconhecendo este direito. No total, 70,73% dos participantes pesquisados e entrevistados concordaram ou concordaram fortemente que o direito ao esquecimento é, de fato, um conceito global.

132 Ver: <https://www.palermo.edu/cele/pdf/investigaciones/Towards_an_Internet_Free_of_Censorship_II_10-03_FINAL.pdf>. Acesso em: 09 mai 2021.

133 Um dos casos mais importantes envolveu a questão de saber se os intermediários poderiam ser responsabilizados por conteúdos que impactaram a privacidade ou a reputação. O tribunal considerou que o desreferenciamento só deveria ser aplicado com uma ordem judicial e/ou quando informações ilegais estivessem envolvidas (Argentina, Suprema Corte, Rodríguez M. Beien c/ Google y Otro s/ daños y perjuicios, Acórdão R.522.XLIX, 28 de outubro de 2014). No Brasil, o direito tem sido amplamente debatido e foi objeto de uma audiência pública no Supremo Tribunal Federal brasileiro. O Tribunal Superior havia concedido o direito com qualificações. Para a ata do debate sobre o processo Aida Curi, ver: <http://www.stf.jus.br/arquivo/cms/audienciasPublicas/anexo/AUDINCIAPUBLICASOBREODIREITOAQUESQUECIMENTO_Transcries.pdf>. Acesso em: 09 mai 2021.

134 Ver: <<https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf>>. Acesso em: 09 mai 2021.

INFOGRÁFICO 6

Você considera que o “direito ao esquecimento” está se tornando um conceito global?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

Como observou um dos atores pesquisados: “O direito ao esquecimento é um novo direito proposto no contexto da sociedade da informação. As reações a esse direito variam de país para país, porque o conceito e a lógica ainda não estão claramente definidos. A ausência de consenso sobre esse ponto tem o potencial de criar incerteza em uma sociedade que está se tornando cada vez mais sem fronteiras. As decisões específicas por país não são suficientes para o bom desenvolvimento deste conceito e é urgente chegar a um consenso em torno dos pontos centrais. Dado o caráter sem fronteiras do mundo atual, o conflito entre valores fundamentais – proteção da dignidade do indivíduo contra o direito ao conhecimento e à liberdade de expressão – está produzindo resultados variados.”

5.2. As leis locais de anistia e a noção compensatória de um “direito à memória” impactam a aplicação do direito ao esquecimento

Certos elementos da ordem jurídica, história e cultura da região divergiram de suas raízes europeias originais. Por exemplo, muitos países da América Latina e do Caribe passaram por regimes autoritários muito recentes, dos quais vários líderes foram acusados de violações graves aos direitos humanos. Na transição para a democracia, a maioria desses Estados emitiu leis de anistia perdoadando os responsáveis pelas violações dos direitos humanos e, em muitos casos, bloqueando tanto o acesso à verdade sobre o que aconteceu quanto qualquer perspectiva de reparação.

Com base em uma forte orientação advinda do Sistema Interamericano de Direitos Humanos,¹³⁵ tem havido um esforço nas últimas décadas para desenvolver o direito oposto, um “direito à memória”, um direito para que as vítimas tenham acesso à verdade. Com base nesse direito, as leis de anistia foram revogadas, as comissões da verdade foram estabelecidas e os perpetradores foram até processados.

Especialistas em proteção de dados, autoridades e organizações da sociedade civil¹³⁶ veem agora um “direito ao esquecimento” como contrário a esta tradição cultural e de direitos humanos.¹³⁷ Assim, regionalmente, o desreferenciamento como conceito tem de existir ao lado de um “direito à memória”, particularmente em situações relativas à informação sobre violações dos direitos humanos, alegadas ou reais.

Alguns países, entretanto, incluíram o direito à eliminação de dados pessoais em sua legislação de proteção de dados com uma redação semelhante à do chamado direito ao esquecimento em questão no caso europeu mencionado.

As diferenças entre a Europa e a América Latina e o Caribe continuam ligadas ao fato de que os países da região tendem a tratar a proteção de dados como se fossem dados armazenados no *back-end*, em oposição ao conteúdo tornado público, que é mais claramente entendido como relacionado à liberdade de

135 As opiniões do Sistema Interamericano de Direitos Humanos podem ser encontradas no relatório “Standards for a Free, Open and Inclusive Internet”, 2016, paras. 134 ff. Ver: <http://www.oas.org/en/iachr/expression/docs/publications/INTERNET_2016_ENG.pdf>. Acesso em: 09 mai 2021.

136 R3D, “El erróneamente llamado ‘derecho al olvido’ no es un derecho, es una forma de censura”, 2015. Disponível em: <<https://r3d.mx/2016/07/12/el-erroneamente-llamado-derecho-al-olvido-no-es-un-derecho-es-una-forma-de-censura/>>. Acesso em: 09 mai 2021; Hiperderecho, “Proteção de dados Casa de hóspedes: la nueva puerta falsa de la censura”, 2016. Disponível em: <<http://www.hiperderecho.org/2016/07/proteccion-datos-personales-la-nueva-puerta-falsa-la-censura/>>. Acesso em: 09 mai 2021.

137 Há aqueles que consideraram isso “um insulto” à história da região. Eduardo Bertoni, “The Right to Be Forgotten: An Insult to Latin American History”, 2014. Disponível em: <https://www.huffpost.com/entry/the-right-to-be-forgotten_b_5870664>. Acesso em: 09 mai 2021. Para uma análise geral da ex-Relatora Especial da Organização dos Estados Americanos (OEA) para a Liberdade de Expressão, Catalina Botero, ver: < <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2016/04/GFOE-Presentation-Catalina-Botero-.pdf>>. Acesso em: 09 mai 2021.

expressão.¹³⁸ Em alguns países, também prevaleceu o princípio da neutralidade da rede, sendo a eliminação do desreferenciamento ou desindexação considerada prejudicial a ela.¹³⁹

A forma precisa de qualquer direito ao esquecimento, seja através do desreferenciamento, da desindexação ou mesmo da remoção, parece não ter sido explicada de forma consistente na região e a divisão entre os atores pesquisados parece ser um reflexo disso.

B. Segurança

1. É NECESSÁRIA MAIOR COORDENAÇÃO DE CIBERSEGURANÇA PARA LIDAR COM INCIDENTES GENERALIZADOS NA REGIÃO

A América Latina e o Caribe têm um histórico de ter tido que lidar com questões de segurança em diferentes níveis, sejam elas relacionadas à segurança pessoal, institucional ou nacional. O surgimento da Internet não mudou isso de maneira radical. No entanto, o panorama de segurança acabou sendo modificado. O ciberespaço tornou-se outro território que carece de proteção e onde outros crimes podem ser cometidos.

A crescente interconexão entre os mundos off-line e on-line, particularmente com a chamada Internet das Coisas, está tornando as questões de segurança ainda mais importantes. Tem havido um número crescente de incidentes de segurança cibernética na América Latina e no Caribe. Ao mesmo tempo, a região se tornou um importante refúgio para os perpetradores de tais ações. Soma-se a isso o fato de que muitos dos serviços de Internet mais populares na região tendem a ser estrangeiros e quantidades significativas de dados passam por ou são

138 Isso pode ser entendido a partir da forma como os tribunais lidam com tais casos. Um exemplo é um caso brasileiro que envolve um promotor acusado de fraude em um exame público de admissão para o cargo de juiz e, posteriormente, inocentado do delito. Superior Tribunal de Justiça, "Recurso especial No 1.660.168 - RJ (2014/0291777-1)", 2018. Disponível em: <https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencia_l=1628798&num_registro=201402917771&data=20180605&formato=P DF>. Acesso em: 09 mai 2021. Outro exemplo pode ser encontrado no México; veja: <<https://perma.cc/N8LW-9ZBZ>>. Acesso em: 09 mai 2021.

139 Colômbia, Tribunal Constitucional, Decisão nº. T-277 de 2015, "Acción de tutela instaurada por Gloria contra la Casa Editorial El Tiempo", 12 Maio 2015. Disponível em: <<https://perma.cc/KF4Q-VW6S>>. Acesso em: 09 mai 2021.

armazenados em países fora da América Latina e do Caribe, principalmente nos mais desenvolvidos. Isso gera desafios transfronteiriços que vão desde dificuldades na determinação da localização de crimes cibernéticos a acesso a provas, controle sobre as normas de segurança de dados, até questões relativas à vigilância.

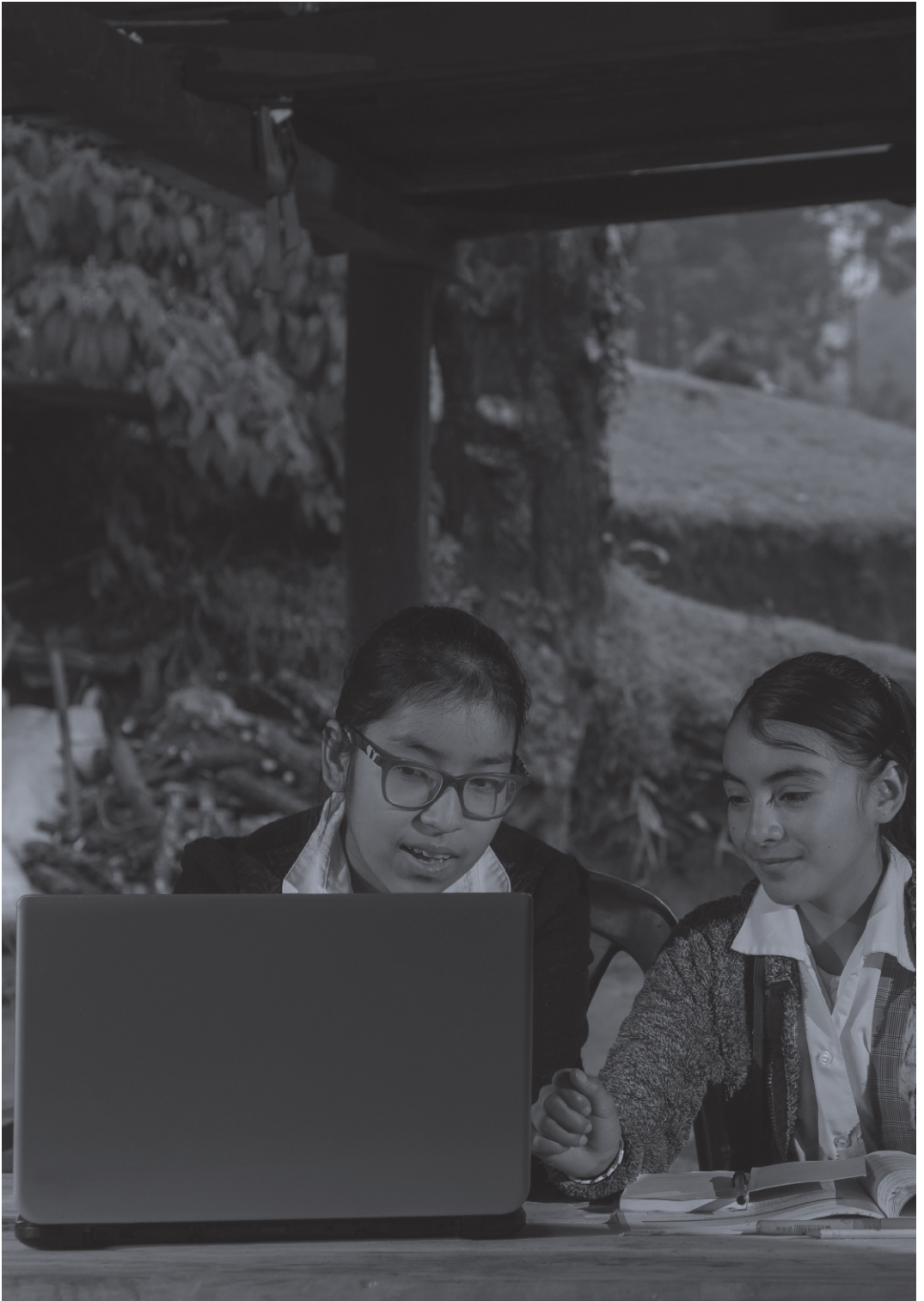
Um dos atores participantes da pesquisa observou como a necessidade de agilizar o acesso aos dados e resolver incidentes de cibersegurança colidiu com as identidades jurídicas nacionais e a soberania jurisdicional. Um grande número de atores observou que a cooperação internacional em tais questões transfronteiriças é essencial para lidar com este desafio.

2. INVESTIGAÇÕES TRANSFRONTEIRIÇAS E PROVAS ELETRÔNICAS

A corrupção não é uma característica da vida na América Latina e do Caribe pela qual a região se orgulha de ser conhecida. Nas últimas duas décadas, os escândalos passaram de casos isolados envolvendo principalmente assuntos domésticos para esquemas organizados, alguns englobando mais de uma ou mesmo várias jurisdições. Um exemplo significativo foi a Operação Lava-Jato, que começou como uma investigação no Brasil, mas desvendou esquemas sofisticados em dezenas de países. Uma empresa, a Odebrecht, tem sido o foco de investigações em vários Estados da região, enquanto ex-presidentes ou vice-presidentes de pelo menos cinco países estão na prisão ou sob investigação. Vários políticos de alto nível de outros países também estão sendo investigados.¹⁴⁰

Esses esquemas de corrupção envolvendo múltiplas jurisdições levaram a investigações que exigiram cooperação transfronteiriça de agentes de execução da lei e vários outros agentes, com importantes debates jurisdicionais. Talvez as mais importantes dessas questões diga respeito ao acesso a provas digitais em múltiplas jurisdições e à necessidade de reformar os instrumentos de cooperação internacional que fornecem mecanismos para a preservação e o acesso a provas eletrônicas além das fronteiras.

140 Para obter uma visão geral do escândalo de corrupção, consulte: <<https://www.bbc.com/news/world-latin-america-41109132>>. Acesso em: 09 mai 2021.



2.1. Acesso às provas digitais em múltiplas jurisdições

No curso de uma investigação em múltiplas jurisdições, as agências de execução da lei precisam ter acesso a informações que podem estar localizadas em outro país, talvez porque as ações em questão tenham atravessado jurisdições. Por exemplo, uma empresa pode transferir fundos para uma conta *off-shore* pertencente a um funcionário corrupto; ou supostos criminosos podem usar serviços de Internet em nuvem que armazenam dados no exterior. As provas produzidas em uma investigação podem ser relevantes para outra e, em alguns casos, a investigação de um caso de corrupção estrangeira pode ter impacto na segurança de uma investigação em outro país.¹⁴¹

O fato de que dados relevantes podem estar conectados a outros países dá origem a uma série de questões jurisdicionais. É importante notar, entretanto, que há uma distinção entre a jurisdição sobre um crime em si e a jurisdição sobre as provas necessárias para investigar esse crime.

No que diz respeito à jurisdição sobre provas, várias questões ainda estão sendo discutidas. Em primeiro lugar, pode haver uma disputa sobre o elemento de conexão necessário para determinar a jurisdição sobre provas digitais. O elemento de conexão mais comum tem sido tradicionalmente a localização das provas. Isso traz pelo menos duas dificuldades. Devido à sua natureza digital e fluidez potencial, as provas digitais (dados) podem ser divididas entre diferentes jurisdições ou transferidas para outro local sem aviso ou esforço. Os serviços de nuvem executam essas duas ações, dividindo pacotes de informações e movendo-os constantemente entre servidores, que podem estar, e geralmente estão, em diferentes jurisdições.

A localização dos dados não é o único fator de conexão possível. Pode haver outros, como a nacionalidade, domicílio ou local de residência habitual do titular dos dados, ou o local de constituição da empresa de posse dos dados.

Além disso, o sucesso de qualquer solicitação de acesso a dados armazenados no exterior pode depender da cooperação com o país onde os dados estão localizados. Tradicionalmente,

141 Para uma análise da interconexão da corrupção, suborno estrangeiro e acesso a informações e provas, ver: <<http://www.oecd.org/daf/anti-bribery/TypologyMLA2012.pdf>>. Acesso em: 09 mai 2021.

também as solicitações estrangeiras e nacionais estão sujeitas a diferentes critérios e procedimentos. Assim, a validade e a execução de um pedido estrangeiro para apresentar provas podem ser contestadas.

Por último, os países podem impor normas de bloqueio que não permitam que os dados sejam transmitidos internacionalmente, exceto em circunstâncias específicas e sujeitos a procedimentos específicos. Algumas legislações de proteção de dados, por exemplo, bloqueiam transferências sem um mandado ou consentimento doméstico.

Essas questões tendem a representar uma série de desafios para os agentes da lei. O acesso às provas de um crime cometido no país “A” por cidadãos do país “A” cujas vítimas também estão no país “A” pode depender de um procedimento internacional simplesmente porque os dados comprobatórios relevantes são armazenados fora desse país.

Alguns dos atores pesquisados destacaram a importância do acesso a provas armazenadas no exterior para investigações criminais e a necessidade de cooperação e compartilhamento de informações. Observaram também que os processos internacionais poderiam ser complicados e não necessariamente bem adaptados à urgência e rapidez das investigações de hoje, sugerindo a necessidade de uma mudança de paradigma na região.

No caso da empresa multinacional brasileira Odebrecht, o Departamento de Justiça dos Estados Unidos (DOJ) fez um acordo com a empresa para monitorar o cumprimento da legislação anticorrupção. O acordo abrangeu o compartilhamento de informações com uma organização de monitoramento e com o DOJ, incluindo um requisito para transferir informações – dados pessoais entre eles – não no contexto de uma investigação, mas após a sua conclusão, para evitar futuras ações ilegais.¹⁴²

142 Ver: <<https://globalinvestigationsreview.com/article/1139256/us-and-brazil-agree-local-odebrecht-monitors>>. Ver também: <<https://www.justice.gov/opa/press-release/file/919916/download>>. Acesso em: 09 mai 2021.

2.2. O sistema de assistência jurídica mútua precisa ser adaptado à era digital

A forma tradicional de solicitar provas extraterritoriais é através da cooperação jurídica internacional. Existe uma rede de acordos internacionais que prevê procedimentos legais para facilitar a assistência e a cooperação transfronteiriça.

Sem dúvida, os mais comuns são os acordos de assistência jurídica mútua (MLA, na sigla em inglês). Os Estados da região são partes em uma série de acordos bilaterais de MLA, bem como de tratados multilaterais de âmbito universal ou regional. A Convenção Interamericana de Assistência Mútua em Matéria Penal (1992), por exemplo, tem 26 países latino-americanos e caribenhos como signatários.¹⁴³ Outras convenções específicas tratam da assistência jurídica mútua e da necessidade de cooperação internacional em tais assuntos. Todos os países da região, exceto Cuba, são partes do Artigo XIV da Convenção Interamericana contra a Corrupção (1996).¹⁴⁴

O sistema dos tratados MLA é um passo à frente em relação ao uso tradicional da cooperação diplomática e das cartas rogatórias, mas tem seu próprio conjunto de dificuldades. Depende de os países serem partes dos tratados MLA e os procedimentos não são uniformes, pois podem variar de acordo para acordo.¹⁴⁵ Além disso, o sistema administrativo em vigor foi estruturado para trabalhar com solicitações excepcionais do exterior, e não com grandes volumes de solicitações. A falta de automação e escalabilidade significa que os procedimentos podem não ser temporalmente oportunos. Nesse meio tempo, as investigações podem ser paralisadas, potenciais culpados podem não ser encontrados e, assim, permanecer em liberdade, pode haver a continuidade dos crimes e as provas podem ser movidas (para outra jurisdição) ou destruídas.

143 Ver: <<https://www.oas.org/juridico/english/treaties/a-55.html>>. A convenção tem um protocolo do qual um número muito menor de países são partes: <<http://www.oas.org/juridico/english/treaties/a-59.html>>. Acesso em: 09 mai 2021.

144 Ver: <http://www.oas.org/en/sla/dil/inter_american_treaties_B-58_against_Corruption.asp>. Acesso em: 09 mai 2021.

145 Ver: <<https://www.justice.gov/archives/jm/criminal-resource-manual-276-treaty-requests>>. Acesso em: 09 mai 2021.

Vários países da região acreditam que o sistema de MLA requer reforma.¹⁴⁶ A maioria dos atores pesquisados também concorda que é necessário introduzir procedimentos mais ágeis nos acordos de cooperação internacional. Alguns advertiram, entretanto, que os procedimentos devem respeitar o devido processo, a privacidade dos dados e os direitos humanos em geral. Um dos atores destacou a necessidade de garantir a autenticidade dos documentos e a credibilidade dos atores que emitem o pedido.

Geralmente, os atores não defendem uma reestruturação completa do sistema MLA, mas, em vez disso, exigem que ele seja adaptado à era digital. A opinião deles é que a maioria das questões deriva do fato de que as empresas de Internet estão estabelecidas no exterior com uma presença local. Suas sugestões tendem a girar em torno de um mecanismo de solicitações diretas a essas empresas (na qualidade de detentoras de dados).

Há pouco consenso, entretanto, sobre o instrumento a ser utilizado para tal reforma. Por serem bilaterais ou multilaterais, os tratados de MLA tendem a levar tempo para serem negociados e podem não abranger todas as necessidades de acesso e preservação de informações. Enquanto isso, os países estão procurando soluções, seja unilateralmente ou como parte de grupos com os mesmos interesses.

INFOGRÁFICO 7

Você concorda com esta declaração: a cooperação jurídica para execução em matéria de provas eletrônicas transfronteiriças (através de tratados de assistência jurídica mútua ou outros procedimentos) necessita de melhorias significativas?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

146 Informações enviadas pelos Estados da América Latina e do Caribe ao Escritório das Nações Unidas sobre Drogas e Crime (UNODC). Ver: <<https://undocs.org/A/74/130>>. Acesso em: 09 mai 2021.

2.3. A contribuição da Convenção de Budapeste sobre Cibercrime para as investigações transfronteiriças

Vários Estados da América Latina e do Caribe são partes ou aderiram à Convenção sobre Cibercrimes do Conselho da Europa de 2001 (Convenção de Budapeste), que, entre outras disposições, estabelece mecanismos de cooperação internacional em matéria de criminalidade cibernética.¹⁴⁷ A Argentina, Chile, Colômbia, Costa Rica, República Dominicana, Guatemala, México, Panamá, Paraguai e Peru são partes da Convenção, e o Brasil foi convidado a aderir-la em dezembro.¹⁴⁸ A Convenção prevê arranjos mais expeditos para a preservação e o acesso a provas.

Os entrevistados foram da opinião de que, embora a Convenção de Budapeste não tenha resolvido todos os problemas com o sistema MLA, ela foi um passo na direção certa. Um dos atores observou que a participação na Convenção de Budapeste proporcionou um fórum importante para discutir os obstáculos ao acesso às provas digitais.

Os membros da Convenção estão discutindo um protocolo adicional¹⁴⁹ que fornecerá ferramentas mais específicas para criar um regime mais abrangente e rápido, especialmente para dados de assinantes armazenados em serviços de nuvem.¹⁵⁰ Uma dificuldade significativa, no entanto, é estabelecer um parâmetro comum de entendimento no que diz respeito à privacidade e outros direitos humanos. Alguns dos entrevistados expressaram essa preocupação.

147 Ver: <<https://www.coe.int/en/web/cybercrime/the-budapest-convention>>. Acesso em: 09 mai 2021.

148 Council of Europe, "Budapest Convention: Brazil invited to accede", 2019. Disponível em: <<https://www.coe.int/en/web/cybercrime/-/budapest-convention-brazil-invited-to-accede>>. Acesso em 09 mai 2021.

149 Ver: <<https://www.coe.int/en/web/cybercrime/t-cy-drafting-group>>. Acesso em: 09 mai 2021.

150 Em uma pesquisa do UNODC, os membros da América Latina e Caribe mencionaram a atualização da Convenção de Budapeste sobre Crimes Cibernéticos como uma solução possível. Ver: <<https://undocs.org/A/74/130>>. Acesso em: 09 mai 2021.

2.4. Alternativas ao sistema MLA estão sendo exploradas fora da região

Como os processos internacionais ainda não atingiram a maturidade plena, vários países embarcaram em iniciativas unilaterais que consistem em reformas jurídicas nacionais. Uma das principais soluções tem sido a delegação de competência para autoridades específicas solicitarem o acesso a dados diretamente àqueles que os detêm, em particular aos Provedores de Serviços de Internet (PSIs).

Os Estados Unidos aprovaram a Lei de Clarificação do Uso Legal de Dados no Exterior (CLOUD Act), que fornece um mecanismo que permite agências de execução da lei em países que têm um acordo executivo com os Estados Unidos solicitar diretamente às empresas a apresentação de dados. A Lei esclarece que a jurisdição sobre provas digitais depende da nacionalidade ou residência do titular dos dados (cliente do PSI). As diretrizes do Departamento de Justiça estabelecem que os PSIs nacionais poderão ser solicitados a produzir os dados que possuem, independentemente de onde esses dados estejam localizados.¹⁵¹

Da mesma forma, a UE iniciou um projeto chamado e-Evidence. Ele consiste em um projeto de regulamento que criaria ordens executivas para a preservação e o acesso a provas digitais a serem enviadas diretamente aos provedores de serviços de Internet que operam na UE, independentemente da localização dos dados; além disso, os PSIs estrangeiros seriam obrigados a indicar ou constituir um representante legal na UE para receber tais decisões e ordens.¹⁵²

151 Ver: <<https://www.justice.gov/opa/press-release/file/1153446/download>> . Acesso em: 09 mai 2021.

152 Ver: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>. Acesso em: 09 mai 2021. Para mais informações, ver Comissão Europeia, "Proposta de Regulamento do Parlamento Europeu e do Conselho sobre Ordens de Produção e Conservação de Provas Eletrônicas em Matéria Penal" (COM(2018) 225 final), 17 de Abril de 2018. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>> Acesso em: 09 mai 2021; "Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece regras harmonizadas para a nomeação de representantes legais para fins de obtenção de provas em processos penais" (COM(2018) 226 final), 17 de abril de 2018. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=PT>>. Acesso em: 09 mai 2021.

Ambos os projetos reconhecem que ainda há uma necessidade de cooperação internacional. Os PSIs podem estar sujeitos a leis em outros países que os impeçam de produzir as provas, o que significa que são necessários procedimentos especiais para ter acesso a elas. O CLOUD Act autoriza o Presidente a negociar com os países que atendem a certos critérios de privacidade e proteção de direitos para chegar a acordos executivos que possam facilitar a cooperação direta, permitindo que os pedidos sejam encaminhados às entidades detentoras dos dados. Em 5 de fevereiro de 2019, a Comissão Europeia recebeu um mandato de duas vias para iniciar negociações sobre acesso transfronteiriço a provas digitais com os Estados Unidos, dentro do contexto do protocolo adicional à Convenção de Budapeste, acima mencionado.¹⁵³

Os entrevistados mencionaram a adesão à Convenção de Budapeste (2001) como um caminho a seguir, ao mesmo tempo em que observaram que ela não pode resolver todas as questões. Os agentes de execução da lei ainda estão buscando maneiras de acessar dados armazenados no exterior. No caso do Brasil, por exemplo, isso se transformou em uma discussão sobre a constitucionalidade do tratado de MLA com os Estados Unidos. O Supremo Tribunal Federal foi chamado a se pronunciar sobre o assunto.¹⁵⁴ O que está em discussão é se uma subsidiária local de um ISP pode ser chamada para produzir provas mantidas pela matriz fora do país e se o artigo 11 do Marco Civil da Internet, que declara que a lei brasileira se aplica a dados coletados no Brasil ou a partir de um dispositivo no Brasil, fornece uma base suficiente para contornar o tratado MLA com os Estados Unidos e solicitar diretamente dados armazenados no exterior.

153 Ver: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en>. Acesso em: 09 mai 2021.

154 Brasil, Supremo Tribunal Federal (STF), "Ação direta de constitucionalidade", nº 51. Disponível em : <<http://portal.stf.jus.br/processos/detalhe.asp?incidente=5320379>>. Acesso em: 09 mai 2021.

3. VIGILÂNCIA

A Internet pode ser um instrumento de libertação, facilitando o acesso à informação e permitindo a sua difusão global. Muitas vezes, isso tem facilitado a comunicação, o encontro, a troca de ideias, a união de forças e o acesso a diferentes tipos de bens e serviços. Ao mesmo tempo, porém, a Internet permite que todas essas ações sejam rastreadas e localizadas. Coletâneas de dados sobre hábitos, gostos e a movimentação das pessoas tornaram-se mais facilmente disponíveis. O comportamento on-line e, até certo ponto, off-line, pode ser mapeado e tornado acessível. Assim, a vigilância se revelou uma realidade a ser enfrentada, e não apenas do ponto de vista de sistemas de monitoramento ou inteligência muito sofisticados. Tanto o setor público quanto o privado, e atualmente talvez mais as empresas do que os órgãos estatais, são capazes de monitorar a população.

Esses dois lados da Internet tendem a ser difíceis de conciliar. Iniciativas importantes podem, deliberada ou inadvertidamente, levar à vigilância. Muitos sistemas de segurança social e de benefícios sociais são informados pela análise de dados e pela formulação de políticas públicas orientadas por dados. Tornar a alocação de recursos mais eficiente, reduzir fraudes, encontrar e distribuir bens e serviços para aqueles que os necessitam ou merecem e se enquadram nos critérios são objetivos muito importantes. Todos eles podem ser melhor alcançados com mais dados e melhor supervisão e análise.

O outro lado desta maior eficiência é que as ferramentas usadas para alcançá-la também podem ser usadas para vigilância. Há um alto risco de que a coleta de tais dados possa invadir muitos direitos fundamentais e que essa riqueza de informações possa ser mal utilizada ou empregada para discriminar, perseguir ou deixar os mais vulneráveis ainda pior do que antes.

Na América Latina e no Caribe, foram relatados casos em que quantidades significativas de dados pessoais foram coletados no âmbito de programas sociais, providências de transporte público e até mesmo eventos populares. O impacto on-line da pandemia aumentou essa tendência.¹⁵⁵ Tais dados tendem a ser

155 Ver: <https://ia801905.us.archive.org/23/items/data-justice-and-covid-19/Data_Justice_and_COVID-19.pdf> . Acesso em: 09 mai 2021.

compilados com ênfase nas porções marginalizadas e mais vulneráveis da população. Isso pode levar à exclusão, ao tratamento desigual e até mesmo discriminação, independentemente do risco de violação de dados.¹⁵⁶ Também na região, certos grupos tendem a ter um risco particularmente alto de vigilância. Estes incluem jornalistas e defensores dos direitos humanos e também ativistas políticos e artistas.¹⁵⁷

Outra questão diz respeito ao uso de tecnologias nas áreas públicas. Muitos países da América Latina e do Caribe estão flertando com a possibilidade de implementar sistemas de reconhecimento facial em ruas e parques e em eventos públicos.¹⁵⁸ O objetivo é frear a criminalidade e aumentar a segurança pública. A tecnologia pode, entretanto, ter um impacto sobre outros direitos, tais como a liberdade de expressão e de reunião, o direito de protesto e à privacidade.¹⁵⁹

A vigilância tende a ser analisada a partir de uma perspectiva nacional, mas na América Latina e no Caribe as implicações transfronteiriças são claramente visíveis. Em vários casos, as ferramentas usadas para coletar e analisar dados ou que estão por trás de tecnologias como o reconhecimento facial tendem a

156 Ver: <<https://www.derechosdigitales.org/1392/vigilancia-control-social-e-desigualdade-a-tecnologia-reforca-vulnerabilidades-estructurais-na-america-latina/>>. Acesso em: 09 mai 2021.

157 Ver: <http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_Violence_WEB.pdf>. Acesso em: 09 mai 2021.

158 Vários países têm iniciativas desse tipo. Para mencionar apenas alguns, eles incluem a Argentina (ver: <https://documentosboletinoficial.buenosaires.gob.ar/publico/ck_PE-RES-MJYSGC-MJYSGC-398-19-5604.pdf>. Acesso em: 09 mai 2021.); Brasil (ver: <<https://www1.folha.uol.com.br/cotidiano/2019/11/151-pessoas-sao-presas-por-reconhecimento-facial-no-pais-90-sao-negras.shtml>>. Acesso em: 09 mai 2021); Chile (ver: <<https://www.infodefensa.com/latam/2020/04/08/noticia-ingesmart-implementara-chile-sistema-teleproteccion-cameras.html>> Acesso em: 09 mai 2021.); Paraguai (ver: <<https://www.tedic.org/quien-vigila-al-vigilante-reconocimiento-facial-en-asuncion/#sdfootnote1sym>>. Acesso em: 09 mai 2021.); e El Salvador, Honduras e Nicarágua (ver: <https://acceso.or.cr/assets/files/Art_Herramientas_Vigilancia_CA-mayo2020.pdf>. Acesso em: 09 mai 2021.). Para uma visão geral das iniciativas na região, ver: <<https://reconocimientofacial.info>>. Acesso em: 09 mai 2021.

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", Outubro de 2019. Disponível em: <https://adc.org.ar/wp-content/uploads/2019/10/AL-SUR_Contribution_New-technologies-in-the-context-of-assemblies-and-peaceful-protests.pdf>. Acesso em: 09 mai 2021.

ser implementadas através de parcerias público-privadas, principalmente com empresas multinacionais. Assim, a tecnologia empregada é frequentemente estrangeira, os servidores onde os dados são armazenados (geralmente serviços em nuvem) na maioria das vezes estão fora da região, e os países vizinhos frequentemente recebem ofertas similares ou competem pelos mesmos serviços. Conflitos jurisdicionais transnacionais, então, deverão ocorrer com certa frequência.

3.1. Criptografia

Quanto mais serviços se tornarem on-line, mais clara a necessidade de segurança. A criptografia é uma das peças do quebra-cabeças de segurança. Um enorme número de serviços de Internet depende da criptografia para a sua confiabilidade.¹⁶⁰ As transações bancárias e financeiras são as primeiras que vêm à mente, mas outras incluem fechaduras eletrônicas, câmeras de segurança, compartilhamento de informações sensíveis e até mesmo reservas de viagens. A pandemia deixou clara a necessidade de criptografia das interações com médicos, hospitais e telemedicina.¹⁶¹ A criptografia é uma pedra angular e, até certo ponto, um pré-requisito para todas essas relações on-line.

O uso de criptografia, no entanto, teve um impacto em outras áreas. Pode ocultar informações importantes dos agentes policiais e de inteligência, criando, assim, tensões entre o uso da criptografia para proteger a privacidade e outros direitos fundamentais muito importantes, por um lado, e a segurança e proteção públicas, por outro. Argumenta-se que o Estado deveria ter acesso às informações que são compartilhadas, mesmo quando codificadas, a fim de proteger a população contra criminosos, terroristas e outras fontes de perigo. Caso contrário, a criptografia atua como uma barreira a este trabalho legítimo e protege os culpados, aqueles que tentam subverter a ordem e causar danos.

160 R. Polk and A. Froncek, "Your day with encryption", Internet Society, 2019. Disponível em: <<https://www.internetsociety.org/blog/2019/10/your-day-with-encryption/>> . Acesso em: 09 mai 2021.

161 Para uma visão geral, ver: D. Rozario, "Secure health care messaging in the era of COVID-19", IAPP, Agosto de 2020. Disponível em: <<https://iapp.org/news/a/secure-health-care-messaging-in-the-era-of-covid-19/>> . Acesso em: 09 mai 2021.

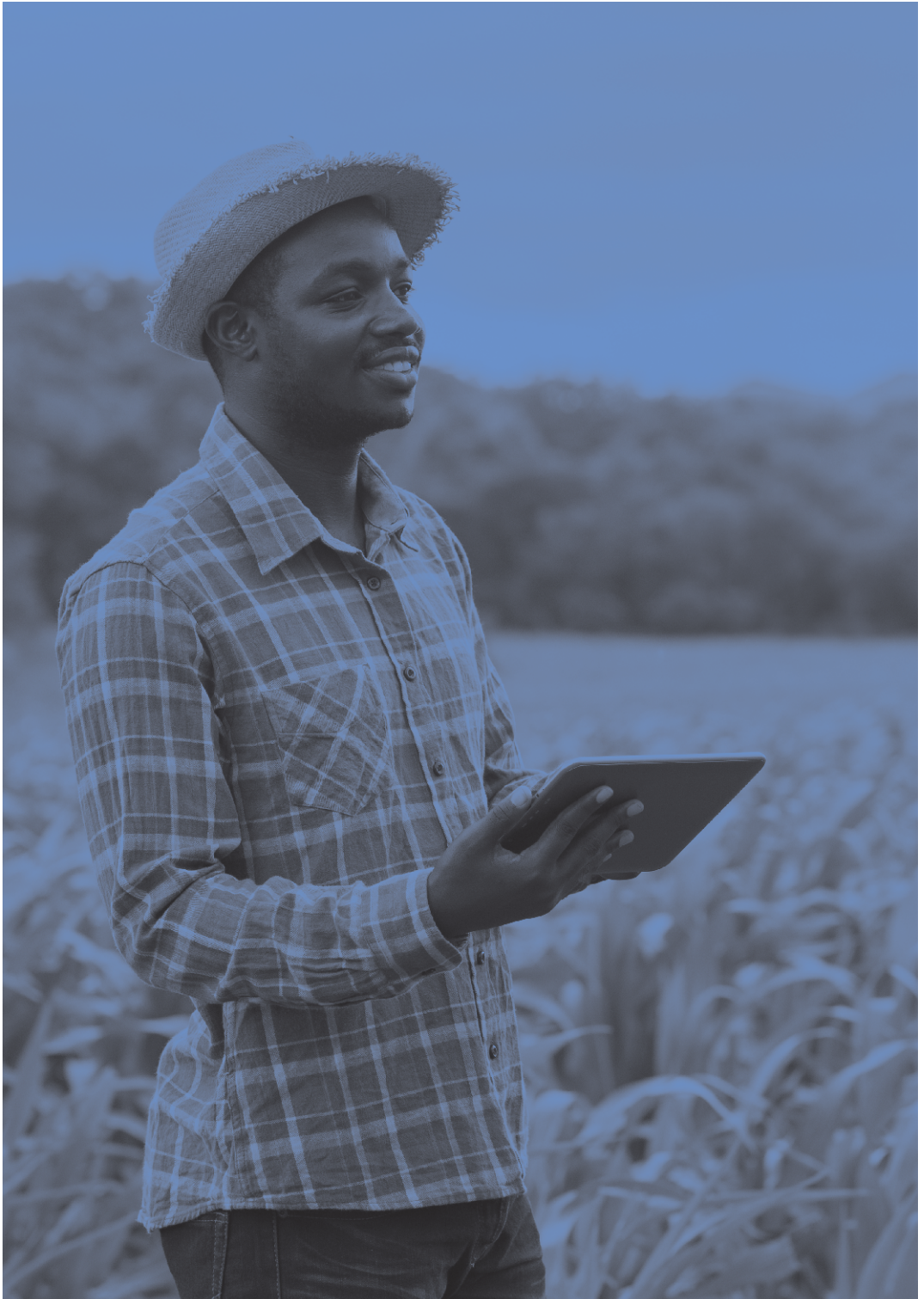
Essa tensão levou a um debate técnico, jurídico e ético que ainda não foi finalmente resolvido. Ambos os lados têm pontos válidos e encontrar o equilíbrio certo entre manter a criptografia para muitos propósitos diferentes e permitir o acesso a dados relevantes por razões de segurança nacional e de segurança pública não é uma tarefa fácil. Na América Latina e no Caribe, a discussão surgiu de diferentes formas: agências de execução da lei exigindo acesso aos dados (particularmente de aplicativos de mensagens) apesar da criptografia, ordenando a coleta de mais informações (com possíveis impactos nos protocolos de criptografia) e solicitando a instalação de acesso por *backdoors* (semelhante a escutas telefônicas).

3.2. Acesso às informações e mensagens criptografadas por autoridades de execução da lei

O acesso a informações criptografadas e mensagens para fins de execução da lei poderia ser solicitado de diferentes maneiras. Os governos poderiam ordenar às empresas que criem mecanismos de criptografia que forneçam uma chave-mestra para que, sob certas condições, possam acessar quaisquer informações solicitadas, conforme necessário.¹⁶² A administração pública poderia solicitar às empresas com acesso a mensagens criptografadas que precisem divulgar essas informações de forma não criptografada, sem considerar como a decodificação deve ser feita.

Do ponto de vista da implementação da lei, a situação na América Latina e no Caribe, durante uma investigação, e com a devida razão, os agentes poderiam exigir que empresas e indivíduos divulguem informações. O uso ou não da criptografia não é necessariamente um problema que o sistema legal aborda. Na esmagadora maioria dos casos, o entendimento é que, se uma empresa presta o serviço em um país, deve cumprir ordens válidas emitidas por suas agências de execução da lei e, em particular, pelas autoridades judiciais.

162 H. Abelson and others, "Keys Under Doormats: Mandating Insecurity by Requiring Government Access to all Data and Communications", Massachusetts Institute of Technology (MIT), 2015. Disponível em: <<http://dspace.mit.edu/bitstream/handle/1721.1/97690/MIT-CSAIL-TR-2015-026.pdf>>. Acesso em: 09 mai 2021.



Devido à forma como os protocolos de criptografia foram desenvolvidos, as empresas intermediárias nem sempre são capazes de fornecer tais informações, seja porque não as possuem mais (sua arquitetura não prevê o armazenamento de mensagens criptografadas) ou porque não têm acesso à chave para descriptografar (com criptografia de ponta a ponta, a chave privada geralmente está nos dispositivos de troca de informações e não está disponível para a empresa intermediária).¹⁶³

Isso pode levar a situações difíceis, como aconteceu na região. O uso de criptografia tornou-se controverso,¹⁶⁴ e os PSIs foram pegos no fogo cruzado. Os aplicativos foram bloqueados por ordem judicial e os funcionários da empresa tiveram até mesmo que enfrentar a prisão por desobediência a ordens de entrega de mensagens (como explorado mais adiante na seção V.B.4).

3.3. Um debate difícil em torno do anonimato

A região tradicionalmente tem se debatido com a ideia de anonimato. Tem-se a ideia de que o anonimato está muito próximo da impunidade e instrumentos que permitem o conteúdo anônimo tendem a ser vistos com maus olhos. O uso de máscaras ou dispositivos similares durante protestos é um exemplo.¹⁶⁵ Da mesma forma, aplicativos que permitem mensagens anônimas foram contestados dentro e fora dos tribunais.¹⁶⁶

163 K. Ermoshina, F. Musiani and H. Halpin, "End-to-end encrypted messaging protocols: an overview", International Conference on Internet Science, 2016. Disponível em: <https://link.springer.com/chapter/10.1007%2F978-3-319-45982-0_22>. Acesso em: 09 mai 2021.

164 Ver: <http://www2.stf.jus.br/portalStfInternacional/cms/destaquesClipping.php?sigla=portalStfDestaque_en_us&idConteudo=330687>. Acesso em: 09 mai 2021.

165 Ver: <<https://www.derechosdigitales.org/wp-content/uploads/freedom-of-expression-encryption-and-anonymity1.pdf>>. Acesso em: 09 mai 2021.

166 Tech Crunch, "Brazil Court Issues Injunction Against Secret and Calls for App to Be Remotely Wiped", 2014. Disponível em: <<http://techcrunch.com/2014/08/20/brazil-court-issues-injunction-against-secret-and-calls-for-app-to-be-remotely-wiped/>>. Acesso em: 09 mai 2021.

A capacidade de trocar mensagens em uma longa cadeia, mesmo que não sejam conteúdos anônimos em si, tende a criar uma situação em que encontrar a origem ou a fonte de uma mensagem específica pode ser um desafio. Isso parece ser particularmente grave no contexto de campanhas de desinformação e potencialmente pior durante as eleições.¹⁶⁷ Assim, no Brasil, por exemplo, um projeto de lei exigindo a coleta de informações sobre todas as mensagens que passam a ser “virais” (encaminhadas mais de 1.000 vezes) está atualmente em análise pelo Congresso.¹⁶⁸ Os serviços de mensagens seriam obrigados a rastrear a origem de tais mensagens, de modo que se seu conteúdo causar danos ou for considerado criminoso, o culpado será mais facilmente identificado. Não apenas a lei exigiria a retenção de dados pessoais não essenciais, mas os especialistas afirmam que os protocolos de criptografia usados pelos serviços podem ser enfraquecidos se eles tiverem que cumprir as exigências da lei.¹⁶⁹

A situação é inquestionavelmente difícil e exige uma análise cuidadosa para determinar se essa é uma resposta proporcional ou se não há outras medidas disponíveis que não comportem os mesmos riscos. O Sistema Interamericano de Direitos Humanos tem ressaltado a importância de respostas aos desafios envolvendo acesso à informação para fins de execução da lei e desinformação para proteger e não prejudicar a “integridade dos sistemas de computador nos quais a Internet funciona e as comunicações que são canalizadas através da rede”, incluindo seus protocolos de criptografia.¹⁷⁰

167 Ver: <<https://en.ejo.ch/specialist-journalism/mexicos-election-and-the-fight-against-disinformation>>. Acesso em: 09 mai 2021.

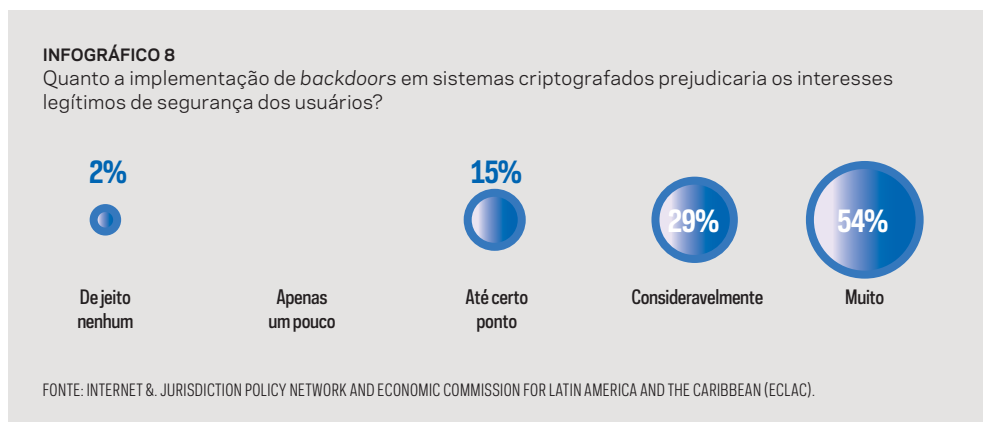
168 A região não está sozinha; medidas semelhantes foram sugeridas na Índia. Ver: <<https://www.policyforum.net/encryption-and-attribution-indias-fake-news-problem/>>. Acesso em: 09 mai 2021.

169 Ver: <<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>>. Acesso em: 09 mai 2021. Veja também: <<https://www.eff.org/deeplinks/2020/06/current-brazils-fake-news-bill-would-dismantle-crucial-rights-online-and-fast>>. Acesso em: 09 mai 2021.

170 Ver: <https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf>. Acesso em: 09 mai 2021.

3.4. As *backdoors* são percebidas como capazes de minar a confiança em sistemas criptografados

Os entrevistados se manifestaram claramente contra a inclusão de *backdoors* em sistemas criptografados. Quando perguntados se essa característica prejudicaria os legítimos interesses de segurança dos usuários, 82,93% dos entrevistados afirmaram que prejudicariam.



Essa constatação é importante porque as agências de execução da lei em países da América Latina e do Caribe estão pressionando por uma maneira de descriptografar o conteúdo das mensagens enviadas através de aplicativos de mensagens instantâneas. Como aplicativos como o WhatsApp têm se tornado cada vez mais populares na região, tem havido uma pressão crescente para refrear a criptografia de ponta-a-ponta a fim de fornecer alguma forma de acesso ao conteúdo das mensagens para investigações criminais.

Deve-se ressaltar que a criptografia é essencial para a confiança não apenas nos aplicativos de mensagens, mas também no comércio eletrônico, nos serviços bancários pela Internet e em todos os tipos de atividades on-line. Quebrar a criptografia para um usuário pode significar quebrá-la também para todos os outros. Ao mesmo tempo, existem outras formas de acessar o conteúdo de uma mensagem em uma investigação devidamente autorizada que não prejudicaria a integridade dos sistemas criptografados, mesmo no caso de aplicativos de mensagens instantâneas criptografadas de ponta-a-ponta. Elas incluem a obtenção de acesso

ao dispositivo real usado para comunicação (como um telefone celular) e a infiltração de agentes da lei em grupos de mensagens.

As agências de execução da lei da região estão explorando alternativas como o amadurecimento do debate legal sobre a criptografia.¹⁷¹ Os dados que estão disponíveis – metadados ou dados de outras fontes – podem ser aproveitados para encontrar as respostas necessárias. O uso de estratégias de investigação modernas é primordial para equilibrar o debate e manter a segurança nacional e a segurança pública, mantendo à distância violações de privacidade, ameaças à segurança cibernética e vigilância ilegítima, estrangeira ou não.

Essas situações podem parecer uma questão doméstica, mas têm implicações transfronteiriças e até internacionais. A maioria dos serviços criptografados tem um alcance global, sendo usado em várias jurisdições. Se a criptografia for prejudicada em benefício da execução da lei de um país, pode muito bem ter um efeito sobre todos os outros. Pode haver um efeito cascata não só para os indivíduos que vivem em países democráticos onde os direitos humanos são respeitados, mas também para os defensores dos direitos humanos em regimes mais autoritários. Outro aspecto é que um número significativo de empresas que oferecem serviços com criptografia incorporada pode realmente estar usando protocolos internacionais ou interfaces de programação de aplicativos (APIs) de outras corporações, nacionais ou estrangeiras, de modo que o impacto poderia se estender além do fornecedor direto do serviço.

Onde quer que o debate possa ir, é importante ter em conta a complexidade dos direitos e interesses que estão sendo equilibrados e o fato de que qualquer negócio pode ser atingido poderia ter um impacto para além do país que os implementa e afetar todos os grupos, inclusive os vulneráveis.

171 Ver: <<https://carnegieendowment.org/2019/05/30/encryption-debate-in-brazil-pub-79219>>. Acesso em: 09 mai 2021.

COMPUTAÇÃO QUÂNTICA E CRIPTOGRAFIA

A criptografia depende da dificuldade e do tempo envolvidos em encontrar a combinação para decifrar qualquer mensagem. Em outras palavras, a criptografia só funciona porque é difícil e demorado forçar o bloqueio. Novas tecnologias, como a computação quântica, que aumentam a velocidade da computação, podem ter um efeito duplo, criando criptografias ainda mais difíceis de quebrar e tornando globalmente inúteis os sistemas disponíveis.¹⁷² Embora ainda seja provavelmente necessário grandes avanços no desenvolvimento tecnológico para obter computadores quânticos em funcionamento, o mero conceito ajuda a destacar a importância da energização e a forma como uma única chave, ou uma única mudança tecnológica, tem o potencial de causar estragos e colocar em risco inúmeras transações vitais.

4. SEGURANÇA CIBERNÉTICA

A importância de proteger o ciberespaço tem crescido exponencialmente nos últimos anos. A pandemia tem destacado a crescente dependência tecnológica da infraestrutura e dos serviços básicos dos países, como energia, água, saneamento, transporte e cadeias de abastecimento de alimentos, transações financeiras, serviços públicos e até mesmo o funcionamento dos procedimentos governamentais. Todos esses serviços são importantes alvos para ataques cibernéticos.

Vários incidentes cibernéticos importantes tiveram origem em Estados da América Latina e do Caribe ou visaram vítimas nesses locais.¹⁷³ Tais incidentes só aumentaram com a expansão da conectividade e do número de indivíduos que acessam a Internet. Os crimes cibernéticos com motivação econômica envolvendo *malware* financeiro e fraude com cartões de crédito e bancos on-line tendem a se destacar fortemente entre as ameaças na América Latina e no Caribe,¹⁷⁴ dando a entender que a segurança pública e nacional está intimamente ligada

172 Ver: <<https://carnegieendowment.org/2019/04/25/implications-of-quantum-computing-for-encryption-policy-pub-78985>>. Acesso em: 09 mai 2021.

173 Norton, "2017 Cyber Security Insights Report. Global Results", 2017. Disponível em: <<https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf>>. Acesso em: 09 mai 2021.

174 "ThreatMetrix Cybercrime Report: An Interview", Novembro 2019. Disponível em: <<https://resources.infosecinstitute.com/threatmetrix-cybercrime-report-an-interview/>>

à segurança cibernética. No entanto, vários países da região ainda têm apenas uma gama limitada de ferramentas, capacidades e instituições para se preparar, identificar e responder aos ataques.¹⁷⁵

Ultimamente, cada vez mais incidentes cibernéticos têm cruzado fronteiras, exigindo cooperação e coordenação internacional para sua resolução. Essa camada internacional para esforços cibernéticos mostra a necessidade de abordagens, padrões e normas comuns, para não mencionar os recursos e a capacidade de montar defesas e aumentar a resiliência. É necessário proteger não só a infraestrutura crítica, mas toda a infraestrutura de informação e comunicação: não apenas de um ou outro país, mas da própria região.

Os níveis de preparação e resiliência na região são muito desiguais. Apenas pouco mais de um terço de seus países tem uma estratégia de cibersegurança (Argentina, Brasil, Chile, Colômbia, Costa Rica, República Dominicana, Guatemala, Jamaica, México, Panamá, Paraguai e Trinidad e Tobago). Um pouco menos (10) têm uma agência governamental responsável pela gestão e coordenação de segurança cibernética. Vinte países da região têm equipes de resposta a incidentes de segurança cibernética (CSIRTs), também comumente referidas como equipes de resposta a emergências de computadores (CERT).¹⁷⁶

É evidente que ainda há muito a ser feito em termos de implementação nacional e de cooperação internacional e regional. No nível das CERTs, há cooperação e coordenação quando são encontrados riscos e incidentes em larga escala. CSIRTAmericas.org, uma plataforma para CSIRTs lideradas por governos nas Américas, serve como uma ferramenta de rede para alertas de ataques de negação de serviço (DDoS) antecipados, alerta de ataque distribuído e construção de capacidade.¹⁷⁷ O Registro

175 Organização dos Estados Americanos (OEA) /Banco Interamericano de Desenvolvimento (IDB), Cybersecurity Report, 2020. Disponível em: <<https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf>>. Acesso em: 09 mai 2021.

176 Ibidem.

177 Ver: <<https://the-gfcoe.instantmagazine.com/magazine/global-cyber-expertise-magazine-volume-5/csirtamericasorg/overlay/strengthening-incident-response-capabilities-in-the-americas/>>. Acesso em: 09 mai 2021.

de Endereços Internet da América Latina e Caribe (LACNIC) também criou sua própria CERT.¹⁷⁸

Há também muito espaço para melhorias na estrutura de governança de segurança cibernética. A inclusão dos diferentes atores (não só governos, mas também empresas, sociedade civil, academia e comunidade técnica) é crucial para o sistema global, tanto para superar a “mentalidade de silo” quanto para garantir uma abordagem sistêmica.¹⁷⁹ Trata-se de um processo em curso, tanto a nível nacional quanto regional. A participação de diferentes atores é uma característica das discussões no nível da Organização dos Estados Americanos. No âmbito do Comitê Interamericano contra o Terrorismo (CICTE), o programa de segurança cibernética é um grande esforço de coordenação e adota uma abordagem multissetorial.¹⁸⁰

Este é também o caso em importantes intersecções entre os níveis regional e internacional. Por exemplo, nas consultas regionais do Grupo de Especialistas Governamentais das Nações Unidas sobre o Avanço do comportamento responsável do Estado no ciberespaço no contexto da segurança internacional, realizadas com a Organização dos Estados Americanos, empresas, sociedade civil, academia e a comunidade técnica foram convidadas a comentar e participar das discussões.¹⁸¹

No nível regional, dois instrumentos destacam a importância da segurança cibernética e fornecem uma estrutura para compromissos comuns e cooperação: a Declaração de 2012 sobre o Fortalecimento da Cibersegurança nas Américas¹⁸² e a Declaração sobre a Proteção da Infraestrutura Crítica contra Ameaças Emergentes de 2015.¹⁸³

178 Ver: <<https://www.lacnic.net/4464/2/lacnic/>>

179 Organização dos Estados Americanos (OEA) /Banco Interamericano de Desenvolvimento (IDB), Cybersecurity Report, 2020. Disponível em: <<https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf>>. Acesso em: 09 mai 2021.

180 Ver: <<http://www.oas.org/en/sms/cicte/default.asp>>. Acesso em: 09 mai 2021.

181 Ver: <<https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf>>. Acesso em: 09 mai 2021.

182 Ver: <https://www.oas.org/en/sms/cicte/Documents/Declarations/DEC_1%20rev_1_DECLARATION_CICTE00749E04.pdf>. Acesso em: 09 mai 2021.

183 Ver: <<https://www.sites.oas.org/cyber/EN/Pages/contacts.aspx>>. Acesso em: 09 mai 2021. Ver também: <<https://www.oas.org/es/sms/cicte/cipreport.pdf>>. Acesso em: 09 mai 2021.

As disposições relativas às infrações cibernéticas na legislação penal são geralmente outra peça do quebra-cabeça. Os países da região ainda não adaptaram plenamente suas legislações às exigências da luta contra o cibercrime. Quanto à camada internacional, cinco países são partes na Convenção de Budapeste sobre o cibercrime.¹⁸⁴ Nesse processo de inclusão da cibersegurança nas agendas nacionais, algumas legislações de segurança cibernética resultaram em restrições aos direitos digitais. Na América Latina e no Caribe, a proposta de Lei Constitucional sobre o Ciberespaço da República Bolivariana da Venezuela tem sido relatada para afirmar amplos poderes no interesse do que é chamado de “defesa abrangente” do país.¹⁸⁵

Alcançar o justo equilíbrio entre a promoção da cibersegurança e, ao mesmo tempo, evitar violações dos direitos fundamentais é uma questão delicada e deve ser uma preocupação permanente para todos os Estados da região. Assim, as medidas de criação de confiança e confiabilidade são importantes para fortalecer a compreensão dos diferentes atores e dos desafios que existem no nível nacional e internacional.

4.1. As violações de segurança expuseram vulnerabilidades no processamento de dados

Atualmente, os incidentes de segurança da informação e violações de dados são comumente relatados. Já foram vazados dados sobre um enorme número de indivíduos. Na maioria das vezes, resultam de erro humano, seja devido a uma falha na configuração adequada dos parâmetros de segurança, deixando espaço para os intrusos explorarem, ou devido a erros básicos como o uso de senhas fáceis de adivinhar e hackear ou mesmo o acesso de *malware* de um e-mail ou mensagem em um computador ou dispositivo sem verificar corretamente sua fonte.

Em 2019, por exemplo, dados sobre quase toda a população do Equador foram expostos: informações detalhadas sobre adultos e crianças, inclusive endereços, relações familiares e situação financeira, emprego e dados escolares, estavam disponíveis em

184 Ver: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=XXw51amG>. Acesso em: 09 mai 2021.

185 Ver: <https://freedomhouse.org/country/venezuela/freedom-net/2019#footnoteref5_7rkdmen>. Acesso em: 09 mai 2021.

um servidor inseguro e de fácil acesso em Miami.¹⁸⁶ Isso mostra a extensão do risco e a sua natureza global.

Os serviços digitalizados não precisam respeitar fronteiras. As informações não precisam ser, e muitas vezes não são, armazenadas ou processadas no país onde são coletadas. As ofertas internacionais de serviços se tornam uma opção importante para alcançar escalabilidade e eficiência de custos. No entanto, esses serviços estão propensos a incidentes de segurança que afetam mais de uma jurisdição.

Os casos de intrusão intencional e apropriação de informações pessoais também se tornaram mais comuns. Eles variam de procedimentos simples a fraudes mais complexas e hackeamento. A origem e a motivação das intrusões podem variar, desde espionagem corporativa até vigilância por uma potência estrangeira.¹⁸⁷ Alguns casos podem envolver motivos aparentemente mais altruístas, como a exposição do crime e da corrupção. O escândalo “Panama Papers” se enquadra nesta categoria.¹⁸⁸

4.2. O desenvolvimento de dados biométricos e identidades digitais tem sido uma fonte de controvérsia

Os serviços estão migrando para o ciberespaço e se tornando totalmente digitais. O serviço bancário é um exemplo de serviço no qual a maioria das funções pode operar on-line sem necessariamente haver necessidade de uma presença física. Outros serviços, incluindo os serviços prestados pelas autoridades públicas, estão sendo estruturados da mesma forma.¹⁸⁹ Isso traz ganhos em escala e eficiência. Um idoso que recebe uma pensão do Estado, por exemplo, não precisa necessariamente comparecer diante de um funcionário público para provar que está vivo: existem métodos digitais que envolvem menos esforço do indivíduo e menos custos para a administração.

186 Ver: <<https://www.nytimes.com/2019/09/17/world/americas/ecuador-data-leak.html>>. Acesso em: 09 mai 2021.

187 Ver: <<https://www.theguardian.com/world/2013/sep/24/brazil-president-un-speech-nsa-surveillanc>>. Acesso em: 09 mai 2021.

188 Ver: <<https://www.icij.org/investigations/panama-papers/pages/panama-papers-about-the-investigation/>>. Acesso em: 09 mai 2021.

189 Informações sobre a América Latina na Pesquisa de Governo Eletrônico das Nações Unidas, 2018. Disponível em: <<https://www.un.org/development/desa/publications/2018-un-e-government-survey.html>>. Acesso em: 09 mai 2021.

No entanto, essa mudança traz o desafio de autenticar a identidade de uma pessoa: confirmar que um indivíduo é realmente quem ele afirma ser. Um sistema de identificação digital parece ser uma maneira de resolver essas dificuldades e autenticar inequivocamente uma pessoa. Uma identificação digital pode atuar como chave para desbloquear o acesso aos serviços digitais, reduzindo os custos de transação, ao mesmo tempo em que aumenta a eficiência.¹⁹⁰

Vários Estados da América Latina e do Caribe estão explorando formas de instituir a identidade digital. Ao contrário de outras regiões do mundo, porém, esses países geralmente têm um sistema de identidade nacional já em vigor,¹⁹¹ o que facilita e complica o processo.¹⁹² Os protocolos e as disposições de segurança disponíveis não se estendem necessariamente ou se encaixam bem com os requisitos das identidades digitais. Os riscos e preocupações não estão perfeitamente alinhados. Entre eles, estão o acesso não autorizado e o controle de dados pessoais e questões relacionadas à inclusão digital e à segurança cibernética.¹⁹³

Muitos dos esforços que estão sendo feitos para criar identidades digitais estão provocando uma variedade de questões transfronteiriças potenciais relacionadas à forma como elas podem ser usadas on-line e seu impacto além das fronteiras do país em questão. Surgem dúvidas sobre os locais onde os dados são armazenados, as origens das ameaças potenciais à segurança cibernética e a melhor forma de gerenciar os mecanismos

190 World Bank, Principles on Identification for Sustainable Development: Toward the Digital Age. Disponível em: <<http://documents1.worldbank.org/curated/en/213581486378184357/pdf/Principles-on-identification-for-sustainable-development-toward-the-digital-age.pdf>>. Acesso em: 09 mai 2021.

191 Inter-American Development Bank (IDB), "Registros civiles y oficinas de identificación: análisis y fichas de país", 2019. Disponível em: <<http://dx.doi.org/10.18235/0001865>>. Acesso em: 09 mai 2021.

192 É importante notar que os países da América Latina e do Caribe não alcançaram registro de nascimento universal, o que significa um problema potencial também para a inclusão geral. Ver: United Nations Children's Fund (UNICEF), "Birth Registration in Latin America and the Caribbean: Closing the Gaps", 2016. Disponível em: <<https://data.unicef.org/resources/birth-registration-latin-america-caribbean-closing-gaps/>>

193 McKinsey, Digital Identification: A Key to Inclusive Growth, 2019. Disponível em: <<https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-identification-a-key-to-inclusive-growth>>. Acesso em: 09 mai 2021.

de registro, autenticação e autorização.¹⁹⁴ O bloqueio de fornecedores, o uso de tecnologia própria, sistemas não-interoperáveis e serviços em nuvem (armazenamento internacional e processamento de dados) também são fatores importantes.¹⁹⁵ Dependendo de como esses desafios forem respondidos, questões de eficiência, inclusão, transparência, segurança, resiliência e privacidade entrarão em jogo de diferentes maneiras.¹⁹⁶

Com esquemas baseados em nuvem, por exemplo, os dados podem ser armazenados no exterior e em vários locais. Lidar com acesso, transferências de dados e incidentes de segurança pode ter grandes repercussões jurisdicionais transfronteiriças que vão além de questões mais comuns de armazenamento de dados da administração pública eletrônica. Um exemplo é a investigação de violações ou crimes relacionados a esses serviços, que se baseia fortemente na cooperação internacional.

O fato de que essas identidades digitais são geralmente acompanhadas por atributos biométricos pessoais capturados eletronicamente (impressões digitais, íris, imagens faciais etc)¹⁹⁷ torna essas decisões ainda mais significativas. Uma pessoa não pode cancelar e reemitir seu rosto ou impressões digitais se os dados biométricos forem vazados, como aconteceria com um cartão de crédito roubado, por exemplo. Isso torna a estruturação de tais soluções uma prioridade e significa que especificações cibernéticas de segurança de alto nível são necessárias desde a concepção.

Uma última questão é que o reconhecimento mútuo das identificações pode ser um motor da integração regional e econômica, incluindo um mercado único digital. Os países do Mercado Comum do Sul (MERCOSUL) reconhecem as identificações uns

194 Ver: <<https://id4d.worldbank.org/guide/hosting-options>>. Acesso em: 09 mai 2021.

195 Isso aconteceu em outras regiões. Para fins de comparação, ver: <http://documents1.worldbank.org/curated/pt/L56111493234231522/pdf/L14628-wp-68p-thestateofidentificationsystemsinafricasynthesisofidAssessments-PUBLIC.pdf>

196 S. Bhadra, Five Surprisingly Consequential Decisions Governments Make About Digital Identity, 2019. Disponível em: <<https://www.omidyar.com/blog/five-surprisingly-consequential-decisions-governments-make-about-digital-identity>>. Acesso em: 09 mai 2021.

197 A. Gelb and J. Clark, "Identification for development: the biometrics revolution", CGD Working Paper, No. 315, Washington, D.C., Center for Global Development, 2013. Disponível em: <<https://www.cgdev.org/publication/identification-development-biometrics-revolution-working-paper-315>>. Acesso em: 09 mai 2021.

dos outros para fins de migração, o que é um primeiro passo. Várias iniciativas de assinatura eletrônica prosperaram tanto no MERCOSUL quanto em outros arranjos regionais.¹⁹⁸ Entretanto, é o reconhecimento das identidades digitais que pode destravar o maior potencial de circulação de bens, serviços e negócios em toda a região e impulsionar a economia digital.¹⁹⁹

Vários países da região estão se movendo para digitalizar seus documentos de identificação. A Argentina, por exemplo, integrou seu processo dentro do Sistema de Identidade Digital (SID). Da mesma forma, o Uruguai tornou-se líder no governo eletrônico e implementou um programa de digitalização que abrange toda a sua população. O Peru introduziu recentemente um sistema de Identidade Nacional de Eletrônica (DNI-e), que dá acesso a uma série de serviços governamentais.²⁰⁰ No que diz respeito às aplicações, graças ao amplo uso de identidades digitais, os benefícios de ajuda emergencial aprovados pelo governo chileno no início da pandemia foram rapidamente colocados à disposição da população mais necessitada, embora tenha sido aplicado um forte mecanismo de verificação.²⁰¹

C. Economia

1. COMÉRCIO ELETRÔNICO: A ASPIRAÇÃO A UM MERCADO ÚNICO DIGITAL

Não é surpresa que a Internet tenha criado uma mudança de paradigma no comércio internacional. A infraestrutura comercial desenvolvida ao longo de milênios para a troca de mercadorias através de transações comerciais internacionais enfrenta grandes desafios no esforço de se ajustar à velocidade e variedade de transações apresentadas por oportunidades on-line. O

198 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market: strategic aspects", 2018. Disponível em: <https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf>. Acesso em: 09 mai 2021.

199 Ver: <<https://id4d.worldbank.org/guide/mutual-recognition-ids-across-borders-0>>. Acesso em: 09 mai 2021.

200 Inter-American Development Bank (IDB), "Registros civiles y oficinas de identificación: análisis y fichas de país", 2019. Disponível em: <<http://dx.doi.org/10.18235/0001865>>. Acesso em: 09 mai 2021.

201 World Bank, "Harnessing the power of Digital ID", 20 Ago 2020. Disponível em: <<https://blogs.worldbank.org/voices/harnessing-power-digital-id>>. Acesso em: 09 mai 2021.

acesso ao mercado de bens e até mesmo serviços é qualitativa e quantitativamente diferente on-line. As novas tecnologias baseadas na Internet reduziram os custos do comércio transfronteiriço. Tanto os serviços quanto os bens cruzam fronteiras, independentemente do volume ou do valor. Com custos mais baixos, empresas de todos os tamanhos podem ser integradas na cadeia de valor internacional e participar no comércio global.

O fato de que a Internet não está baseada em um país ou outro significa que uma pessoa no país “A” pode fornecer serviços ou bens a alguém no país “B” através de uma plataforma – um serviço intermediário – que não está em nenhum dos dois países. Isso acontece claramente com o *streaming* de música e vídeo, bens (especificamente, comércio eletrônico), mídia, finanças, saúde e outros serviços. Esse tipo de comércio internacional pode vir em diferentes formatos e formas: transações entre empresas (B2B), transações entre empresas e consumidores (B2C) e transações entre empresas e governos (B2G). O denominador comum entre tais transações é que a Internet tem facilitado o acesso a mercados além das fronteiras nacionais.²⁰² Um mercado diferente está sendo forjado, um mercado completamente digital.

As transações transfronteiriças, porém, não podem necessariamente estar sujeitas a uma única jurisdição. Em outras palavras, os mercados podem parecer globais, mas as leis que se aplicam a eles tendem a ser locais. Os entrevistados observaram que isso se aplicava a transações contratuais, mecanismos de resolução de disputas (acesso aos tribunais), proteção ao consumidor, pagamentos transfronteiriços (discutido mais adiante na seção IV.C.4), fluxos internacionais de dados (seção IV.C.6) e leis antitruste.

Para encontrar soluções para esses problemas, algumas regiões propuseram estratégias para harmonizar regras e normas.²⁰³ Um dos esforços mais conhecidos é o mercado único digital europeu.²⁰⁴

202 As estimativas para as posições relativas a cada tipo de transação podem ser encontradas no estudo da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD). Disponível em: <https://unctad.org/en/PublicationsLibrary/tij_unctad_ict4d06_en.pdf>. Acesso em: 09 mai 2021.

203 Há estudiosos que, em vez de harmonização, usam o conceito de “glocalização”, misturando aspectos da distribuição global e do acesso com a conformidade personalizada com as leis locais. Ver A. Chander, “Glocalization and harmonization”, *The Electronic Silk Road*, Yale Press, 2013.

204 Iniciativa da Comissão Europeia, Mercado Único Digital Europeu. Disponível em: <<https://ec.europa.eu/digital-single-market/en/policies/shaping-digital-single-market.>>

Também na América Latina e no Caribe existem iniciativas destinadas a facilitar o comércio digital com vista à estruturação de um mercado único digital regional.²⁰⁵ Esta seção irá discutir as oportunidades e desafios transfronteiriços de tais iniciativas e algumas das peculiaridades da região.

1.1. Oportunidades e desafios para um mercado digital regional único

A digitalização assumiu a forma de serviços públicos entregues on-line; de aplicativos que tornam a chamada Internet das Coisas uma realidade em casas, fábricas e fazendas; de automação de processos; e do uso em larga escala de big data e inteligência artificial para melhorar diversos tipos de atividades. A economia digital teve um impacto sobre os bens e serviços que são mais importantes para o comércio internacional. Os bens e serviços digitais passaram a fazer parte da vida e o acesso on-line a bens e serviços físicos tornou-se uma rotina diária. Assim, a importância econômica e social dos mercados digitais está sendo sentida em todos os níveis.

O pleno aproveitamento desses avanços requer acesso ao mercado, além da integração ou interoperabilidade do mercado. A promoção de um mercado digital único constitui uma estratégia importante. Está ligada à natureza sem fronteiras da Internet, não obstante as divisões geográficas e jurisdicionais, espalhando os benefícios de um mercado digital entre os participantes. Indivíduos e organizações residentes em qualquer parte da região podem oferecer serviços e bens a toda região, assim como indivíduos e organizações podem buscar os serviços e bens que desejam, independentemente de sua origem.

Essa estratégia deve incluir a integração e a harmonização das regras jurídicas. A maioria dos Estados da América Latina e do Caribe pertence a uma ou mais organizações e acordos regionais ligados ao comércio digital transnacional, como a Organização dos Estados Americanos (OEA), a Comissão Econômica para a América Latina e o Caribe (CEPAL), a Comunidade Andina, a Comunidade Caribenha (CARICOM), a Associação Latino-Americana de Integração (ALADI), a

205 Ver: <https://repositorio.cepal.org/bitstream/handle/11362/43633/1/si800569_en.pdf>

Cooperação Econômica Ásia-Pacífico (APEC), o Sistema de Integração Centro-Americana (SICA), o Mercado Comum do Sul (MERCOSUL), o Acordo de Livre Comércio Norte-Americano (NAFTA), o Projeto Mesoamérica, a Aliança do Pacífico e a Parceria Trans-Pacífico (TPP).²⁰⁶ Uma iniciativa notável é o Espaço Único de TIC CARICOM, que visa facilitar a criação de um espaço digital unificado para que mercadorias, pessoas, serviços e capital circulem.²⁰⁷

Ainda há muito a ser desenvolvido na região no que diz respeito à infraestrutura comum e à estrutura jurídica harmonizada. Não existe uma entidade central unificadora com a capacidade de vincular os países às iniciativas. Os esforços de fiscalização são igualmente deixados para que cada jurisdição os administre separadamente. Isso se reflete nas opiniões dos atores entrevistados, que indicaram que a dificuldade de estabelecer um mercado único digital na América Latina e no Caribe reside no fato de que nenhum dos esforços de integração propostos foi implementado com sucesso. Assim, as diferenças jurisdicionais impactam o acesso ao mercado e as oportunidades de crescimento na região. Um especialista mencionou que as disparidades jurídicas e econômicas e a falta de padrões regulatórios mínimos em comum eram as maiores barreiras.

Existem, no entanto, algumas tendências comuns entre os países da região. O comércio eletrônico está em constante expansão. Além disso, o ambiente de *start-ups* está crescendo exponencialmente em áreas como logística, transporte, pagamentos digitais e tecnologia agrícola (*agritech*).²⁰⁸ O caminho a seguir continua longo, no entanto, especialmente no que diz respeito aos acordos intrarregionais.²⁰⁹

206 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market", 2018. Disponível em: <<https://ec.europa.eu/digital-single-market/en/shaping-digital-single-market?etrans=pt>>. Acesso em: 09 mai 2021.

207 Ver: <https://www.internetsociety.org/wp-content/uploads/2017/08/ISOC_Unleashing_Internet_in_Caribbean_20170221.pdf>. Acesso em: 09 mai 2021.

208 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market", 2018. Disponível em: <https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf>. Acesso em: 09 mai 2021.

209 Os dados do Banco Mundial indicam que há muito a melhorar no mercado digital da América Latina e do Caribe. Ver: <www.doingbusiness.org>. Acesso em: 09 mai 2021.

Vários dos participantes pesquisados mencionaram a digitalização da economia como uma oportunidade, mas ressaltaram a necessidade de harmonização regulatória. A harmonização foi considerada particularmente crucial em áreas como a proteção do consumidor, a proteção de dados pessoais, a identidade digital, os meios de pagamento digitais, os valores mobiliários digitais, os padrões de transporte e logística e os regimes fiscais.

Essa percepção parece estar em sintonia com as recomendações das organizações internacionais.²¹⁰ Poucas iniciativas legislativas ou regulatórias na região levaram em consideração os desafios transfronteiriços da criação de um mercado digital mais integrado.²¹¹ Elas tendem a ser concebidas de um ponto de vista doméstico, resultando em uma situação muito fragmentada com uma multiplicidade de padrões.

1.2. A região tem uma forte cultura de direitos do consumidor, mas com diferentes padrões locais

Praticamente todos os países da região têm legislação de proteção ao consumidor em vigor, na maioria dos casos sob a forma de leis específicas.²¹² Alguns países têm leis específicas sobre transações de consumo on-line, mas na maioria dos países o regime de proteção ao consumidor é voltado principalmente para as relações off-line. Essa situação cria uma oportunidade para desenvolver um mercado único digital para plataformas de Internet e comércio eletrônico em geral.

210 Ver, por exemplo, o estudo da Organização para a Cooperação e Desenvolvimento Econômico (OCDE). Disponível em: <<https://www.oecd-ilibrary.org/docserver/9789264251823-16-en.pdf?expires=1588103565&id=id&acname=guest&Checksum=233F2db69A0b854F11bc076348793b73>>. Acesso em: 09 mai 2021.

211 Corporação Andina de Fomento (CAF), "Building a Digital Single Market Strategy for Latin America". Disponível em: <<https://scioteca.caf.com/handle/123456789/980?show=full>>. Acesso em: 09 mai 2021.

212 Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market", 2018. Disponível em: https://repositorio.cepal.org/bitstream/handle/11362/43633/1/S1800569_en.pdf>. Acesso em: 09 mai 2021. Ver também "World Consumer Protection Map". Disponível em: <<https://unctadwcpm.org>>. Acesso em: 09 mai 2021. Para uma visão geral de vários regimes nacionais e como eles se comportam em comparação com outros países do mundo, ver: Hans-W. Micklitz e Geneviève Saumier (eds.), *Enforcement and Effectiveness of Consumer Law*, Springer, 2018.

A internacionalização do mercado traz desafios jurisdicionais para as empresas que operam além das fronteiras. Essas empresas, nas áreas de comércio eletrônico, mercados ou mídias sociais, devem estar preparadas para cumprir as leis de defesa do consumidor em todas as jurisdições onde realizam negócios. As leis nacionais de proteção do consumidor são aplicáveis onde quer que a sede física de uma empresa de Internet possa estar. O simples fato de oferecer bens e serviços aos consumidores locais desencadeia proteções nacionais.²¹³

A presença de uma cultura comum de defesa do consumidor na América Latina e no Caribe coexistiu até agora com a falta de um quadro harmonizado adequado ou de um mercado único digital, expondo as empresas a uma variedade de diferentes normas nacionais de proteção. Além disso, os consumidores podem procurar resolver suas disputas em seu próprio país, com o resultado de que as empresas são obrigadas a comparecer aos tribunais de várias jurisdições ou a participar de diferentes procedimentos de resolução de disputas fora do país onde estão estabelecidas.

Em outra camada de complexidade, muitas das leis em questão são entendidas como normas imperativas (*lois de police*), o que significa que na maioria dos casos as estipulações contratuais não devem contradizê-las. Em outras palavras, tais leis são aplicáveis independentemente dos termos e condições e das estipulações contratuais presentes nas transações via Internet.²¹⁴

Durante as negociações da Conferência Interamericana de Direito Internacional Privado (CIDIP VII) sobre a proteção internacional dos consumidores, vários países argumentaram que as transações internacionais de consumo deveriam estar sujeitas a um “princípio de proteção mais favorável”. A lei aplicável ao contrato seria a mais favorável ao consumidor, seja a

213 Corporación Andina de Fomento (CAF), "Building a Digital Single Market Strategy for Latin America". Disponível em: <<https://scioteca.caf.com/handle/123456789/980?show=full>>. Acesso em: 09 mai 2021.

214 C. Marques, "A proteção da parte mais fraca em direito internacional privado e os graus da CIDIP VII de proteção dos consumidores", Curso de Direito Internacional da OEA. Disponível em: <http://www.oas.org/es/sla/ddi/docs/publicaciones_digital_XXXIV_curso_derecho_internacional_2007_Claudia_Lima_Marques.pdf>. Acesso em: 09 mai 2021.

lei aplicável no local de jurisdição, da residência habitual do consumidor ou do contrato.²¹⁵

A falta de normas comuns de proteção do consumidor impacta a forma como os provedores de Internet podem interagir com os consumidores na região. Diferentes leis de proteção ao consumidor podem significar uma variedade de padrões para publicidade, práticas de faturamento desleais, rescisão de contrato e mudança de empresa (portabilidade e interoperabilidade também).²¹⁶ Essa situação pode atuar como uma barreira ao comércio.²¹⁷

O outro lado da equação é que, em contraste com o mercado digital na Europa, por exemplo, as leis de defesa do consumidor na América Latina e no Caribe tendem a ser aplicadas apenas dentro dos limites de cada jurisdição nacional. Assim, é uma prática comum que as empresas utilizem tecnologias de geolocalização para restringir o acesso a bens e serviços em determinados locais.²¹⁸

No MERCOSUL, houve iniciativas para harmonizar as normas de defesa do consumidor. Recentemente, os membros propuseram estruturar e utilizar uma plataforma digital para a resolução de disputas de consumo.²¹⁹ Isso poderia ajudar a promover serviços de Internet e o comércio eletrônico transfronteiriços na região, reduzindo os custos de disputas e litígios de consumo.

215 As negociações não foram concluídas, mas o conceito permaneceu significativo nos fóruns internacionais e forneceu uma referência para a discussão intrarregional. Disponível em: <<http://aebm.mo/en/2018Vol1Issue1/8>>. Acesso em: 09 mai 2021.

216 Ver: <<https://www.oecd-ilibrary.org/docserver/9789264251823-16-en.pdf?expires=1588103565&id=id&accname=Guest&checksum=233f2db69a0b854f11bc076348793b73>>. Acesso em: 09 mai 2021.

217 M. Durovic, "Direito internacional do consumidor: o que se trata?", *Journal of Consumer Policy*, vol. 43, 2020. Disponível em: <<https://doi.org/10.1007/s10603-019-09438-9>>. Acesso em: 09 mai 2021.

218 Corporação Andina de Fomento (CAF), "Building a Digital Single Market Strategy for Latin America". Disponível em: <<https://scioteca.caf.com/handle/123456789/980?show=full>>. Acesso em: 09 mai 2021.

219 Ver: <<https://www.cancilleria.gob.ar/es/actualidad/noticias/comunicado-conjunto-de-los-presidentes-de-los-estados-partes-del-mercosur>>. Acesso em: 09 mai 2021.

1.3. Cláusulas de escolha da lei aplicável e de foro tendem a ser mal-vistas no comércio eletrônico devido à proteção do consumidor a nível nacional.

A falta de regras harmonizadas e de um mercado digital único, com a natureza livre da Internet, torna a determinação da jurisdição sobre as transações transfronteiriças particularmente desafiadora. Para proporcionar mais previsibilidade, a maioria das empresas de Internet opta por incluir em seus contratos cláusulas de escolha de foro, ou um método de resolução de litígios (arbitragem, mediação ou conciliação), bem como cláusulas de escolha da lei aplicável. Essas estipulações limitam sua exposição e reduzem o potencial emaranhado jurisdicional.

Os regimes legais no mundo todo geralmente permitem tais escolhas sob o que é chamado de autonomia das partes. Os países da América Latina e do Caribe lutaram com o conceito durante a maior parte do século XX,²²⁰ culminando na aprovação da Convenção Interamericana sobre Direito Aplicável aos Contratos Internacionais de 1994, embora, em parte porque consagra o princípio da autonomia das partes, esta não foi amplamente aceita, tendo sido ratificada apenas pela República Bolivariana da Venezuela e pelo México.²²¹ Nas últimas duas décadas, entretanto, o princípio ganhou força, e muitos países adotaram uma postura mais flexível, aceitando a autonomia das partes para certas categorias de contratos.²²²

Além disso, vários Estados são partes da Convenção das Nações Unidas sobre Contratos para a Venda Internacional de Mercadorias (CISG) de 1980. As vendas transfronteiriças de mercadorias pela Internet podem, assim, ser cobertas por suas

220 Ver: <http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf>. Acesso em: 09 mai 2021.

221 Ver: <<https://www.oas.org/juridico/english/signs/b-56.html>>. Acesso em: 09 mai 2021.

222 Na região, apenas o Uruguai rejeita explicitamente a autonomia das partes, embora tenha havido alguma aceitação na doutrina e na jurisprudência. No Brasil, ainda há discussão sobre se é totalmente aplicável, e a jurisprudência não é consistente. Para uma visão geral, consulte o Comitê Jurídico Interamericano, "Guide on the Law Applicable to International Commercial Contracts", fevereiro de 2019. Disponível em: <https://www.oas.org/en/sla/iajc/docs/Guide_Law_Applicable_to_International_Commercial_Contracts_in_the_Americas.pdf>. Acesso em: 09 mai 2021.

disposições, que preveem a autonomia das partes. No entanto, a convenção não substitui necessariamente outras considerações, nomeadamente a defesa do consumidor.²²³

A questão do local do foro e da legislação aplicável tornou-se, assim, uma dentre três partes: (i) se um país permite a escolha da lei aplicável e a escolha do foro; (ii) se a autonomia das partes é aceita para escolhas de meios não-judiciais para resolver disputas (por exemplo, arbitragem e mediação) e sob quais condições; e (iii) se certas categorias de transações, tais como transações de consumidores, recebem um nível diferente de proteção.

A forte cultura de proteção ao consumidor da região deixou sua marca na forma como os contratos são interpretados na região. Muitos países da América Latina e do Caribe consideram que os contratos nos quais há um desequilíbrio inerente entre as partes, com a parte mais forte impondo obrigações contratuais, devem ser sujeitos a um escrutínio mais rigoroso.²²⁴ A consequência é que as cláusulas de lei aplicável e de escolha de foro tendem a ser mal vistas quando podem ser desvantajosas para a parte mais fraca.²²⁵ Em algumas circunstâncias, elas são percebidas como abusivas, particularmente se limitarem as opções de solução de controvérsias ou o acesso ao judiciário.

223 Para uma lista de países interessados, ver: <https://uncitral.un.org/en/texts/salegoods/conventions/sale_of_goods/cisg>. Acesso em: 09 mai 2021.

224 Ver: <http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf>. Acesso em: 09 mai 2021.

225 A International Law Association reconheceu que os consumidores tendem a ser as partes mais fracas nos contratos transfronteiriços. Ver: International Law Association (ILA), "Resolution No.I/2016. Committee on the International Protection of Consumers". Disponível em: <https://www.ila-hq.org/images/ILA/docs/No.1_Resolution_2016_ProtectionOfConsumers_4Models.pdf>. Acesso em: 09 mai 2021. Um exemplo claro é o artigo 2651 do Código Civil Argentino, que permite a autonomia das partes para todos os contratos, exceto aqueles que envolvem consumidores. Outros são os artigos 89 e seguintes do Código de Direito Internacional Privado do Panamá, que estabelecem um regime especial para contratos em que as partes não estão em pé de igualdade ("contratos desiguais ou de adesão").

Esse é particularmente o caso de transações envolvendo um consumidor.²²⁶

A maioria das transações na Internet (comércio eletrônico e serviços de Internet, por exemplo) são regidos pelos chamados “contratos *click-wrap*” ou “contratos do tipo *browse-wrap*”, cujas cláusulas substantivas são encontradas nos termos e condições disponíveis on-line. Esses contratos deixam pouco espaço para negociação. Normalmente, a parte mais fraca (um consumidor) não tem outra opção senão aceitar todas as cláusulas como estão ou renunciam ao acesso a esse serviço ou bem. Tais contratos são considerados contratos de adesão e tendem a ser interpretados a favor da parte mais fraca. Não somente as leis de proteção ao consumidor podem ser aplicadas, mas as cláusulas de escolha do foro e de lei aplicável podem ser consideradas ineficazes ou inválidas, especialmente se os consumidores as contestarem nos tribunais.²²⁷

Da mesma forma, uma cláusula de mecanismo de resolução de litígios pode sofrer o mesmo destino. Se a cláusula impedir um consumidor de ter acesso ao Judiciário, isto pode ser interpretado como abusivo e os tribunais podem não aplicá-las. Empresas de Internet que querem limitar sua exposição a diferentes tribunais e leis podem acabar recorrendo a técnicas de geolocalização, a fim de limitar seu alcance geográfico (ver seção V.B.1 abaixo para mais informações sobre estas técnicas).

226 Houve esforços intrarregionais para elaborar convenções internacionais para lidar com questões jurisdicionais internacionais transfronteiriças envolvendo consumidores, das quais o CIDIP VII. Os esforços não se concretizaram, entre outras razões, porque não houve acordo sobre o papel da autonomia das partes ou sobre a opção de escolher a arbitragem como meio de resolução de disputas. Para uma visão geral deste esforço, ver: D. Fernández Arroyo e J. A. Moreno Rodríguez, *Protección de los consumidores en América: trabajos de la CIDIP VII (OEA), Asuncion, La Ley-CEDEP, 2007*. Ver também: <http://www.oas.org/es/sla/ddi/docs/publicaciones_digital_XXXIV_curso_derecho_internacional_2007_Claudia_Lima_Marques.pdf>. Acesso em: 09 mai 2021.; e <<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>>. Acesso em: 09 mai 2021.

227 Ver: <http://www.oas.org/es/sla/ddi/docs/publicaciones_Contratos_Internacionales_OEA-ASADIP_2016_Publicacion_Completa.pdf>. Acesso em: 09 mai 2021.

1.4. Os governos da região estão impondo regras mais rígidas para moderação e remoção de conteúdo em plataformas on-line

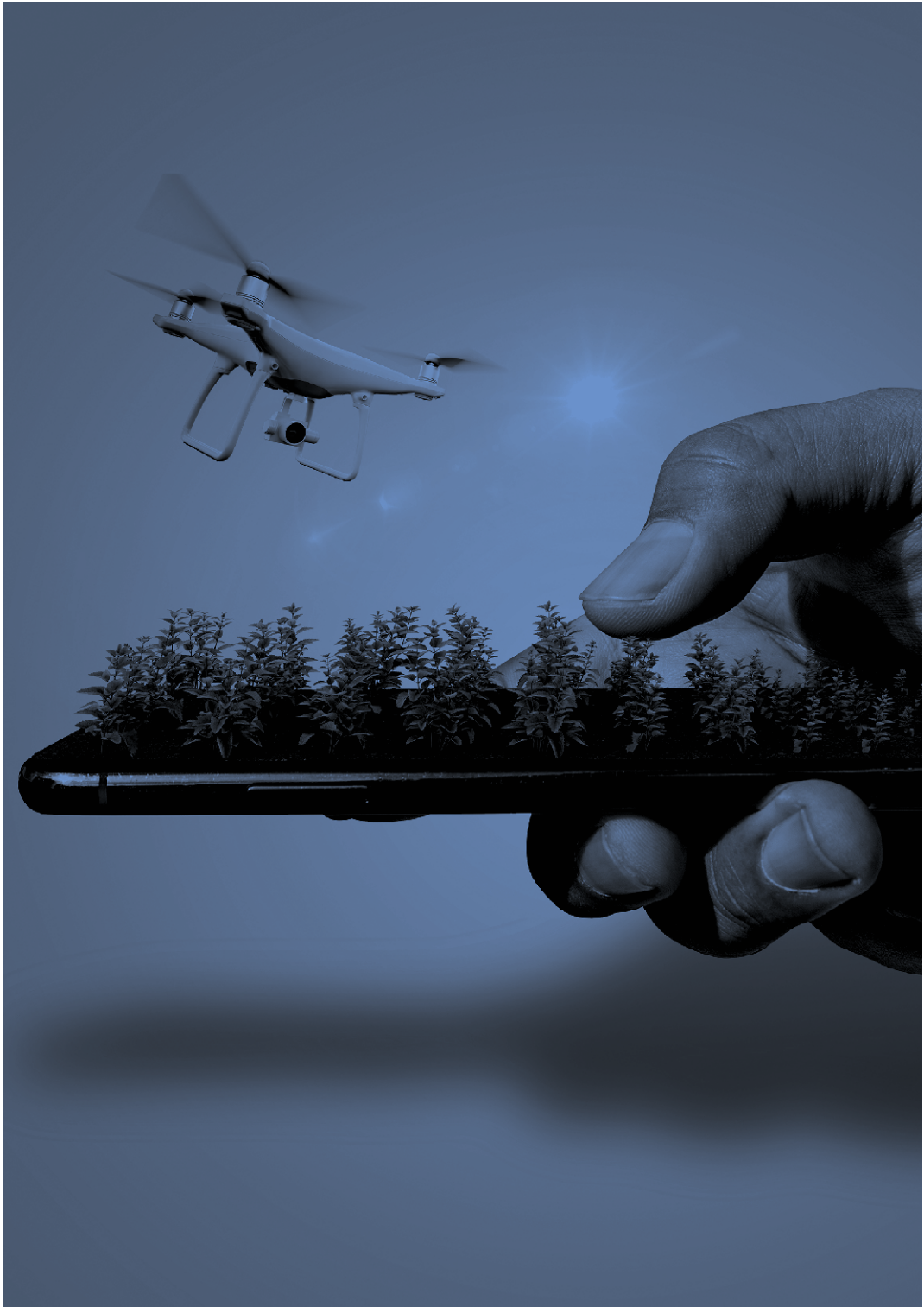
O *Relatório de Status Global 2019* da Rede de Políticas Internet & Jurisdição identificou uma tendência global de que os Estados venham a assumir uma atitude mais dura em relação às plataformas da Internet. Países da América Latina e do Caribe fazem parte dessa tendência.

As peculiaridades das empresas de Internet e os serviços que prestam inicialmente levaram à adoção generalizada de regras e garantias que as protegeriam de grandes litígios sobre conteúdos criados por terceiros, principalmente seus próprios usuários. Essa tendência surgiu na segunda metade dos anos 90, quando a seção 230 da Lei de Decência das Comunicações (Communications Decency Act-CDA) e a Lei de Direitos Autorais Digitais do Milênio (DMCA) criaram algo como um refúgio seguro para os provedores de Internet nos Estados Unidos. A UE seguiu o exemplo com a Diretiva de Comércio Eletrônico (2000/31/CE).

Muita coisa mudou desde o final dos anos 90, uma vez que as plataformas de comércio eletrônico se tornaram onipresentes e as empresas de mídia social podem ter a maioria da população de um país como seus usuários, sem ter nenhum escritório nesse país. Ao mesmo tempo, a velocidade surpreendente com que o conteúdo é produzido on-line continua a reforçar a necessidade de se conceber um regime especial de moderação de conteúdo e responsabilidade. É inquestionavelmente desafiador lidar com números como os 6.000 *tweets* enviados por segundo e as 400 horas de vídeo do YouTube carregadas a cada minuto.

Alguns países da região consagraram proteções para intermediários da Internet em sua legislação, criando uma exceção específica para a aplicação de regras gerais de responsabilidade ou regimes gerais de proteção ao consumidor para produtos ou serviços com mau funcionamento.²²⁸

228 Somente o Brasil e o Chile possuem disposições de "porto seguro", que limitam a responsabilidade dos intermediários da Internet pela hospedagem ou transferência de conteúdo de terceiros, promulgadas como parte de sua legislação. Ver: Inter-American Development Bank (IDB), "Accelerating Digital Trade in Latin America and the Caribbean". Disponível em: <<https://publications.iadb.org/publications/english/document/Accelerating-Digital-Trade-in-Latin-America-and-the-Caribbean.pdf>>. Acesso em: 09 mai 2021.



Embora a situação esteja mudando rapidamente e muitas empresas locais de Internet estejam surgindo, os países da América Latina e do Caribe ainda são servidos principalmente por empresas e plataformas de Internet estabelecidas fora da região. Assim, toda interação tende a ser transnacional, levantando potencialmente questões jurisdicionais.

A abordagem em relação às plataformas da Internet mudou em pelo menos duas áreas: conteúdo de terceiros (moderação de conteúdo) e proteção da propriedade intelectual (pirataria e contrafação). Como mencionado em outras seções, áreas como a execução da lei (seção IV.B.2), *cyberbullying* (seção IV.A.3) e exposição não autorizada de imagens íntimas (seção IV.A.4) também pressionaram os intermediários da Internet para assumir um papel mais ativo e cooperar com as agências de execução da lei.

No Brasil, o Supremo Tribunal Federal foi chamado a decidir sobre se a cláusula de "porto seguro" (artigo que limita a responsabilidade dos intermediários da Internet pela hospedagem ou transferência de conteúdo de terceiros) presente no Marco Civil da Internet é consistente com a Constituição Federal.

Um projeto de lei para regular a responsabilidade de intermediários não recebeu o apoio necessário na Argentina.²²⁹ Da mesma forma, o México tem lutado para encontrar apoio para o estabelecimento de um regime de responsabilidade consistente com o Acordo entre os Estados Unidos da América, os Estados Unidos Mexicanos e o Canadá (USMCA), que prevê a criação de um porto seguro para o comércio digital transfronteiriço entre suas partes.²³⁰

No Equador, foi proposto um projeto de lei para regulamentar o conteúdo on-line, incluindo disposições que tornariam os intermediários da Internet diretamente responsáveis por retirar o conteúdo considerado ilegal.²³¹ Um projeto semelhante foi proposto em Honduras, fornecendo definições muito amplas dos tipos de conteúdo ilegal que os intermediários da Internet deveriam monitorar.²³²

229 Ver: <<https://www.lanacion.com.ar/tecnologia/los-intermediarios-internet-debate-seguira-pendiente-nid2192063>>. Acesso em: 09 mai 2021.

230 Ver: <<https://www.derechosdigitales.org/l2564/usmca-y-el-futuro-de-internet/>>. Acesso em: 09 mai 2021.

231 Ver: <<https://www.eluniverso.com/opinion/2017/06/13/nota/6229435/redes-sociales-censura/>>. Acesso em: 09 mai 2021.

232 Ver: <<https://www.accessnow.org/comunicado-ley-que-regula-los-actos-de-odio-y-discriminacion-en-internet-de-hons/>>. Acesso em: 09 mai 2021. Ver também: <<https://www.hrw.org/news/2018/04/09/honduras-cybersecurity-bill-threatens-free-speech>>. Acesso em: 09 mai 2021.

Na mesma linha, uma lei aprovada na República Bolivariana da Venezuela enfatizou a responsabilidade dos intermediários e previu sanções se eles não removeassem conteúdo ilegal. As entidades estatais também podem solicitar diretamente que o conteúdo seja retirado.²³³ Um projeto de lei no Paraguai tentou impor aos PSIs a obrigação de remover discursos considerados "ofensivos".²³⁴

As organizações da sociedade civil têm manifestado preocupação com iniciativas para aumentar a responsabilidade civil dos intermediários.²³⁵ O Relator Especial para a Liberdade de Expressão ecoou dúvidas sobre os potenciais riscos em matéria de direitos humanos destas iniciativas legislativas.²³⁶

Muito do foco tem sido as plataformas de mídia social, mas os sites e mercados de comércio eletrônico (*marketplaces*) não têm sido ignorados. Os governos da região reforçaram as medidas contra a pirataria e os produtos contrafeitos, ambos restringindo o conteúdo considerado ilegal e fortalecendo as proteções para os direitos de propriedade intelectual.

A reforma dos direitos de propriedade intelectual, inclusive os direitos autorais, também pode proporcionar uma oportunidade para que os países harmonizem seus pontos de vista e desenvolvam abordagens regionais, facilitando a circulação de bens e serviços protegidos por direitos autorais e de outras classes de propriedade intelectual.

2. PROPRIEDADE INTELECTUAL

Várias interseções entre a Internet e os direitos de propriedade intelectual já foram destacadas no *Relatório de Status Global*

233 Ver: <<http://espaciopublico.org/ley-odio-venezuela-amenaza-la-libre-expresion-america-latina/>>. Acesso em: 09 mai 2021.

234 TEDIC, "Un proyecto de censura política", 11 outubro de 2017. Disponível em: <<https://www.tedic.org/un-proyecto-de-censura-politica/>>. Acesso em: 09 mai 2021.

235 Ver: <<https://www.derechosdigitales.org/internetesnuestra/desafios-gobernanza.pdf>>. Acesso em: 09 mai 2021.

236 Organization for Security and Cooperation in Europe (OSCE), "Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda". Disponível em: <<https://www.osce.org/fom/302796>>. Acesso em: 09 mai 2021. A Comissão Interamericana de Direitos Humanos também divulgou sua preocupação com uma iniciativa semelhante no contexto eleitoral. Ver: <https://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf>. Acesso em: 09 mai 2021.

2019 da Rede de Políticas Internet & Jurisdição. Os direitos de propriedade intelectual sobre patentes, marcas e design no ambiente digital não precisam estar restritos a nenhum território em particular. Sua concretização em forma física pode parecer uma limitação, como, por exemplo, quando um vídeo no passado tinha que estar no formato de um filme, fita ou vídeo disco digital (DVD) para poder circular. Mas quanto mais a “carne” se torna “palavra”, parafraseando Barlow, menos as barreiras físicas que dificultam a circulação da propriedade intelectual atuam como uma restrição.²³⁷ O material protegido por direitos autorais pode ser baixado ou transmitido ao vivo sem levar em conta as fronteiras.

A regulação da propriedade intelectual, entretanto, ainda é, em muitos aspectos, um assunto doméstico, particularmente quanto às suas exceções. Assim, as diferenças regulatórias, que vão desde interpretações de tratados internacionais até mecanismos reais de execução, tendem a conduzir a dificuldades transfronteiriças. Isso é particularmente desafiador quando indivíduos e empresas utilizam a natureza sem fronteiras da Internet para contornar a legislação ou mesmo decisões judiciais destinadas a efetivamente proteger a propriedade intelectual.

2.1. Proteção da propriedade intelectual: impactos na economia e nos direitos humanos

Os mecanismos de proteção dos direitos autorais variam de Estado para Estado. A forma como estão estruturados é um aspecto importante de um equilíbrio muito intrincado entre o incentivo aos autores, a proteção dos interesses econômicos da indústria e a salvaguarda do direito e do interesse da sociedade em acessar os frutos da criação. Em outras palavras, os direitos autorais são uma instituição-chave que tanto fomenta, quanto salvaguarda a cultura. No entanto, a aplicação dos direitos autorais de maneira muito rigorosa pode acabar por restringir o acesso ao conhecimento e ao avanço da cultura.

Em um ambiente onde os “memes” são uma grande tendência social, novas obras são muitas vezes produzidas com base em material anterior, geralmente protegido por direitos autorais. A restrição de acesso e uso de conteúdo protegido por direitos

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

autorais limita o acesso tanto ao conhecimento (ideias e material) quanto à inovação.²³⁸

Na América Latina e no Caribe, é primordial que o equilíbrio entre a proteção dos direitos autorais e a salvaguarda do acesso seja bem refletido nas regulações. Os entrevistados observaram a relação entre direitos autorais e progresso, mas enfatizaram que em muitas circunstâncias os direitos autorais poderiam ser usados para restringir o acesso das sociedades à informação. Os direitos autorais têm sido usados até mesmo como uma ferramenta para restringir a liberdade de expressão. Esse tem sido o caso com material crítico ao Presidente Correa durante as eleições equatorianas.²³⁹

Outro aspecto a ser levado em consideração é que em muitas circunstâncias informações imprecisas (inclusive desinformação) estão disponíveis gratuitamente e circulam sem barreiras, mas o conhecimento real e as informações necessárias são restritas, “protegidas” por *paywalls* e bancos de dados de difícil acesso.²⁴⁰

Neste contexto, tem-se debatido como equilibrar melhor a proteção da propriedade intelectual, em especial os direitos autorais, e os direitos à educação, acesso à informação, autodesenvolvimento e outros direitos humanos. A questão, em alguns casos, tem sido se a melhor maneira de alcançar os objetivos da política de direitos autorais é através de fortes procedimentos de execução da lei contra a pirataria e, em algumas circunstâncias, a reprodução não autorizada.

238 A. Chander and M. Sunder, "Dancing on the grave of copyright?", *Duke Law & Technology Review*, vol. 18, 2019. Disponível em: <<https://ssrn.com/abstract=3436972>>. Acesso em: 09 mai 2021.

239 Ver: <<https://www.hrw.org/world-report/2018>>. Acesso em: 09 mai 2021. Foi noticiado que isso aconteceu também outras circunstâncias. Ver: A. Ellerbeck, "How U.S. copyright law is being used to take down Correa's critics in Ecuador", *Committee to Protect Journalists*, 21 de janeiro de 2016. Disponível em: <<http://bit.ly/1Lu5Uoj>>. Acesso em: 09 mai 2021.

240 A. J. Robinson, "The truth is paywalled but the lies are free", *Current Affairs*, Ago 2020. Disponível em: <<https://www.currentaffairs.org/2020/08/the-truth-is-paywalled-but-the-lies-are-free>>. Acesso em: 09 mai 2021.

Um exemplo importante é a proteção do conhecimento tradicional. A proteção adequada dos conhecimentos, tradições, procedimentos e manifestações culturais dos grupos tradicionais e populações indígenas da região é primordial para a proteção de seu modo de vida; e, por extensão, de seus direitos humanos. Muitos países da região têm se tornado mais sensíveis à necessidade de fornecer regras melhores e mais específicas, que reconheçam o conhecimento tradicional. A República Bolivariana da Venezuela, o Brasil, a Costa Rica e o Peru são exemplos claros desta tendência. Houve casos de países que apresentaram reclamações a corporações internacionais por sua exploração de conhecimentos tradicionais, com relações sendo transferidas em alguns casos para intermediários da Internet, que vendem produtos com a devida proteção.²⁴¹

2.2. Os efeitos transfronteiriços da filtragem utilizada para fazer valer os direitos de propriedade intelectual

A dinâmica de proteção dos direitos autorais on-line tem diferentes facetas. O setor privado, e os intermediários da Internet em particular, ultimamente têm sido chamados a desempenhar um papel mais significativo. Voluntariamente ou através de acordos com o setor público, várias empresas, principalmente de mercados on-line (*marketplaces*) e redes sociais, desenvolveram mecanismos de proteção de direitos autorais.

A Amazon, por exemplo, expandiu seu “Projeto Zero” anti-contrafação para 17 países no total, incluindo Brasil e México na região da América Latina e Caribe, como parte de sua iniciativa de propriedade intelectual e proteção da marca.²⁴² A plataforma de comércio eletrônico Mercado Livre, com operações em 18 países da América Latina, também conta com um programa de proteção de direitos autorais que opera de forma semelhante. Esses programas incluem ferramentas para os detentores de direitos e preveem sanções para possíveis violações, que podem

241 Ver: <<https://yourlatamflagship.com/2020/01/16/how-latin-america-countries-protect-their-traditional-knowledge-through-ip/>>. Acesso em: 09 mai 2021. Para saber mais sobre esta tendência a partir de uma perspectiva latino-americana, ver: L. Lixinski, *International Heritage Law for Communities: Exclusion and Re-Imagination*, Oxford University Press (OUP), 2019.

242 Comunicado à Imprensa, “Amazon Project Zero launches in seven new countries”, 20 de agosto de 2020. Disponível em: <<https://press.aboutamazon.com/news-releases/news-release-details/amazon-project-zero-launches-seven-new-countries/>>. Acesso em: 09 mai 2021.

chegar à suspensão ou cancelamento de contas para infratores reincidentes.²⁴³

Esses mecanismos voluntários não são necessariamente suficientes e certas jurisdições solicitaram uma revisão das leis em vigor sobre o assunto. Recentemente, a UE emitiu a Diretiva 2019/790, que causou grande controvérsia tanto na Europa quanto na região.²⁴⁴ A diretiva visa aumentar a responsabilidade dos intermediários da Internet pelos conteúdos de terceiros nos seus ambientes on-line (ver seção III.F para mais informações sobre o novo papel dos intermediários da Internet).

Tais regulações impactaram a região de duas maneiras. Em primeiro lugar, elas estimularam os países a rever a sua própria legislação de direitos autorais, a fim de incluir obrigações semelhantes. Em segundo lugar, como efeito transfronteiriço direto, os materiais que pertencem a vários artistas ou detentores de direitos de autor podem ser retirados por essas plataformas, o que terá de ser contestado em outros países (ver seção V.A.5 para saber mais sobre os mecanismos on-line para contestar tais decisões).²⁴⁵

As organizações da sociedade civil expressaram a preocupação de que a nova diretiva de direitos autorais da UE possa se tornar um modelo para a reforma dos direitos autorais na região, ter um efeito inibidor no conteúdo e dificultar o comércio on-line. Segundo elas, os requisitos desta legislação podem levar à filtragem automática e proporcionar muito pouco espaço e tempo para análise contextual.²⁴⁶

243 Mercado Libre, "Brand Protection Program: qué es y cómo usarlo". Disponível em: <<https://vendedores.mercadolibre.com.ar/blog/notas/brand-protection-program-que-es-y-como-usarlo/>>. Acesso em: 09 mai 2021.

244 Ver: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790>>. Acesso em: 09 mai 2021.

245 Ver: <<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/>>. Acesso em: 09 mai 2021.

246 Ver: <<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/>>. Acesso em: 09 mai 2021.

No Brasil, o Projeto de Lei sobre as *Fake News* (ver seção IV.A.1) incentivou as associações do setor de rádio e televisão a propor compensações para os editores de material de imprensa como forma de compensação de direitos autorais quando esse material fosse utilizado pelos PSIs. Na opinião deles, essa medida seria eficaz para impulsionar o jornalismo profissional, potencialmente ajudando a combater a desinformação e as notícias falsas.²⁴⁷ Um mecanismo semelhante (o "imposto sobre links") previsto pelo artigo 15 da Diretiva sobre Direito Autoral da UE²⁴⁸ tem sido amplamente criticado por poder prejudicar o acesso à informação e pelas desvantagens que poderia trazer aos serviços menores e não-comerciais.²⁴⁹

Os filtros, que são ferramentas automatizadas para detectar e derrubar conteúdo protegido por direitos autorais, agravam ainda mais esse fenômeno. As técnicas que eles usam geralmente geram falsos positivos, sinalizando e restringindo conteúdo legal ou que se encaixa em uma das exceções às restrições de direitos autorais (paródia, uso justo, uso educacional, etc.). Assim, as empresas devem adaptar seus filtros a diferentes leis e contextos locais ou terão que optar por um filtro geral que possa criar mais restrições do que o necessário.

A América Latina e o Caribe provavelmente serão afetados por esses filtros e controles de direitos autorais. A circulação de materiais protegidos por direitos autorais pode sofrer [impactos]. Os setores cultural e do entretenimento são exemplos claros. Os países se beneficiam da polinização cultural cruzada

247 O Globo, "Entidades pedem transparência e valorização do jornalismo profissional no projeto contra fake news", 18 de agosto de 2020. Disponível em: <<https://oglobo.globo.com/brasil/entidades-pedem-transparencia-valorizacao-do-jornalismo-profissional-no-projeto-contrafake-news-24593224>>. Acesso em: 09 mai 2021.

248 União Europeia, "Diretiva (UE) 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativa aos direitos de autor e direitos conexos no Mercado Único Digital e que altera as Diretivas 96/9/CE e 2001/29/CE". Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32019L0790>>. Acesso em: 09 mai 2021.

249 Cory Doctorow, "The European Copyright Directive: what is it, and why has it drawn more controversy than any other directive in EU history?", Electronic Frontier Foundation, 19 de março de 2019. Disponível em: <<https://www.eff.org/pt-br/deeplinks/2019/03/european-copyright-directive-what-it-and-why-has-it-drawn-more-controversy-any>>. Acesso em: 09 mai 2021.

entre os artistas da região. O compartilhamento on-line tende a significar mercados e públicos muito maiores para artistas locais. Os filtros podem proteger os direitos autorais, mas também podem limitar a exposição e dificultar o recurso contra decisões tomadas pelas plataformas (veja a seção V.A.5 sobre recursos).

3. A INTERNET DAS COISAS (IOT)

Um duplo fenômeno vem ocorrendo em todo o mundo: a digitalização do espaço físico e uma fusão do mundo físico com o digital. Essa superposição do físico e do digital está reduzindo os custos de produção, transação e distribuição. Também está criando novas oportunidades. O conceito da Internet das Coisas (IoT, na sigla em inglês) abrange uma parte significativa disso. A conexão de dispositivos que tradicionalmente não estavam conectados, de geladeiras a tratores e de sistemas de abastecimento de água a redes de energia, torna mais dados e funções disponíveis. Assim, bens e serviços mais especializados podem ser fornecidos, decisões baseadas em fatos (baseadas em dados) podem ser racionalizadas e experiências gerais, inclusive a pontualidade, podem ser melhoradas.

A IoT vai além de fornecer uma conexão à Internet: ela cria ecossistemas de base tecnológica cujo valor é gerado pela captura, registro e análise de dados. O valor dessas funções é aumentado ao combiná-las com computação em nuvem, *blockchain*, robótica e inteligência artificial.²⁵⁰ Assim, um fabricante de equipamentos agrícolas pode ter acesso, por exemplo, a dados sobre o clima, os hábitos de condução e o rendimento das colheitas. Um desenvolvedor de relógios inteligentes (*smartwatches*) pode usar os recursos de monitoramento do produto para fornecer uma gama de bens e serviços que podem ajudar as pessoas a administrar melhor seus exercícios e seus hábitos alimentares e consumo de bebida: em uma palavra, sua saúde. Uma cidade pode tomar decisões melhores sobre como os recursos de seu sistema de transporte são alocados.

Os modelos de negócios centrados na IoT não precisam respeitar as estruturas econômicas verticais nem ser limitados pelas fronteiras nacionais. Eles se beneficiam da natureza sem

250 Economic Commission for Latin America and the Caribbean (ECLAC), Data, algorithms and policies: redefining the digital world (LC/CMSI.6/4), Santiago, 2018.

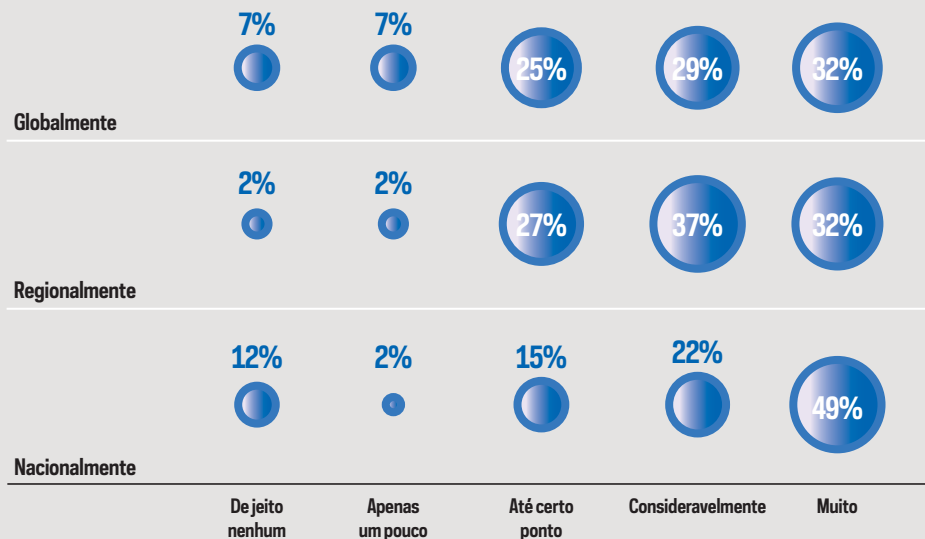
fronteiras da Internet à qual estão conectados e, em certa medida, da desmaterialização que vem com a digitalização. Isso significa uma “sociedade de sensores”, onde tudo que pode ser ligado à Internet será e quaisquer dados que possam ser compartilhados também o serão. O comércio internacional e os fluxos de dados transfronteiriços são uma consequência provável da implementação da IoT. Para tirar o máximo proveito disso, há necessidade de escala, convergência, harmonização e um ambiente interoperável com um mercado interconectado.

Os entrevistados apontaram que os principais desafios estão relacionados ao estabelecimento de protocolos, padrões comuns, modelos industriais e a harmonização de regras e regulações. Suas preocupações com a região coincidiram principalmente com aquelas registradas no *Relatório de Status Global 2019*: segurança e privacidade; normas técnicas comuns; segurança do produto; disponibilidade de largura de banda e conectividade; regras sobre responsabilidade; e interoperabilidade regional.

Um dos atores observou que a plena harmonização das regulações e normas dentro da região pode ser um objetivo difícil de alcançar, mas que um acordo sobre regras ou diretrizes sobre como empresas e Estados poderiam navegar em diferenças regulatórias na América Latina e no Caribe poderia ser gerenciável. Alguns dos atores enfatizaram que a estruturação de um sistema em torno de incentivos ao investimento privado deve ser a prioridade, para permitir que a indústria possa operar em todos os países. Todas essas preocupações e sugestões salientam a necessidade de coordenação e cooperação intrarregional e global.

INFOGRÁFICO 9

Considerando o potencial da IoT para revolucionar muitas áreas da economia, como agricultura, medicina e transporte, até que ponto você acredita que harmonização regulatória é necessária global, regional ou nacionalmente (por exemplo, nos Estados federais)?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

3.1. Do privado ao público: casas inteligentes conectadas em cidades inteligentes conectadas

As oportunidades oferecidas pela IoT estendem-se a qualquer coisa que possa ter um sensor instalado e estar conectada à Internet, desde o mais íntimo (o corpo humano) até o mais público (cidades), incluindo casas, indústrias e campos.²⁵¹ A natureza transversal da IoT significa que oportunidades e desafios podem ser encontrados em uma vasta gama de áreas temáticas e setores.

A aplicação mais próxima da experiência humana está nos vestíveis: dispositivos inteligentes que as pessoas têm sobre elas, ao lado de seus corpos e ajudando-as em suas atividades diárias. Eles abrangem os dispositivos mais utilizados, como relógios inteligentes (*smartwatches*), até os mais sofisticados que medem

251 Ver: <<https://www.internetsociety.org/policybriefs/iot-privacy-for-policy-makers/>>. Acesso em: 09 mai 2021.

ondas cerebrais ou ritmos cardíacos. Sua conveniência e valor derivam da sua capacidade de fornecer facilmente informações sobre o status de uma pessoa, permitindo uma melhor tomada de decisões.

A situação é semelhante com eletrodomésticos conectados (IoT). Eles, sem dúvida, oferecem muitos benefícios, aumentando a facilidade e eficiência do uso de bens e serviços que podem reduzir o consumo doméstico (eletricidade, água e gás), por exemplo, ou fornecendo segurança e proteção, no caso de câmeras que monitoram uma residência ou aparelhos que apresentam um incêndio ou bloqueiam a propriedade quando há perigo. Eles podem servir para estabelecer uma melhor conexão com o mundo exterior, facilitando a compra de alimentos ou a chamada de serviços.

No entanto, eles também trazem riscos potenciais. A IoT trabalha com dados que fornecem as percepções necessárias para que bens e serviços inovadores sejam fornecidos. A ubiquidade²⁵² e a intimidade de muitos desses dispositivos minam a separação entre as esferas pública e privada e podem perverter a presunção de privacidade que as pessoas associam com seus lares e corpos.²⁵³ É difícil para as pessoas controlar e compreender as classes de dados coletados e processados. Assim, questões de transparência, controle, consentimento e responsabilidade precisam ser abordadas.

Considerando que os fornecedores podem ter um alcance global,²⁵⁴ a cooperação e a coordenação parecem ser de suma importância. Muitas das iniciativas assumiram a forma de planos, estratégias e políticas nacionais. A maioria apenas incorporou marginalmente uma dimensão global ou regional, não conseguindo estabelecer uma ligação entre essas dimensões e o tema da própria IoT. Os atores entrevistados concordaram sobre a necessidade de harmonização, mas pareciam estar

252 Alguns dispositivos estão sempre ligados, coletando dados pessoais. Disponível em: <https://fpf.org/wp-content/uploads/2016/04/FPF_Always_On_WP.pdf>.

253 Internet Society, "Policy Brief: IoT Privacy for Policymakers", 19 de setembro de 2019. Disponível em: <<https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/>>. Acesso em: 09 mai 2021.

254 Um estudo realizado pela McKinsey chamou a atenção para o alcance global de certos prestadores de serviços. Ver: <<https://www.mckinsey.com/industries/technology-media-and-telecommunications/our-insights/unlocking-value-from-iot-connectivity-six-considerations—for-choosing-a-provider>>. Acesso em: 09 mai 2021.

divididos quanto à necessidade de regras específicas para a IoT. Por exemplo, alguns questionaram se regulações subjacentes que tratam de assuntos como proteção de dados pessoais, de consumidores e segurança cibernética deveriam ser interpretadas de forma ampla para englobar os desafios apresentados por essa tecnologia.

PLANOS, ESTRATÉGIAS E AÇÕES DE IOT

O Brasil tem um Plano Nacional de Internet das Coisas focado em quatro setores principais: cidades inteligentes, saúde, agronegócio e manufatura. O plano também enfatiza quatro áreas estratégicas para o desenvolvimento: inovação e internacionalização, capital humano, segurança regulatória e privacidade, infraestrutura para conectividade e interoperabilidade.²⁵⁵

O México fez da Internet das Coisas industrial uma prioridade política. A fabricação de automóveis é um dos pontos focais.²⁵⁶

A Argentina e Colômbia desenvolveram políticas de IoT em parceria com o setor privado. O foco é incentivar parcerias estratégicas, cooperação e acordos comerciais para promover um ambiente propício ao desenvolvimento da IoT.²⁵⁷

As cidades inteligentes são outra área onde a IoT desempenha um papel transformador. Essa tecnologia pode ser integrada à paisagem da cidade, captando e analisando dados para permitir que as autoridades resolvam melhor os problemas dos seus municípios, seja através de meios tradicionais ou tecnológicos.²⁵⁸ A IoT ajuda a organizar o ambiente urbano, criando

-
- 255 Em 2019, o plano foi institucionalizado pelo Decreto Presidencial nº 2984/2019. Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Decreto/D9854.htm>. Acesso em: 09 mai 2021. O plano original foi lançado em 2017 por meio de uma iniciativa multissetorial em parceria com o Banco Nacional de Desenvolvimento Econômico e Social (BNDES). Disponível em: <<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>>. Acesso em: 09 mai 2021.
- 256 Ver: <<https://www.gob.mx/promexico/acciones-y-programas/mapas-de-ruta-22850>>. Acesso em: 09 mai 2021.
- 257 Na Colômbia, isso foi feito através do Centro de Excelência para a Internet das Coisas (CEA-IoT). Ver: <<http://www.cea-iot.org>>. Acesso em: 09 mai 2021. Na Argentina, a Internet e a Câmara de IoT desempenham o mesmo papel. Ver: <<http://cabaseiot.com.ar>>. Acesso em: 09 mai 2021.
- 258 Inter-American Development Bank (IDB), "Big urban data: a strategic guide for cities", 2019. Disponível em: <<https://publications.iadb.org/en/big-urban-data-strategic-guide-cities>>. Acesso em: 09 mai 2021.

a base para respostas mais rápidas e baseadas em evidências. A implementação está a caminho de áreas como tráfego, estacionamento, segurança, poluição e higiene.²⁵⁹

Projetos de cidades inteligentes tendem a ser implementados através de parcerias público-privadas envolvendo uma infinidade de atores, nem todos eles do país em causa. Cada camada envolve uma série complexa de decisões sobre, por exemplo, quais instituições e empresas devem ser envolvidas, de onde os suprimentos devem vir, qual deve ser a estrutura e como e por quem o projeto deve ser administrado. As respostas podem exigir coordenação regional e internacional.

Potenciais complexidades jurisdicionais estão, portanto, surgindo em muitos pontos de contato internacionais. Cada camada, a partir da infraestrutura de conectividade (5G, por exemplo), depende de alianças estratégicas e cooperação entre um número de fornecedores e provedores que podem estar situados em qualquer lugar do planeta. À medida que o ecossistema de IoT na região se torna mais complexo e bens e serviços são cada vez mais fornecidos, através de uma cadeia de fornecedores que pode não estar estabelecida no mesmo país que o usuário, soluções jurisdicionais podem precisar ser revistas.

A região da América Latina e do Caribe é uma das mais urbanizadas do mundo e os desafios são proporcionalmente grandes. Assim, a IoT para serviços públicos poderia ter um impacto substancial, alterando todo o panorama das cidades e a forma como as políticas públicas são projetadas para elas. As próprias cidades e os países da região, sozinhos, não podem fornecer todas as soluções necessárias.²⁶⁰ Há uma tendência a buscar parcerias e alianças com fornecedores estrangeiros, o que torna a necessidade de coordenação ainda maior.

Dois outros aspectos assumem um caráter particular na América Latina e no Caribe: dados municipais abertos e participação

259 Inter-American Development Bank (IDB) IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean. Disponível em: <<https://publications.iadb.org/en/iot-lac-2019-taking-pulse-internet-things-latin-america-and-caribbean>>. Acesso em: 09 mai 2021.

260 Inter-American Development Bank (IDB), The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City, 2016. Disponível em: <<https://publications.iadb.org/handle/11319/7743?locale-attribute=es&>>. Acesso em: 09 mai 2021.

cidadã. Em comparação com seus pares em outros lugares, as cidades da região foram rápidas em abraçar dados abertos. Isso permite que os dados disponíveis sejam reaproveitados para serviços inovadores. A partir de uma iniciativa brasileira na década de 1990, a participação cidadã na alocação de recursos municipais tornou-se parte da dinâmica administrativa de muitas cidades da região.²⁶¹ Nesse contexto, o uso de plataformas on-line em combinação com a IoT pode levar a discussões sobre responsabilização, controle e alocação de responsabilidade.

INICIATIVAS NOTÁVEIS DE CIDADES INTELIGENTES ENVOLVENDO A IOT NA AMÉRICA LATINA E NO CARIBE

Várias cidades na Argentina têm implantado soluções de IoT.²⁶² Tigre, uma cidade na grande Buenos Aires, foi um dos primeiros municípios da América Latina e do Caribe a implementar um centro de operações para proteger o público e combater o crime, empregando câmeras de reconhecimento facial e de placas de veículos para rastrear criminosos e carros roubados, entre outras coisas. Essa iniciativa foi possível através de uma parceria público-privada com empresas multinacionais e análise de dados em nuvem.²⁶³

Um mecanismo de "semáforos inteligentes" foi desenvolvido para rotas de transporte em Chacao e Maracay, na República Bolivariana da Venezuela. O sistema proporciona uma melhor gestão do tráfego, reduzindo o tempo gasto em trânsito e os acidentes rodoviários.

Medellín, na Colômbia, desenvolveu um centro de operações integrado que coordena ações de segurança e emergência, permitindo que agências nas áreas de segurança, transporte, assistência médica emergencial, gestão de desastres, meio ambiente e bem-estar respondam de forma coordenada a uma única chamada. O programa conta com o uso extensivo de câmeras de vigilância e o georreferenciamento de chamadas.

261 Inter-American Development Bank (IDB), "Big urban data: a strategic guide for cities", 2019. Disponível em: <<https://publications.iadb.org/en/big-urban-data-strategic-guide-cities>>. Acesso em: 09 mai 2021.

262 Para uma visão geral das diferentes iniciativas de cidades inteligentes na Argentina, ver: <<https://www.camarabilbao.com/ccb/contenidos.downloadatt.action?id=5334087>>. Acesso em: 09 mai 2021.

263 Ver: <<https://www.nec.com/en/case/tigre/index.html>>. Acesso em: 09 mai 2021.

Em 2017, o Chile lançou um programa-piloto em Temuco para buscar soluções inteligentes para cidades em uma plataforma aberta. Foram selecionadas quatro áreas principais: monitoramento da qualidade do ar, pontos de ônibus virtuais, gerenciamento de coleta de lixo e gerenciamento de incidentes na cidade.²⁶⁴

Itu, no estado de São Paulo, Brasil, emprega uma parceria público-privada para gerenciar a disposição de resíduos. A prefeitura utiliza um número de contêineres e instalações subterrâneas de armazenamento de resíduos conectados a sensores que indicam se há necessidade de reparos ou substituições, além de notificar os níveis de enchimento. Isso permite um melhor encaminhamento de caminhões de coleta, reduzindo tempo, custos e impactos ambientais.²⁶⁵

Inclusão digital e acesso a serviços digitais é o objetivo do programa Cidade Digital Chihuahua, no México. A iniciativa é uma parceria público-privada que oferece cobertura Wi-Fi em várias áreas públicas do município, incluindo escritórios públicos e parques. A iniciativa visa democratizar o acesso à Internet e aos serviços públicos digitais.²⁶⁶

A cidade de Nassau, nas Bahamas, desenvolveu um sistema de gerenciamento de água que detecta vazamentos, permite o reparo avançado e a substituição de tubulações, monitora a pressão e gerencia diferentes níveis de medição. Isso permitiu ao município cortar custos e reduzir o desperdício de água de 58% para 29%.²⁶⁷

3.2. A agricultura inteligente pode ser uma grande oportunidade regional

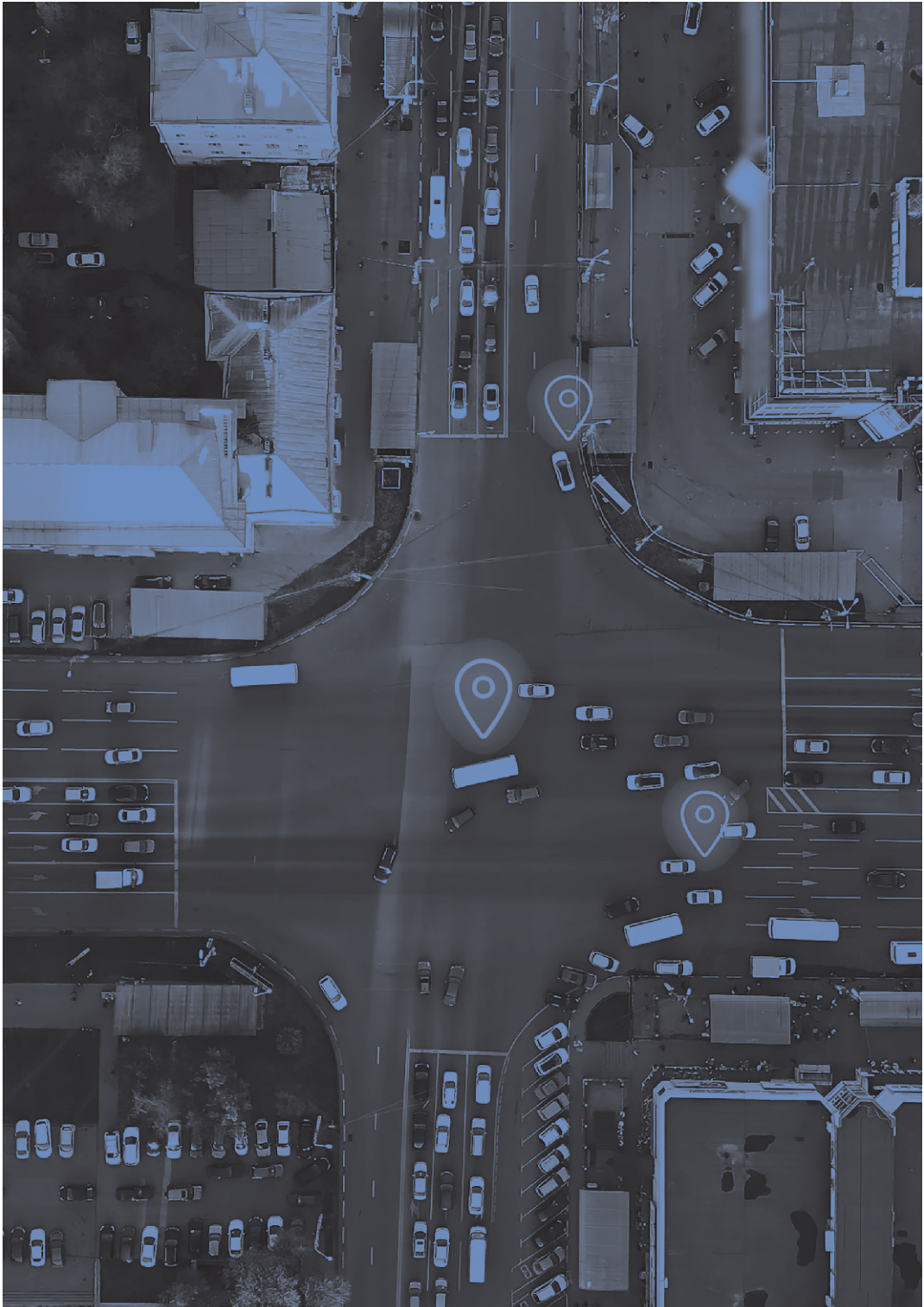
Alguns setores da economia da América Latina e do Caribe parecem mais dispostos do que outros a empregar a Internet

264 Ver: <<https://www.ufro.cl/index.php/noticias/12-destacadas/1424-temuco-sera-la-primera-ciudad-inteligente-de-chile-y-piloto-para-otras-ciudades-de-latinoamerica>>. Acesso em: 09 mai 2021.

265 Ver: <<https://exame.abril.com.br/revista-exame/o-que-aprender-com-a-excecao/>>. Acesso em: 09 mai 2021.

266 Ver: <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>. Acesso em: 09 mai 2021.

267 Inter-American Development Bank (IDB), *The Road toward Smart Cities: Migrating from Traditional City Management to the Smart City*, 2016. Disponível em: <<https://publications.iadb.org/handle/11319/7743?locale-attribute=es&>>. Acesso em: 09 mai 2021.



das Coisas em suas atividades, e nenhum deles mais do que a agricultura. A agricultura representa uma parte substancial da economia na maioria dos países da região e tende a ser um alicerce das exportações.²⁶⁸ O aumento da produtividade nesta área pode ter um impacto exponencial sobre o produto interno bruto (PIB) e, incidentalmente, também ter um efeito positivo sobre o meio ambiente, levando a um uso mais eficiente da terra e de outros recursos naturais.²⁶⁹

A agricultura inteligente (*smart farming*)²⁷⁰ e as *start-ups* de tecnologia agrícola (*agritech*) podem representar uma grande oportunidade para a região. A implantação da tecnologia IoT para o agronegócio pode impactar muitas áreas, tais como o gerenciamento de culturas, cultivo de precisão, monitoramento de rebanhos, agricultura vertical intensiva, tanto em ambientes internos quanto externos, e melhor utilização da aquicultura. A IoT para fazendas pode ter um impacto positivo em toda a cadeia de valor, melhorando tanto a tomada de decisões quanto a eficiência e precisão das ações tomadas. Plantio, monitoramento, colheita, distribuição, armazenamento e comercialização podem ser revolucionados.²⁷¹

Uma parte significativa do valor agregado pela Internet das Coisas na agricultura vem do acesso a dados que de outra forma seriam muito difíceis de coletar. Exemplos notáveis são indicadores de umidade do solo e microclima. Estes podem variar bruscamente. A implantação de tecnologias de IoT pode facilitar o mapeamento e o monitoramento desses indicadores. Os maiores benefícios vêm de análises avançadas que dependem

268 Inter-American Development Bank (IDB), *The Next Global Breadbasket: How Latin America Can Feed the World: a Call to Action for Addressing Challenges and Developing Solutions*, 2018. Disponível em: <<https://publications.iadb.org/en/publication/17428/next-global-breadbasket-how-latin-america-can-feed-world-call-action-addressing>>. Acesso em: 09 mai 2021.

269 Inter-American Development Bank (IDB), *IoT IN LAC 2019: Taking the Pulse of the Internet of Things in Latin America and the Caribbean*. Disponível em: <<https://publications.iadb.org/en/iot-lac-2019-taking-pulse-internet-things-latin-america-and-caribbean>>. Acesso em: 09 mai 2021.

270 Food and Agriculture Organization of the United Nations (FAO), "Smart farming is key for the future of agriculture", 2018. Disponível em: <<http://www.fao.org/family-farming/detail/en/c/897026/>>. Acesso em: 09 mai 2021.

271 Ver: <https://www.researchandmarkets.com/research/lv69c3/global_iiot_in?w=4>. Acesso em: 09 mai 2021.

da escala e do volume dos dados disponíveis e da capacidade de processamento.²⁷² Esses dois aspectos podem levar à prestação de serviços em todas as jurisdições e através de parcerias com entidades que operam transnacionalmente.²⁷³

Os aspectos transfronteiriços não terminam aí. Muitas dessas soluções de IoT não provêm de empresas tradicionais do setor agrícola, como aquelas envolvidas na agricultura, ou de fornecedores convencionais, como fabricantes de equipamentos agrícolas, fornecedores ou distribuidores de sementes, alimentos vegetais ou produtos químicos. Os desenvolvedores de software e as empresas de análise preditiva de dados estão se tornando cada vez mais parte das operações agrícolas. Muitas dessas empresas não tradicionais não estão sediadas no mesmo país que os usuários (fazendas), são assistidas por ou fazem parte de uma parceria ou acordo com entidades de outros países. Um exemplo claro é o uso de serviços em nuvem: a maioria dos provedores não está na região, nem são necessariamente processados localmente.

DESENVOLVIMENTOS E INICIATIVAS NOTÁVEIS NA AGRICULTURA INTELIGENTE

A agricultura de arroz na Colômbia está se beneficiando de um projeto realizado em parceria com uma empresa japonesa. A solução IoT possui sensores que coletam dados ambientais, como temperatura do ar e do solo, umidade e irradiação solar. Esse projeto levou a uma melhor tomada de decisões e respostas mais eficientes e oportunas.²⁷⁴

O monitoramento da pecuária também está recebendo atenção, uma vez que é necessária uma verificação constante da ingestão de água e ração animal. No Brasil, um projeto realizado em parceria com empresas multinacionais facilitou a

272 Ver: <<https://www.researchandmarkets.com/reports/4600903/iot-in-agriculture-market-outlook-and-forecasts#rela1-4669235>>. Acesso em: 09 mai 2021.

273 Em um estudo realizado pelo Banco Mundial, essas parcerias são apontadas como cruciais para o desenvolvimento do setor. Ver: <<http://documents.worldbank.org/curated/en/610081509689089303/pdf/120876-REVISED-WP-PUBLIC-Internet-of-Things-Report.pdf>>. Acesso em: 09 mai 2021.

274 Ver: <<https://www.e-kakashi.com/en/case/details01>>. Acesso em: 09 mai 2021.

pesagem dos animais e a análise de dados sobre seu desenvolvimento.²⁷⁵ Além disso, *start-ups* e empresas tradicionais fornecem tecnologia que monitora a geolocalização dos rebanhos e o estado de saúde dos animais.²⁷⁶ Outros gerenciam toda a cadeia “da fazenda à mesa”, adicionando sensores e inteligência agrícola a todos os processos.²⁷⁷ Da mesma forma, na Argentina, as *start-ups* estão ajudando a monitorar lavouras e rebanhos, usando uma série de estratégias que vão desde rastreadores a drones autônomos para capturar e analisar informações sobre atividades agrícolas.²⁷⁸

No Peru, algumas iniciativas procuram usar a IoT para monitorar as condições ambientais e climáticas.

Antenas e drones são utilizados para capturar dados dos campos em uma série de aspectos que vão da topografia à qualidade do ar.²⁷⁹

No Chile, os recursos naturalmente disponíveis sob a forma de vinhas geneticamente antigas estão sendo aproveitados, ao combinar esses recursos com tecnologia para produzir uma estufa *in vitro* para variedades antigas de videiras.²⁸⁰

Em Guanajuato, México, um centro de tecnologia agrícola surgiu e está incentivando uma série de projetos para empresas, desde o monitoramento de lavouras até estratégias de irrigação.²⁸¹

275 Ver: <<https://blog.bosch-si.com/agriculture/connected-agriculture-beefed-up-networking-in-brazil/>>. Acesso em: 09 mai 2021. Para um estudo geral sobre sua implantação no sul do Brasil, ver: <<https://lume.ufrgs.br/handle/10183/178439?locale-attribute=pt>>. Acesso em: 09 mai 2021.

276 Um exemplo é Allflex (ver: <<http://www.allflex.com.br/identificacao-eletronica/brincos-eletronicos-fdx/>>. Acesso em: 09 mai 2021). Outros são: Intergado, Cowmed e Imeve (ver: <<https://www.beefpoint.com.br/o-olho-do-dono-que-engorda-o-boi-agora-e-digital/>>. Acesso em: 09 mai 2021).

277 Um exemplo é BovControl (ver: <<https://www.bovcontrol.com>>. Acesso em: 09 mai 2021; <<http://g1.globo.com/tecnologia/blog/startup/post/app-permite-a-fazendeiro-monitorar-bois-e-vacas-na-tela-do-pc.html>>. Acesso em: 09 mai 2021).

278 Por exemplo, o Tambero conecta dados de informações agrícolas a uma plataforma de serviços em nuvem (ver: <<https://www.tambero.com>>. Acesso em: 09 mai 2021). No outro extremo do espectro, a Skyagro usa drones autônomos para coletar os dados necessários (ver: <<https://www.infocampo.com.ar/skyagro-drones-hechos-en-argentina-que-toman-y-analizan-imagenes-en-los-campos/>>. Acesso em: 09 mai 2021).

279 As *start-ups* peruanas, como Spacedat e Qaira, são exemplos significativos. Ver: <<http://www.qairadrones.com/index.php?r=site/nosotros>>; e <<https://www.spacedat.com>>. Acessos em: 09 mai 2021.

280 Ver: <<https://www.andeswines.com/business-acceleration-service/>>. Acesso em: 09 mai 2021.

281 Ver: <<http://agrobioteg.org>>. Acesso em: 09 mai 2021.

4. MEIOS DE PAGAMENTOS DIGITAIS

A Internet mudou o cenário de diversos negócios em todo o mundo. O setor financeiro tem sofrido recentemente as consequências disso.²⁸² Novos serviços e novos modelos de negócios estão aproveitando a conectividade do mundo on-line para diminuir as barreiras de entrada no mercado financeiro, de modo que mais produtos e serviços possam ser fornecidos a uma base mais ampla de clientes. Sua natureza virtual significa que eles não precisam estar sediados em nenhum país, mas podem fomentar e permitir transações transfronteiriças.

No entanto, ainda existe uma lacuna significativa entre as pessoas que são servidas por instituições financeiras tradicionais e aquelas que não o são. Uma parte substancial da população é pouco atendida ou excluída dos serviços financeiros. Estas lacunas representam um impedimento significativo para um mercado único digital: as pessoas são dissuadidas de entrar no mercado ou simplesmente não conseguem acessá-lo. Assim, os bens e serviços fornecidos pela Internet também são impactados, tornando-se inacessíveis ou de difícil acesso para grande parte da população.

Na América Latina e no Caribe, isso é agravado pela penetração relativamente baixa dos serviços bancários e dos cartões de crédito internacionais, por uma cultura persistente de pagamento em dinheiro e pela volatilidade cambial. Isso representa uma oportunidade para os novos participantes encontrarem novas soluções, não só oferecendo novos produtos e serviços, mas aumentando o acesso ao financiamento.²⁸³

Assim, *start-ups* e projetos inovadores estão tentando resolver as desigualdades de acesso financeiro da região.²⁸⁴ A Amé-

282 O Banco Mundial e o Fundo Monetário Internacional (FMI) patrocinaram a Agenda Fintech de Bali, destacando as oportunidades e os riscos para os prestadores de serviços financeiros inovadores. Ver: <<https://www.worldbank.org/en/topic/fintech>>. Acesso em: 09 mai 2021.

283 Banco Interamericano de Desenvolvimento (IDB), FINTECH: Innovations You May Not Know were from Latin America and the Caribbean, 2018. Disponível em: <<https://publications.iadb.org/en/fintech-innovations-you-may-not-know-were-latin-america-and-caribbean>>. Acesso em: 09 mai 2021.

284 Inter-American Development Bank (IDB), Regulatory Sandboxes in Latin America and the Caribbean for the FinTech Ecosystem and the Financial System, 2018. Disponível em: <<https://publications.iadb.org/publications/english/document/Regulatory-Sandboxes-in-Latin-America-and-the-Caribbean-for-the-FinTech-Ecosystem-and-the-Financial-System.pdf>>. Acesso em: 09 mai 2021.

rica Latina e o Caribe experimentam um *boom* de empresas que estão alinhando novas tecnologias com novas oportunidades no mercado financeiro.²⁸⁵ Tem havido um crescimento extraordinário no chamado mercado de tecnologias financeiras (*fintech*).²⁸⁶ As iniciativas se espalharam em diferentes áreas. Duas delas ganharam impulso especial na região: os pagamentos digitais, apoiados pelo crescimento de novas empresas bancárias (neobancos), e as tecnologias de *blockchain*, na forma de criptomoedas e outras aplicações potenciais que serão exploradas a seguir.

Os entrevistados destacaram essa tendência e a importância que as empresas de tecnologias financeiras vêm adquirindo na região. Eles destacaram o seu potencial para diminuir a desigualdade de acesso aos serviços financeiros e aproveitar o mercado digital. No entanto, eles observaram que as iniciativas de harmonização podem ser dificultadas pelas diferenças nas tradições de regulação financeira da região e pela dimensão e natureza díspares das suas economias.

4.1. Impactos jurisdicionais transfronteiriços nas atividades das empresas *fintech*

Os mecanismos de pagamento são cruciais para o desenvolvimento do comércio digital de bens e serviços. A capacidade de realizar pagamentos digitalmente não é um fato consumado, particularmente em transações transfronteiriças. É necessário que os acordos de pagamento sejam eficientes e acessíveis se quiserem servir como canais para que os fundos fluam de um lado para o outro em uma transação on-line.²⁸⁷ Os aspectos econômicos das transações pela Internet, então, dependem ou podem ser resolvidos através de uma série de intermediários em várias camadas que mantêm a infraestrutura de pagamentos digitais.

285 Inter-American Development Bank (IDB) /Finnovista, Fintech. Latin America 2018: Growth and Consolidation. Disponível em: <<https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf>>. Acesso em: 09 mai 2021.

286 Economic Commission for Latin America and the Caribbean (ECLAC), Data, algorithms and policies: redefining the digital world (LC/CMSI.6/4), Santiago, 2018.

287 Ver: <<https://www.fsb.org/wp-content/uploads/P090420-2.pdf>>. Acesso em: 09 mai 2021.

Na ausência de meios de pagamento acessíveis e baratos, nenhum mercado digital pode funcionar adequadamente. Na América Latina e no Caribe, o ambiente financeiro está repleto de oportunidades para desenvolver novas abordagens, sejam eles novos modelos de negócios ou novos produtos e serviços. O crescimento na disponibilidade de smartphones e na conectividade móvel também impulsionou a mudança para as primeiras abordagens on-line e até mesmo de aplicativos móveis.

Existem várias soluções bancárias e de pagamento digital na região. O mercado vem se movendo em direção a novas abordagens, levando à criação de um ecossistema de empresas que as fornecem.

O ambiente *fintech* na América Latina e no Caribe é composto por centenas de *start-ups* e novas iniciativas lançadas por atores mais tradicionais.²⁸⁸ Em 2018, por exemplo, já havia 380 *start-ups fintech* no Brasil, 273 no México, 148 na Colômbia, 116 na Argentina, e 84 no Chile.²⁸⁹ Elas englobam uma série de atividades diferentes. Entre as mais importantes estão soluções relacionadas a transferências e gerenciamento de fundos; transferências e remessas internacionais; pontos de venda móveis; *gateways* de pagamento e agregadores para aceitar, autorizar e processar pagamentos em plataformas digitais; e neobancos, entidades financeiras de alta tecnologia que possuem licenças bancárias por direito próprio ou de terceiros.²⁹⁰

Algumas dessas empresas oferecem serviços transfronteiriços, como remessas internacionais, ou são elas próprias empresas transfronteiriças que internacionalizaram suas operações. As iniciativas governamentais são importantes para proporcionar um quadro institucional para fomentar o crescimento e

288 Inter-American Development Bank (IDB)/Finnovista, Fintech. Latin America 2018: Growth and Consolidation. Disponível em: <<https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf>>. Acesso em: 09 mai 2021.

289 Segundo a Finnovista, os números são ainda maiores em 2020. Ver: <<https://www.finnovista.com/tag/fintech-radar/>>. Acesso em: 09 mai 2021.

290 Inter-American Development Bank (IDB)/Finnovista, Fintech. Latin America 2018: Growth and Consolidation. Disponível em: <<https://publications.iadb.org/publications/english/document/Fintech-Latin-America-2018-Growth-and-Consolidation-final.pdf>>. Acesso em: 09 mai 2021.

criar as condições para novas soluções financeiras. As tentativas de promover a convergência regulatória poderiam ajudar a garantir mercados regionais e internacionais para essas empresas. Entretanto, os aspectos jurisdicionais transfronteiriços devem ser levados em consideração para que o processo seja apoiado em vez de dificultado.

Já existe uma tendência para regular o setor *fintech*, o que criou uma oportunidade de coordenação e cooperação entre os países da região. Em julho de 2018, por exemplo, os membros da Aliança do Pacífico concordaram em um conjunto de princípios orientadores para a regulação das *fintech*.²⁹¹

No nível nacional, dois caminhos são explorados pelos países da região: (i) regular o setor *fintech* como um todo, incluindo pagamentos digitais e transações bancárias de neobancos; e (ii) regulá-lo através da adaptação da estrutura jurídica existente.²⁹²

O México, por exemplo, tem liderado o caminho com a legislação geral para regular o setor *fintech*.²⁹³ A legislação trata de quatro áreas principais: instituições de tecnologia financeira, incluindo empresas de *crowdfunding* e instituições de pagamento eletrônico; ativos virtuais (criptomoedas); interface de programação de aplicativos (API, na sigla em inglês); e *sandboxes* regulatórias. O Brasil, por outro lado, seguiu a segunda abordagem, integrando as questões relativas às tecnologias financeiras à regulamentação existente.²⁹⁴ Honduras emitiu uma regulamentação para permitir o uso de carteiras

291 Ver: <<https://alianzapacifico.net/wp-content/uploads/Principios-orientadores-para-la-regulacion-Fintech.pdf>>. Acesso em: 09 mai 2021.

292 International Monetary Fund (IMF), "Fintech: the experience so far", Jun 2019. Disponível em: <<https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056>>. Acesso em: 09 mai 2021.

293 Ley para regular las instituciones de tecnologia financiera, Março 2018. Disponível em: <<https://perma.cc/SB6N-RQY7>>. Acesso em: 09 mai 2021.

294 International Monetary Fund (IMF), "Fintech: the experience so far", Jun 2019. Disponível em: <<https://www.imf.org/en/Publications/Policy-Papers/Issues/2019/06/27/Fintech-The-Experience-So-Far-47056>>. Acesso em: 09 mai 2021.

eletrônicas.²⁹⁵ O Peru tem uma regulação semelhante,²⁹⁶ assim como El Salvador.²⁹⁷ Na Colômbia, os diferentes atores estão atualmente debatendo se é necessário ter um marco regulatório específico para as *fintechs*.²⁹⁸

4.2. Open Banking e o ecossistema fintech

O *open banking* (sistema bancário aberto) é uma das iniciativas que estão crescendo na região a partir do ecossistema das tecnologias financeiras. É uma oportunidade para gerar a infraestrutura jurídica e técnica necessária para um ambiente financeiro mais competitivo. O *open banking* torna diferentes serviços financeiros interoperáveis e abre o mercado para que os usuários possam optar por compartilhar seus dados financeiros com diferentes instituições financeiras e se beneficiar de um conjunto mais amplo de produtos e serviços. Estabelece um ambiente de compartilhamento de dados entre setores, integrando diferentes plataformas e infraestruturas. Geralmente envolve o desenvolvimento de uma interface de programação de aplicativos (API) que permite que diferentes provedores de serviços financeiros interajam.

O escopo da maioria dessas iniciativas indica pouca consciência aparente do potencial transfronteiriço do sistema de *open banking*. Sob um arcabouço legal regional ou mais amplo, os clientes poderiam se beneficiar de produtos e serviços financeiros fornecidos por uma rede muito maior de fornecedores. Ao mesmo tempo, a internacionalização da tecnologia financeira da região levará à exportação de diferentes soluções bancárias abertas que poderão entrar em conflito ou terão que ser reformuladas.

295 Ver: <<https://www.elheraldo.hn/pais/936203-466/uso-de-la-billetera-electrica-legal-en-honduras>>. Acesso em: 09 mai 2021.

296 Ver: <<https://www.mef.gob.pe/es/por-instrumento/decreto-supremo/9970-decreto-supremo-n-090-2013-ef/file>>. Acesso em: 09 mai 2021.

297 Ver: <https://www.bcr.gob.sv/regulaciones/upload/NORMAS_PARA_LA_AUTORIZACION_DE_ADMINISTRADORES_DE_SISTEMAS_DE_PAGOS_MOVILES.pdf?v=1589709520>. Acesso em: 09 mai 2021.

298 Inter-American Development Bank (IDB)/Finnovista, "The Fintech ecosystem in Costa Rica", 2019. Disponível em: <<https://www.finnovista.com/el-bid-y-finnovista-publican-un-diagnostico-del-ecosistema-fintech-en-costa-rica-2019/?lang=en>>. Acesso em: 09 mai 2021.

Internacionalmente, as iniciativas tomaram uma das duas rotas possíveis: uma orientada para o mercado, com a indústria, o governo ou uma parceria dos dois que estabelecem orientações e normas comuns e, em seguida, deixando o mercado livre para desenvolver nessa base; e uma regulação, com as autoridades governamentais estabelecendo o quadro global a ser seguido pelas instituições financeiras.

Na região, pelo menos dois países parecem estar seguindo a segunda rota. Em 4 de maio de 2020, o Brasil emitiu um conjunto de regulações por meio de suas instituições de supervisão financeira. A implementação é dividida em quatro fases, proporcionando alguma margem de manobra para que a indústria estabeleça seus próprios padrões de compartilhamento de dados e forneça acesso aos serviços.²⁹⁹ A estrutura legal proposta pelo México para o sistema bancário aberto faz parte de sua regulação *fintech*.³⁰⁰ Em outros países da região, a própria indústria tem insistido na regulação para que o setor possa avançar.³⁰¹

4.3. Soluções regulatórias inovadoras: o apelo das *sandboxes* regulatórias

Novas soluções financeiras de alta tecnologia dependem da experimentação e inovação em produtos e serviços financeiros e de modelos de negócios. No entanto, isso pode acarretar

299 Ver: <<https://www.bcb.gov.br/en/pressdetail/2284/nota>>. Acesso em: 09 mai 2021. Para a Resolução Conjunta nº 4 de 2020, em português, ver: <<http://www.in.gov.br/en/web/dou/-/resolucao-conjunta-n-1-de-4-de-maio-de-2020-255165055>>. Acesso em: 09 mai 2021.

300 Ver: <<https://iupana.com/2020/02/28/mexicos-fintech-law-open-banking-rules-delayed/?lang=en#widget/?lang=en>>. Acesso em: 09 mai 2021.

301 Ver, por exemplo, o estudo realizado pela FinteChile e pela EY sobre o futuro dos bancos abertos no Chile. Disponível em: <https://www.ey.com/es_cl/financial-services/open-banking—oportunidades-y-desafios-para-chile>. Acesso em: 09 mai 2021. A Colômbia Fintech, em parceria com entidades do Reino Unido, procurou desenvolver padrões bancários abertos para o ambiente colombiano. Ver: <<https://www.ebankingnews.com/noticias/open-banking-desafios-y-oportunidades-en-colombia-0047125>>. Acesso em: 09 mai 2021. Para uma análise do ambiente colombiano, ver D. P. García Abella e J. C. Segura Cárdenas, "Open Banking: del concepto a la competencia". Disponível em: <https://repository.eafit.edu.co/bitstream/handle/10784/14228/DianaPatricia_GarciaAbella_2019_JuanCarlos_SeguraCardenas_2019.pdf?sequence=2&isAllowed=y>. Acesso em: 09 mai 2021.

riscos individuais e/ou sistêmicos que devem ser explorados de antemão. A regulação tradicional geralmente não é capaz de abranger esses quadros inovadores em tempo hábil. Muitos países, então, estão testando estruturas regulatórias não tradicionais para lidar com esses riscos de forma segura e eficiente em termos de tempo. As áreas de segurança (*sandboxes*) foram propostas como uma estratégia atraente e estão sendo implementadas por alguns Estados, inclusive alguns na América Latina e no Caribe.

As *sandboxes* regulatórias oferecem uma oportunidade para soluções inovadoras operarem para um número restrito de usuários (clientes) durante um período limitado. As iniciativas estão frequentemente sujeitas a obrigações menos rigorosas, desde que sejam continuamente monitoradas e supervisionadas por um órgão governamental autorizado.

Essas *sandboxes* têm a vantagem de proporcionarem espaços para teste de novos projetos. Limitam o seu impacto e, conseqüentemente, os seus riscos, permitindo às autoridades de supervisão monitorizar as reações dos agentes e do mercado, de modo a poderem propor abordagens, normas e regras específicas.

A maioria dos entrevistados afirmou que abordagens inovadoras, como *sandboxes* regulatórias, ajudam a fomentar o crescimento econômico na região. Destacaram as diferenças nas economias dos países da região, a possível falta de capacidade institucional e a limitada disponibilidade de recursos humanos como potenciais obstáculos à aplicabilidade dessas soluções regulatórias.

Estas reflexões destacam a necessidade e a oportunidade de cooperação e coordenação transfronteiriça. Os países da região podem se beneficiar de sua proximidade e reunir recursos. A elaboração de normas e abordagens comuns pode facilitar o trabalho de supervisão e reduzir a variação regulatória, tornando, assim, possível atender aos clientes excluídos ou não atendidos pelo setor de serviços financeiros tradicionais.

Alguns dos países da região já estão implantando tais soluções e podem liderar o caminho. Por exemplo, a lei do México que regula as empresas *fintech*³⁰² inclui a possibilidade de autorizações temporárias para "novos modelos financeiros".³⁰³ Da mesma forma, na Colômbia, a Superintendência Financeira criou um quadro legal que permite o uso *sandboxes* regulatórias para iniciativas financeiras inovadoras.³⁰⁴ O Brasil tem iniciativas de áreas de segurança regulatórias supervisionadas pelo Banco Central do Brasil³⁰⁵ e pela Comissão de Valores Mobiliários (CVM).³⁰⁶ As associações industriais também apresentaram propostas, com uma federação internacional de associações nacionais, com o objetivo de criar sinergia regulatória na região.³⁰⁷

INFOGRÁFICO 10

Alguns países da região da América Latina e do Caribe usaram estruturas inovadoras (por exemplo, *sandboxes* regulatórias) para permitir experiências em tecnologias de pagamento digital e *fintech*. Você acha que tal abordagem ajuda a fomentar o crescimento econômico regional?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

- 302 Ley para regular las instituciones de tecnologia financiera, Março 2018. Disponível em: <<https://perma.cc/SB6N-RQY7>>. Acesso em: 09 mai 2021.
- 303 Ver C. Kurc e A. Portilla, "México: Fintech 2019. Guías Jurídicas Comparativas Internacionales": <<https://iclg.com/practice-areas/fintech-laws-and-regulations/mexico>>. Acesso em: 09 mai 2021.
- 304 Ver: <<https://forbes.co/2020/02/06/economia-y-finanzas/hacienda-cobijara-con-decreto-el-sandbox-de-la-superfinanciera/>>. Acesso em: 09 mai 2021.
- 305 Ver: <<https://www.centralbanking.com/fintech/4397616/sandbox-initiative-central-bank-of-brazil>>. Para uma breve análise sugerindo que esta pode ser uma abordagem inovadora de área de segurança reguladora setorial, ver: <<https://www.jota.info/coberturas-especiais/inova-e-acao/banco-central-ganha-premio-de-melhor-iniciativa-de-sandbox-do-mundo-04092019>>. Acesso em: 09 mai 2021.
- 306 Em 15 de maio de 2020, a CVM emitiu a Instrução nº 626/2020 implementando *sandboxes* regulamentares. Ver: <<http://www.cvm.gov.br/noticias/arquivos/2020/20200515-l.html>>. Acesso em: 09 mai 2021.
- 307 Ver: <http://fintechiberoamerica.com/wp-content/uploads/2018/06/protocolo_implementaci0n_sandbox_iberoamerica.pdf> Acesso em: 09 mai 2021.

5. BLOCKCHAIN E CRIPTOMOEDAS

Blockchain é outra tecnologia que está sendo desenvolvida para facilitar as transações. *Blockchain* pode ser entendido como um livro contábil distribuído, onde os registros de transações de ponta a ponta (*peer-to-peer*) são mantidos sem a necessidade de uma autoridade central para coordená-lo. Satoshi Nakamoto conceituou a tecnologia em 2008 para eliminar o intermediário de confiança habitual envolvido na maioria das transações.³⁰⁸ A tecnologia de *blockchain* fornece uma maneira de lidar com a incerteza. A natureza distribuída do livro e sua natureza imutável (inviolável) e auto-execução tornam desnecessário para as partes conhecerem ou confiarem umas nas outras. A confiança passa a ser o resultado do uso de *blockchain*.³⁰⁹

O *Relatório de Status Global 2019* já destacou o interesse internacional por essa tecnologia tanto do setor privado quanto do público. No entanto, também notou o considerável ceticismo de alguns atores, especialmente dos Estados, em relação a aplicações específicas, mais notadamente as criptomoedas. A *bitcoin* tornou-se amplamente conhecida como uma dessas moedas. As dificuldades legais com essas moedas e com *blockchain* geralmente decorrem das próprias características que, na maioria dos casos, as tornam atraentes: a falta de uma autoridade central e o fato de que as pessoas não precisam conhecer ou confiar umas nas outras.

A natureza distribuída e desmaterializada do livro-razão (*ledger*) faz com que as fronteiras e os elementos jurídicos tradicionais sejam significativamente menos relevantes. O *blockchain* permite que o comércio transfronteiriço de todos os tipos seja realizado sem a necessidade de um intermediário para supervisioná-lo e inspecioná-lo. Isso significa que as transações legais e ilegais podem fluir sem o conhecimento das autoridades ou qualquer necessidade de estabelecer jurisdição.

As discussões sobre *blockchain* e criptomoedas tendem a se concentrar em contextos potencialmente ilegais, onde as transações podem ocorrer. Por um lado, *blockchain* e criptomoedas

308 S. Nakamoto "Bitcoin: A peer-to-peer electronic cash system", 2008. Disponível em: <<https://bitcoin.org/bitcoin.pdf>>. Acesso em: 09 mai 2021.

309 Economic Commission for Latin America and the Caribbean (ECLAC), Data, algorithms and policies: redefining the digital world (LC/CMSI.6/4), Santiago, 2018.

podem apoiar atividades criminosas, porque podem mudar de mãos facilmente, remotamente e sem referência a qualquer autoridade de controle. Por outro, eles parecem anônimos porque nenhuma informação sobre a identidade das pessoas que participam na transação é registrada. No entanto, isso não significa necessariamente que os envolvidos não possam ser identificados. O protocolo de *blockchain* permite que todas as transações sejam rastreadas, tornando possível recriar todo o seu histórico. Nesse aspecto, é muito menos anônimo do que a moeda física, cujos movimentos são difíceis de rastrear uma vez que tenha mudado de mãos.

O *blockchain*, além disso, pode ter muitas aplicações em diferentes áreas além das criptomoedas. A tecnologia de *blockchain* é usada mais notavelmente para registro de terras e imóveis e chamados “contratos inteligentes” (*smart contracts*), mas pode ser implantada em muitas áreas, tanto privadas quanto públicas, onde serve para criar um registro on-line confiável com funções automatizadas.³¹⁰ No que diz respeito aos “contratos inteligentes”, o termo não significa necessariamente contratos feitos usando *blockchain*. Os contratos habilitados para *blockchain*, no entanto, são considerados inteligentes de três maneiras: eles podem ser registrados permanentemente no *blockchain*; suas cláusulas podem ser baseadas em código; e há uma “garantia de execução” devido à aplicação automática através da rede *blockchain*.³¹¹ As implicações são enormes e podem mudar o cenário jurídico em muitos setores.

A escalabilidade, privacidade de dados e interoperabilidade são vistos como desafios significativos. O primeiro deles depende das operações da rede *blockchain* e da tecnologia subjacente a ela. Com relação à privacidade, a questão principal é o exercício dos direitos da pessoa em questão.³¹²

310 Para uma ampla gama de aplicações potenciais, ver: Economic Commission for Latin America and the Caribbean (ECLAC), *Data, algorithms and policies: redefining the digital world (LC/CMSI.6/4)*, Santiago, 2018.

311 D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World*, 2016.

312 C. Kuner and others, “Blockchain versus data protection”, *International Data Privacy Law*, vol. 8, No. 2, Mai 2018, pp. 103-104. Disponível em: <<https://academic.oup.com/idpl/article/8/2/103/5047578>>. Acesso em: 09 mai 2021.

A interoperabilidade tende a ser um dos problemas mais difíceis. Sem padrões técnicos comuns claros, o ecossistema pode se tornar fragmentado e os benefícios do *blockchain* são limitados. Assim, a padronização é essencial para melhorar a competitividade e aumentar os níveis globais de conformidade com outras regras e valores, como a proteção dos direitos humanos e a privacidade já referida.³¹³

Até agora, a liderança no desenvolvimento de padrões globais foi assumida pela Organização Internacional de Normalização (ISO)³¹⁴ e pela União Internacional de Telecomunicações (UIT).³¹⁵ A região da América Latina e do Caribe ainda precisa fazer um esforço coordenado para participar em fóruns globais de configuração de padrões ou para estabelecer seus próprios padrões regionais.

No entanto, existem algumas iniciativas nacionais que visam regular o *blockchain*. A tendência é se concentrar nos aspectos financeiros da tecnologia, particularmente criptomoedas. Bermudas emitiu uma regulação específica que inclui criptomoedas e visa se tornar um *hub* internacional para negociar aquilo que é definido como “ativos digitais”, inclusive, entre outros, os ativos baseados em *blockchain*.³¹⁶ Na Colômbia, o parlamento está discutindo um projeto de lei específico sobre ativos criptográficos e moedas virtuais.³¹⁷

Uma abordagem ligeiramente diferente é adotada pela Lei de Fintech do México, por exemplo, que fornece um conjunto de

313 Anna-Maria Osula, "The Global Rush for Standards in the Blockchain", abril de 2020. Disponível em: <<https://directionsblog.eu/the-global-rush-for-standards-in-blockchain/>> Acesso em: 09 mai 2021.

314 Anna-Maria Osula, "The Global Rush for Standards in the Blockchain", abril de 2020. Disponível em: <<https://directionsblog.eu/the-global-rush-for-standards-in-blockchain/>> Acesso em: 09 mai 2021.

315 International Telecommunication Union (ITU), "Focus Group on Application of Distributed Ledger Technology". Disponível em: <<https://www.itu.int/en/ITU-T/focusgroups/dlt/Pages/default.aspx>>. Acesso em: 09 mai 2021.

316 Ver: <<http://www.bermudalaws.bm/laws/Annual%20Laws/2018/Acts/Digital%20Asset%20Business%20Act%202018.pdf>>. Acesso em: 09 mai 2021. Para as regulações introduzidas pela Autoridade Monetária das Bermudas, ver: <<https://www.bma.bm/document-centre/policy-and-guidance-digital-asset-business>>. Acesso em: 09 mai 2021.

317 Ver: <<http://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2018%20-%202019/PL%20028-18%20Criptomonedas.pdf>>. Acesso em: 09 mai 2021.

regras para lidar com “ativos virtuais”.³¹⁸ O governo do Chile está seguindo um caminho semelhante, propondo regular as aplicações financeiras de *blockchain* no contexto das regulações das tecnologias financeiras.³¹⁹ A Argentina, como um dos principais centros regionais para negociação de criptomoedas, está explorando uma série de opções regulatórias, inclusive, regulações específicas das tecnologias financeiras.³²⁰

Alguns governos têm procurado usar regulamentos administrativos emitidos por bancos centrais e outras agências de supervisão financeira para fornecer diretrizes sobre ativos criptográficos.³²¹

Com relação à tributação, diferentes países procuraram interpretar sua legislação atual para incluir criptomoedas e conter o potencial de fraude financeira.³²² Ainda existem vastas áreas onde a América Latina e o Caribe podem projetar uma iniciativa coordenada e cooperativa.

As discussões futuras devem distinguir claramente entre criptomoedas e *blockchain* como uma tecnologia genérica com muitas aplicações potenciais diversas.

-
- 318 Ley para regular las instituciones de tecnología financiera, Março 2018. Disponível em: <<https://perma.cc/SB6N-RQY7>>. Acesso em: 09 mai 2021. Para uma visão positiva da aplicação do blockchain no México, ver: Y. Martínez, "Compartimos los avances y retos de la estrategia digital en el Foro OCDE México 2018", Governo do México, 2018. Disponível em: <<https://www.gob.mx/mexicodigital/articulos/compartimos-los-avances-y-retos-de-la-estrategia-digital-en-el-foro-ocde-mexico-2018>> Acesso em: 09 mai 2021.
- 319 Ver: <<https://www.criptonoticias.com/gobierno/regulacion/gobierno-chileno-adelanta-proyecto-regulacion-criptoactivos-2019/>>. Acesso em: 09 mai 2021.
- 320 Ver: <<https://www.ambito.com/politica/criptomonedas/senado-analiza-regular-el-uso-las-laargentina-n5066872>>. Acesso em: 09 mai 2021.
- 321 O Brasil é um exemplo e Costa Rica outro. Ver: Banco Central do Brasil, Comunicado, nº 31.379, 16 Novembro 2017. Disponível em: <<https://perma.cc/G4GM-8HV6>>. Acesso em: 09 mai 2021; Banco Central da Costa Rica, Posición del Banco Central de Costa Rica (BCCR) y sus Organos de Desconcentración Máxima (ODM) con respecto a las criptomonedas, Out 2017. Disponível em: <<https://perma.cc/KD4P-WXX8>>. Acesso em: 09 mai 2021.
- 322 International Monetary Fund (IMF), "Fintech in Latin America and the Caribbean: Stocktaking", 2019. Disponível em: <<https://www.imf.org/en/Publications/WP/Issues/2019/03/26/Fintech-in-Latin-America-and-the-Caribbean-Stocktaking-46677>>. Acesso em: 09 mai 2021.

CASOS E INICIATIVAS REGIONAIS DIGNOS DE NOTA

O projeto do Banco Central do Caribe Oriental (ECCB) desenvolveu um programa-piloto para facilitar a conformidade com as regulações internacionais de lavagem de dinheiro e financiamento de terrorismo e desenvolveu uma "moeda baseada em *blockchain*", disponível para vários Estados em todo o Caribe.³²³

Em 2018, a República Bolivariana da Venezuela anunciou um plano de lançamento de uma moeda criptográfica com lastro em petróleo, chamada "petro". O plano era de emitir 100 milhões de *petro-tokens* no valor de US\$ 6 bilhões com a intenção de facilitar as transações internacionais, reduzindo a dependência de moedas como o dólar e o euro.³²⁴

O Banco Interamericano de Desenvolvimento (BID) lançou o LACChain, uma aliança global para promover o uso do *blockchain* na América Latina e no Caribe, com o objetivo de coordenar esforços e desenvolver tecnologia *blockchain* na região. A aliança já identificou a falta de coordenação e padronização como um dos principais obstáculos que impedem o desenvolvimento do ecossistema de *blockchain* na América Latina e no Caribe.

6. FLUXOS INTERNACIONAIS E REGIONAIS DE DADOS: REGIMES DE PROTEÇÃO DE DADOS

A privacidade dos dados (ou proteção de dados) ganhou impulso na América Latina e no Caribe na última meia década. Alguns fatores pesaram muito para isso. O mais notável é o impacto que o Regulamento Geral de Proteção de Dados da UE (GDPR) tem tido sobre a ordem jurídica transnacional. Isso levou muitos países a rever ou desenvolver a sua própria legislação em matéria de proteção de dados. O potencial acesso (ou a falta dele) ao mercado de dados europeu é importante para muitos países, enquanto a UE é considerada um modelo regulatório para os esforços internos.

Outro evento importante foi o escândalo da Cambridge Analytica. A empresa sediada no Reino Unido traçou o perfil do eleitorado, a fim de fornecer serviços de consultoria eleitoral, procurando inferir quem votaria em cada partido e influenciar os pontos de vista dos indecisos, supostamente

323 Ver: <<https://www.eccb-centralbank.org/news/view/eccb-to-issue-worlds-first-blockchain-based-digital-currency>>. Acesso em: 09 mai 2021.

324 Ver: <<https://www.washingtonpost.com/news/worldviews/wp/2018/02/20/venezuela-launches-the-petro-its-cryptocurrency/>>. Acesso em: 09 mai 2021.

bombardeando-os com opiniões unilaterais e/ou desinformação no processo. A vista disso, países de todo o mundo decidiram ser prudente ter em vigor leis de proteção de dados fortes o suficiente para desencorajar esse comportamento e proteger o processo democrático.

Além disso, a digitalização de muitos aspectos diferentes da sociedade, incluindo os serviços públicos e as violações cibernéticas decorrentes, criaram uma maior consciência da questão na população. As pessoas sabem que seus dados pessoais estão sendo coletados e podem ficar disponíveis para que qualquer pessoa possa ver se há uma violação.

6.1. As regulações de proteção de dados têm se desenvolvido fortemente nos países da América Latina e do Caribe

A região tem visto um aumento nas iniciativas regulatórias que lidam com a proteção de dados. Em 2012, de acordo com um estudo realizado pela Organização dos Estados Americanos, 24 países da região não possuíam legislação de proteção de dados ou possuíam instrumentos domésticos que abrangiam apenas setores específicos, deixando muitos aspectos dos dados pessoais desprotegidos por qualquer instrumento jurídico em particular.³²⁵

Hoje, 16 países têm uma regulação específica de proteção de dados (Antígua e Barbuda, Argentina, Bahamas, Brasil, Chile, Colômbia, Costa Rica, República Dominicana, México, Nicarágua, Panamá, Peru, São Cristóvão e Nevis, Santa Lúcia, Trinidad e Tobago e Uruguai), seis países estão discutindo um projeto de lei (Barbados, Equador, Guatemala, Honduras, Jamaica e Paraguai) e 11 países não possuem regulações específicas de proteção de dados (Belize, República Bolivariana da Venezuela, Cuba, Dominica, El Salvador, Granada, Guiana, Haiti, Estado Plurinacional da Bolívia, São Vicente e Granadinas e Suriname).

No entanto, dos 10 países que não dispõem de uma regulação geral de proteção de dados, a maioria tomou medidas no sentido de proteger os dados pessoais em algum nível. Dominica,

325 Organization of American States (OAS), "Comparative study: data protection in the Americas. Different existing legal regimes, policies and enforcement mechanisms for the protection of personal data, including domestic legislation, regulation, and self-regulation", 2012, p. 8. Disponível em: <http://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12_en.pdf>. Acesso em: 09 mai 2021.

Granada e São Vicente e Granadinas são partes da Organização dos Estados do Caribe Oriental (OECS), que aprovou o projeto de lei de proteção de dados como parte de seu projeto de governo eletrônico para integração regional.³²⁶ Belize, Guiana, Haiti e Suriname, como membros da Comunidade do Caribe (CARI-COM), também participaram de iniciativas relacionadas com a proteção de dados: o projeto Harmonização das Políticas, Legislação e Procedimentos Regulatórios no Caribe (HIPPAR) oferece uma série de dados de modelo políticas de proteção que servem como diretrizes regulatórias.³²⁷

Alguns pontos devem ser ressaltados. Os países que já possuem legislação geral de proteção de dados estão passando por um processo de reforma e modernização que levou à adoção de normas semelhantes ao GPDR da UE. Argentina³²⁸ e Chile³²⁹ são os principais exemplos. Barbados também está discutindo a adoção de legislação em matéria de proteção de dados inspirada na regulação europeia.³³⁰

6.2. Rumo a um marco regional para a proteção de dados?

Os entrevistados enfatizaram as disparidades institucionais na região no que diz respeito à proteção de dados pessoais. Um especialista apontou para a necessidade de coordenação regional e o estabelecimento de padrões comuns de proteção de dados pessoais verdadeiramente regionais.

-
- 326 Organisation of Eastern Caribbean States (OECS), "Data Protection Act", 2016. Disponível em: <<https://www.oecs.org/en/procurement/e-gov/data-protection-act>>. Acesso em: 09 mai 2021.
- 327 Ver: <<https://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/HIPCAR/Pages/default.aspx>>. Acesso em: 10 mai 2021.
- 328 A Argentina está introduzindo várias mudanças em suas regulações de proteção de dados, incluindo uma grande reforma em sua legislação geral de proteção de dados para torná-la mais parecida com o GDPR da UE. Ver: <<https://www.oecd-ilibrary.org/sites/5f8ec188-en/index.html?itemId=/content/component/5f8ec188-en>>. Acesso em: 10 jan 2021.
- 329 Jaime Urzúa, "Avances en el Proyecto de ley sobre protección de datos personales: Consejo para la Transparencia será la nueva Agencia de protección de datos", Set 2019. Disponível em: <<https://www.alessandri.legal/avances-en-el-proyecto-de-ley-sobre-proteccion-de-datos-personales/>>. Acesso em: 10 jan 2021.
- 330 Bartlett D. Morgan, "Barbados: a modern data protection regime", Set 2019. Disponível em: <<https://platform.dataguidance.com/opinion/barbados-modern-data-protection-regime>>. Acesso em: 10 mai 2021.

Alguns países da região, como Argentina³³¹ (2000), Uruguai³³² (2008) e México (2010), estabeleceram leis de proteção de dados na última década. Outros, como o Brasil (2018) e o Panamá³³³ (2019), concluíram o processo nos últimos anos, claramente inspirados pelo GDPR da UE.

Uma vez que as iniciativas regionais têm abordado a privacidade e a proteção de dados como uma questão importante para os esforços para promover a integração e o crescimento econômicos, espera-se que sejam envidados novos esforços para promover um diálogo regional sobre proteção de dados, conectando as experiências de países cujas leis já foram reconhecidas como adequadas de acordo com as normas da UE (como Argentina e Uruguai)³³⁴ com países que estão prestes a enfrentar os desafios da implementação de uma nova regulação de proteção de dados. O Chile está seguindo o mesmo caminho, com uma proposta de legislação que está em sintonia com grande parte da lógica do GDPR.³³⁵ O mesmo se aplica à legislação brasileira de proteção de dados, sendo que até mesmo sua topografia é inspirada pelas normas europeias.

Igualmente importante é o fato de que a proteção de dados se tornou parte da agenda de comércio digital dentro de fóruns comerciais regionais, como a Aliança do Pacífico e o MERCOSUL. O Protocolo Adicional ao Pacto da Aliança do Pacífico exige que os países partes mantenham ou adotem legislação sobre proteção de dados.³³⁶ Na agenda digital da Aliança, a abordagem adotada é que os países devem seguir os melhores padrões internacionais, adotando a máxima de proteção de dados pessoais.³³⁷

331 Ver: <https://www.oas.org/juridico/PDFs/arg_ley25326.pdf>. Acesso em: 10 mai 2021.

332 Ver: <<https://www.impo.com.uy/bases/leyes/18331-2008>>. Acesso em: 10 mai 2021.

333 Ver: <https://www.sucrelaw.com/blog/media/2019/04/Ley-81-de-2019_Sobre-Proteccion-de-Datos.pdf>/ Acesso em: 10 mai 2021.

334 Ver: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 10 mai 2021.

335 Ver: <<https://www.senado.cl/appsenado/index.php?mo=transparencia&ac=doct oInformeAsesoría&id=7045>>. Acesso em: 10 mai 2021.

336 Ver: <http://www.sice.oas.org/Trade/PAC_ALL/Pacific_Alliance_Text_s.asp#c13_a13_8>. Acesso em: 10 mai 2021.

337 Ver: <<https://alianzapacifico.net/wp-content/uploads/Hoja-de-Ruta-SGAD2016-2017.pdf>>. Acesso em: 10 mai 2021.

No plano de ação conjunto entre o MERCOSUL e a Aliança do Pacífico, os países declararam sua intenção de trabalhar em conjunto para encontrar uma base comum sobre a regulação de dados pessoais. Eles consideram o assunto como um importante passo político no caminho para a criação de um mercado digital comum.³³⁸ Propostas para o MERCOSUL estão sendo desenvolvidas e parecem ser uma opção oportuna.³³⁹

6.3. Restrições à privacidade dos dados em transferências transfronteiriças de dados

As transferências transfronteiriças de dados ocorrem diariamente em uma vasta gama de situações, desde simples contratos de comércio eletrônico até transações internacionais complexas. Tais transferências são frequentemente confundidas com mercados regionais ou zonas de comércio, mas os dados pessoais atravessam fronteiras mesmo sem tais acordos comerciais internacionais.

A região da América Latina e Caribe, como um grande consumidor de serviços digitais, está continuamente tendo que lidar com serviços transnacionais que operam na região e, em muitos casos, exportando dados para seus servidores no exterior. Esse tem sido um tema importante de discussões em relação a muitas áreas, particularmente serviços em nuvem, e tem motivado propostas para impor a localização de certas categorias de dados dentro do território nacional de cada país (ver seção V.B.4 para mais discussões sobre a localização de dados).

Os fluxos transnacionais, no entanto, não são restritos apenas por estratégias de localização de dados. A legislação de proteção de dados destinada a garantir padrões fortes de proteção de dados para os cidadãos também pode criar mecanismos que indiretamente impactam ou dificultam o fluxo de dados fora das fronteiras dos países. As regulações sobre transferências internacionais de dados pessoais inspiradas nas regulações europeias (primeiro, na Diretiva 95/46/CE da UE e agora, no GDPR) surgiram em

338 Ver: <<http://www.cartillaciudadania.mercosur.int/oldAssets/uploads/Plan%20de%20Acci%C3%B3n%20-%20Anexo%20declaraci%C3%B3n%20Puerto%20Vallarta.pdf>>. Acesso em: 10 mai 2021.

339 Inter-American Development Bank (IDB), "Fueling Digital Trade in MERCOSUR: A Regulatory Roadmap", 2018. Disponível em: <<https://publications.iadb.org/publications/english/document/Fueling-Digital-Trade-in-Mercosur-A-Regulatory-Roadmap.pdf>>. Acesso em: 10 mai 2021.

muitos países da região. A Colômbia, por exemplo, estabeleceu uma lista de países que cumpriram as normas de transferência de dados com os quais, sob certas circunstâncias, os dados podem fluir livremente; para todos os outros países, há um procedimento elaborado que normalmente inclui cláusulas contratuais padrão fortes.³⁴⁰ Da mesma forma, a legislação na Argentina, Bahamas, Brasil, Colômbia, Costa Rica, República Dominicana, México, Nicarágua, Panamá, Peru, Santa Lúcia, Trinidad e Tobago e Uruguai têm disposições que restringem as transferências internacionais.

Dos países mencionados, Argentina e Uruguai se destacam por terem sido reconhecidos pela UE como países aprovados para a transferência de dados pessoais. Assim, as restrições unilaterais entre esses dois países e a UE foram suspensas em ambos os sentidos, garantindo que os dados pessoais possam fluir entre cada um dos dois e qualquer dos países da UE.³⁴¹

7. FLUXOS TRANSFRONTEIRIÇOS DE DADOS INTERNACIONAIS E REGIONAIS

7.1. Os fluxos de dados internacionais e regionais são a pedra angular do comércio digital

Os fluxos internacionais de dados recentemente cresceram significativamente em importância.³⁴² O crescente comércio internacional de serviços, principalmente nos setores em que a prestação era exclusivamente doméstica, como educação, cuidados de saúde e bancos, e tecnologias intensivas de dados da Internet das Coisas e da Inteligência Artificial, entre outros,

340 Internet & Jurisdiction Policy Network, "Colombia establishes list of countries with adequate data protection for cross-border transfers", I&J Retrospect Database, Jul 2017. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6188_2017-07>. Acesso em: 10 mai 2021.

341 Para uma lista completa dos países cujas proteções são consideradas adequadas pela UE, Ver: <https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en>. Acesso em: 10 mai 2021.

342 De acordo com um estudo realizado pela McKinsey, os fluxos de dados transfronteiriços têm um impacto mais significativo na economia global do que o comércio de bens. McKinsey Global Institute, Digital globalization: The new era of global flows, 2016. Disponível em: <<https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows>>. Acesso em: 10 mai 2021.

trouxeram uma nova urgência aos esforços para determinar padrões de proteção de dados.³⁴³ São grandes as potenciais implicações econômicas transfronteiriças. Assim, as questões envolvendo dados pessoais estão se tornando cada vez mais importantes na agenda do comércio internacional.

Uma vez que organizações internacionais como a Organização Mundial do Comércio (OMC) e a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) ainda não encontraram uma base estabelecida para resolver questões de comércio eletrônico, comércio digital, proteção de dados e fluxos de dados transfronteiriços,³⁴⁴ acordos comerciais regionais e bilaterais começaram a definir suas próprias normas. Na América Latina e no Caribe, vários países são partes em acordos comerciais (bilaterais ou não), contendo cláusulas específicas sobre tais assuntos.

Um dos primeiros acordos a conter uma disposição sobre comércio eletrônico foi o Acordo de Parceria Econômica (APE) dos Estados da África, Caribe e Pacífico do Fórum União Europeia – Caribe, que entrou em vigor em 2008 e envolveu Antígua e Barbuda, Bahamas, Barbados, Belize, Dominica, República, Granada, Guiana, Jamaica, Santa Lúcia, São Vicente e Granadinas, São Cristóvão e Neves, Suriname e Trindade e Tobago.³⁴⁵ Países como Belize, Colômbia, Costa Rica, El Salvador, Guatemala, Honduras, México, Nicarágua, Panamá e Peru também celebraram acordos contendo cláusulas de comércio eletrônico com Estados fora da região. Intra-regionalmente, há também casos como os acordos celebrados pela Colômbia com os países

343 Ver: <<https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/>>. Acesso em: 10 mai 2021.

344 Ver, por exemplo, a discussão da OCDE sobre a abertura da Internet e os fluxos de dados, o debate do Fórum Econômico Mundial sobre a governança internacional do fluxo de dados, a proposta do G20 Japão para o livre fluxo de dados com confiança, representando um potencial acordo internacional sobre fluxos de dados transfronteiriços, ou a controvérsia da OMC em relação ao comércio eletrônico. Ver: <https://www.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en;jsessionid=dFRe-gxHPx7Res_noe9wGNEb.ip-10-240-5-18>; <http://www3.weforum.org/docs/WEF_Trade_Policy_Data_Flows_Report.pdf>; <<https://pecc.org/resources/digital-economy/2616-data-free-flow-with-trust-and-data-governance/file>>; e <https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm>. Acessos em: 10 mai 2021.

345 O Haiti assinou o tratado, mas ainda não o ratificou. Ver: <<https://ec.europa.eu/trade/policy/countries-and-regions/regions/caribbean/>>. Acesso em: 10 mai 2021.

do Triângulo Norte da América Central (El Salvador, Guatemala e Honduras), com a Costa Rica e com o Peru; os celebrados pelo México com a América Central e o Panamá; e os acordos entre Chile e Uruguai. O escopo e conteúdo dos acordos variam, mas eles tendem a estabelecer políticas sobre uma ampla gama de questões, desde a proteção do consumidor on-line até a proteção dos direitos de propriedade intelectual no ciberespaço.³⁴⁶

No entanto, nem todos os acordos contêm cláusulas de proteção de dados. O acordo de Parceria Trans-Pacífico (TPP), que inclui três países da região (Chile, México e Peru), é um dos que contém essas cláusulas. Seu capítulo de comércio eletrônico trata de uma série de aspectos importantes, como privacidade e proteção de dados, fluxos de dados transfronteiriços e localização de dados. Reconhece os benefícios da legislação de proteção de dados e exige que os países membros mantenham ou adotem uma “estrutura legal” para proteger “informações pessoais”. O conteúdo de tal estrutura está em aberto: cada país pode decidir como exatamente os dados pessoais devem ser regulados. Uma disposição importante, no entanto, reconhece a necessidade de criar mecanismos para “promover a compatibilidade entre esses regimes [potencialmente] diferentes”.³⁴⁷

O Acordo dos Estados Unidos, México e Canadá (USMCA) é outro exemplo. O capítulo do comércio digital, o primeiro de seu tipo, segue muito a mesma estratégia da Parceria Trans-Pacífico (TPP), muito mais ampla, negociada anteriormente.³⁴⁸ Há disposições que exigem que cada Estado estabeleça leis para proteger os dados pessoais (“informações pessoais”, nos termos do acordo). O tratado não estabelece, no entanto, um padrão comum mínimo que deve ser seguido, mas apenas afirma que, ao regular “informações pessoais”, “cada Parte deve

346 Inter-American Development Bank (IDB)/International Centre for Trade and Sustainable Development (ICTSD), Digital Trade-Related Provisions in Regional Trade Agreements: Existing Models and Lessons for the Multilateral Trade System, 2017. Disponível em: <<https://www.ictsd.org/themes/global-economic-governance/research/digital-trade-related-provisions-in-regional-trade>>. Acesso em: 10 mai 2021.

347 Trans-Pacific Partnership (TPP), art. 14(8)(5). Ver: <<https://www.mfat.govt.nz/assets/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf>>. Acesso em: 10 mai 2021.

348 Ver: <<https://www.cfr.org/blog/coming-north-american-digital-trade-zone>>. Acesso em: 10 mai 2021.

levar em conta os princípios e diretrizes dos órgãos internacionais relevantes”.³⁴⁹

Quanto mais bens e serviços conectados (particularmente bens com serviços de informação incorporados) ganharem impulso, mais importante será ter padrões comuns de proteção de dados. Isso significa não apenas padrões aplicáveis nacionalmente, mas também que permitam que os dados fluam internacionalmente. Diferentes abordagens podem afetar o comércio internacional, tornando mais difícil para as empresas ganhar escala e operar em todos os mercados. Regulações divergentes de proteção de dados tornam necessário adaptar bens e serviços para atender aos requisitos regulatórios de cada mercado específico. Da mesma forma, as restrições aos fluxos transfronteiriços têm um impacto nas ofertas transfronteiriças de bens e serviços. Tomando o exemplo da IoT, no primeiro caso, as configurações de arquitetura e privacidade têm que ser adaptadas antes que o dispositivo possa ser oferecido em um determinado país. No segundo, a infraestrutura usada para fornecer o serviço subjacente que requer os dados pode se tornar muito mais complexa, com o fluxo de dados sendo confinado dentro das fronteiras do país ou procedimentos para permitir a transferência internacional de dados tendo que ser resolvidos com antecedência. Esses procedimentos podem afetar a concorrência entre empresas nacionais e estrangeiras, levantando potencialmente questões de discriminação arbitrária ou injustificável. Assim, dois tipos de iniciativas são importantes: harmonização das normas de proteção de dados e facilitação de fluxos de dados internacionais responsáveis e seguros.

7.2.Regionalização: desafios e oportunidades transfronteiriças

Várias das recentes iniciativas comerciais em que a América Latina e o Caribe estão envolvidos tomaram providências para fluxos de dados transfronteiriços. Elas reconhecem que leis diferentes podem proporcionar diferentes oportunidades

349 Acordo entre Estados Unidos-México-Canadá, art. 19 (8), 30 de novembro de 2018. Ver: <<https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>>. Acesso em: 10 mai 2021.

e condições para fluxos de dados internacionais. As iniciativas procuram fornecer um quadro que facilite os fluxos, estabelecendo as condições que devem ser cumpridas e/ou o escopo do assunto para o qual os fluxos de dados pessoais são permitidos.

O artigo 14(11)(2) da Parceria Trans-Pacífico (TPP) estabelece que os fluxos de dados transfronteiriços devem ser permitidos sempre que o fluxo “seja para a condução dos negócios de uma pessoa abrangida [pela parceria]”. O artigo 19.11 da USMCA impõe a mesma obrigação. Ambos acrescentam linguagem semelhante à dos tratados internacionais, como o artigo XX do Acordo Geral sobre Tarifas e Comércio (GATT) e o artigo XIV do Acordo Geral sobre Comércio de Serviços (GATS), permitindo aos países regular por “um objetivo legítimo de política pública”.

A cláusula que trata dos serviços financeiros no Acordo de Parceria Econômica entre os Estados do CARIFORUM e a UE (artigo 107) estabelece de forma semelhante que os países devem permitir o fluxo de dados para a condução desse tipo de negócio (serviços financeiros). O tratado acrescenta uma cláusula mais específica que afirma que as partes adotarão salvaguardas adequadas para proteger a privacidade, os direitos fundamentais e a liberdade pessoal dos titulares dos dados, que devem incluir a proteção de dados e a privacidade.

No caso do Acordo Comercial UE-México atualmente em negociação, o capítulo do comércio digital não especifica qualquer regime para os fluxos de dados transfronteiriços, mas inclui uma “cláusula *rendez-vous*” que prevê um período de três anos para avaliar se é necessário incluir “disposições sobre o livre fluxo de dados”.³⁵⁰

Alguns acordos comerciais bilaterais da região têm cláusulas que tratam de fluxos de dados bilaterais. O artigo 14(10) do Acordo de Livre Comércio México-Panamá estabelece que os dados podem atravessar fronteiras, com a ressalva de que isso deve estar de acordo com as exigências de proteção de dados pessoais e práticas internacionais. Outros apenas enfatizam

350 Svetlana Yakovleva and Kristina Irion, “Pitching trade against privacy: reconciling EU governance of personal data flows with external trade”, *International Data Privacy Law*, 30 Mar 2020. Disponível em: <<https://doi.org/10.1093/idpl/ipaa003>>. Acesso em: 10 mai 2021. Para o texto do acordo negociado, ver: <http://trade.ec.europa.eu/doclib/docs/2018/april/tradoc_156811.pdf>

a necessidade de cooperação para facilitar e manter os fluxos de dados, sendo exemplos o Acordo de Livre Comércio Costa Rica-Colômbia, o Acordo de Livre Comércio Chile-Colômbia e o Acordo de Livre Comércio Colômbia-Triângulo Norte.

Essas disposições fornecem a base para compreensões comuns sobre a forma como os dados podem fluir para além das fronteiras. As tensões potenciais entre regimes e restrições aos fluxos de dados são limitadas pelos acordos e os fluxos internacionais tendem a ser priorizados. Ainda não existe um acordo geral ou regional que envolva países da América Latina e do Caribe. Tal acordo provavelmente traria maior segurança ao fluxo de dados e reforçaria o comércio, particularmente na economia digital.

7.3. Iniciativas regionais estão promovendo a padronização das transferências de dados transfronteiriças

Nos níveis internacional e regional, não há acordos gerais que tratem da proteção da reputação de uma pessoa ou que permitam (ou impeçam) o livre fluxo de dados. No entanto, algumas organizações regionais emitiram princípios orientadores destinados a harmonizar as normas dos diferentes países.

O décimo primeiro dos Princípios da OEA sobre Privacidade e Proteção de Dados Pessoais, “Fluxo Transfronteiriço de Dados e Responsabilização”, reconhece a necessidade de harmonização das normas de proteção de dados, a fim de não dificultar o fluxo de dados através das fronteiras.³⁵¹

As normas de proteção aprovadas pela Rede Ibero-Americana de Proteção de Dados, da qual vários dos países da região são partes, também contém uma recomendação de que as transferências transfronteiriças de dados sejam sujeitas a uma série de requisitos que seguem padrões semelhantes aos da legislação europeia, indicando que ambos os países devem ter proteção considerada adequada ou as partes que desejam transferir dados para o estrangeiro devem seguir procedimentos pré-estabelecidos.³⁵²

351 Ver: <<http://scm.oas.org/pdfs/2016/CP35451EREPORTCJL.pdf>>. Acesso em: 10 mai 2021.

352 Ver: <https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf>. Acesso em: 10 mai 2021.





03 .

Principais abordagens para os dilemas transfronteiriços da Internet na América Latina e no Caribe

O Relatório de Status Global 2019 argumentou que não era exagerado dizer que uma corrida legal armamentista estava em curso entre muitos dos principais atores internacionais, principalmente os Estados Unidos, a União Europeia, a China e, até certo ponto, a Rússia. Como observado anteriormente, suas medidas afetam diretamente a região. Muitos Estados da América Latina e do Caribe estão adotando e implementando soluções técnicas e legais dentro de suas jurisdições internas que se assemelham ou são inspiradas nas soluções normativas e técnicas adotadas por outros atores internacionais.

Assim, as iniciativas na América Latina e no Caribe espelham em grande parte as propostas advindas de outros lugares. Elas incluem legislação nacional com ampla aplicação extraterritorial, ordens judiciais locais com implicações globais, multas e sanções para empresas sem presença física no país e filtragem obrigatória de conteúdo, localização de dados e bloqueio de aplicativos. Na aplicação real, no entanto, elas tendem a adquirir uma tonalidade regional à medida que as soluções são transferidas de um contexto para outro totalmente diferente.

Como mencionado no capítulo II, as peculiaridades sociais, econômicas, políticas e jurídicas têm o efeito de mudar a forma como as soluções técnicas são implantadas em diferentes países. Em uma região tão diversificada como a América Latina e o Caribe, todas essas condições desempenham um papel importante na determinação do sucesso de soluções jurídicas e técnicas para dilemas transfronteiriços.

Entretanto, essas soluções jurídicas e técnicas foram, em sua maioria, implementadas sem uma discussão adequada de seus efeitos transfronteiriços. Assim, esta parte do Relatório se propõe a analisar uma seleção de tais iniciativas e lançar luz sobre seus impactos transfronteiriços.

A. Principais tendências jurídicas

Os Estados da América Latina e do Caribe variam no grau em que empregam soluções legais para as questões percebidas relacionadas à regulação da Internet. De um modo geral, existe uma tendência crescente no sentido de alargar a aplicação das legislações nacionais a situações além das fronteiras físicas dos países. Está se tornando cada vez mais habitual determinar a competência jurisdicional de um tribunal com base no que é

chamado de “doutrina dos efeitos” ou um “teste de direcionamento” (*targeting test*). Os tribunais emitem ordens de remoção (e/ou suspensão) e ordens de permanência de conteúdo on-line. Há também uma ênfase em acoplar a regulação aplicável à Internet a grandes multas e sanções. Termos de serviço e diretrizes de comunidade criadas pelas principais plataformas internacionais da Internet estão desempenhando um papel cada vez mais importante e fundamental na orientação do comportamento on-line.

1. OS ESTADOS ESTÃO CADA VEZ MAIS RECORRENDO A UMA “DOUTRINA DOS EFEITOS” NA AFIRMAÇÃO DE SUA JURISDIÇÃO

Há uma ampla tendência para os Estados afirmarem jurisdição sobre condutas e atividades cuja origem reside noutro Estado ou território sempre que eles têm uma ligação substancial com o país, afirmando, assim, jurisdição. As atividades geralmente entendidas para criar tal conexão incluem segmentar consumidores, fazer negócios, causar danos ou afetar de forma concreta pessoas ou ativos localizados dentro das fronteiras de um país.

De acordo com o direito internacional, essa abordagem é geralmente entendida como situada sob o título da “doutrina dos efeitos”. A lógica é que os Estados devem ser capazes de afirmar jurisdição sobre condutas e atividades que tenham um impacto (“efeito”) sobre pessoas ou bens em seu território. Isso se justifica tanto por intenção, porque o participante ativo sabia ou, pelo menos, deveria ter sabido que a atividade ou conduta teria consequências nesse país, quanto com base em que os Estados deveriam poder regular atividades que impactem os seus mercados, seus cidadãos ou bens no seu território.³⁵³Essa abordagem foi originalmente desenvolvida para fins de concorrência e lei antitruste, mas ganhou impulso com a propagação da Internet. Geralmente é discutida com referência a um “teste de direcionamento” (*targeting test*). Nos primeiros exemplos desta abordagem, a atenção centrou-se no estabelecimento da

353 Ver: B. Simma e A. Müller, “Exercise and limits of jurisdiction”, *The Cambridge Companion to International Law*, J. Crawford e M. Koskeniemi (eds.), Cambridge, Cambridge University Press, 2012.

competência jurisdicional com particular referência à difamação (e conteúdo nocivo) e comércio eletrônico. Em *Young versus New Haven Advocate*, um tribunal de recurso dos Estados Unidos foi instado a decidir se os tribunais de um estado tinham competência para decidir sobre um caso de difamação envolvendo um jornal (publicado on-line e off-line) destinado à distribuição em outro estado. O Tribunal decidiu que não era suficiente que estivesse disponível no segundo estado, ou que discutisse assuntos envolvendo aquele estado; o fato de o público-alvo da leitura ser direcionada ao outro estado era o ponto principal.³⁵⁴

Nos casos conjuntos de *Peter Pammer versus Reederei Karl Schlüter GmbH & Co. KG e Hotel Alpenhof GesmbH v. Oliver Heller*, o Tribunal de Justiça da União Europeia foi chamado a decidir sobre as características que determinariam a competência em casos relativos ao comércio eletrônico, quer dizer, um consumidor que compra bens e serviços on-line. O Tribunal afirmou que vários elementos deveriam ser levados em consideração, tais como a natureza internacional do serviço, itinerários de outros Estados-membros (como o local de onde a transação foi negociada), o idioma e as opções de moeda do site ou aplicativo, números de telefone com códigos internacionais prefixados a eles, nomes de domínio de primeiro nível diferentes do Estado-membro em que o comerciante estava baseado e menção de uma clientela internacional composta de clientes domiciliados em vários Estados-membros.

A decisão também tornou explícito que o simples fato de o serviço estar disponível on-line no país do consumidor não era uma conexão suficiente (isso tem um impacto no uso de tecnologias de geolocalização, como discutido abaixo).³⁵⁵ A lógica para tais decisões é que os comerciantes só devem ser regulados no nível da União Europeia se eles visarem primeiro o mercado da União Europeia. A abordagem foi replicada no considerando 23

354 Ver: United States Court of Appeals for the Fourth Circuit, *Young v. New Haven Advocate*, No. 315 F.3d 256, Richmond, 13 de dezembro de 2002.

355 Ver: Tribunal de Justiça da União Europeia, Acórdão do Tribunal (Plenário) de 7 de dezembro de 2010 (pedidos de decisão preliminar de Oberster Gerichtshof (Áustria) - Peter Pammer c. Reederei Karl Schlüter GmbH & Co KG (C-585/08) e Hotel Alpenhof GesmbH c. Oliver Heller (C-144/09), No. 2011/C 55/06, Luxemburgo, 19 de fevereiro de 2011.

do Regulamento Geral sobre a Proteção de Dados (GDPR)³⁵⁶ e informou outros processos regulatórios da União Europeia.³⁵⁷

Essa visão também teve um impacto na América Latina. Casos em diferentes países que vão da Colômbia ao Brasil estabeleceram que a jurisdição sobre as atividades da Internet deve ser determinada pelos efeitos pretendidos ou esperados das ações tomadas on-line.³⁵⁸ O ciberespaço é visto como onipresente, mas as ações e a conduta dos participantes nele são entendidas como tendo um foco, um alvo. Ao afirmar a sua jurisdição, os tribunais tendem a decidir tomando como base o local onde o dano ocorreu, considerando a aparente intenção dos atores envolvidos

No caso *Jerónimo A. Uribe*, o Supremo Tribunal de Justiça da Colômbia determinou que o conteúdo on-line, incluindo ameaças de morte, não deveria ser entendido como tendo ocorrido apenas no local onde o perpetrador estava localizado, ou

356 Regulamento Geral sobre a Proteção de Dados (GDPR), considerando 23: "A fim de determinar se o responsável pelo tratamento ou subcontratante oferece ou não bens ou serviços aos titulares dos dados que se encontrem na União, há que determinar em que medida é evidente a sua intenção de oferecer serviços a titulares de dados num ou mais Estados-Membros da União. O mero facto de estar disponível na União um sítio web do responsável pelo tratamento ou subcontratante ou de um intermediário, um endereço eletrónico ou outro tipo de contactos, ou de ser utilizada uma língua de uso corrente no país terceiro em que o referido responsável está estabelecido, não é suficiente para determinar a intenção acima referida, mas há fatores, como a utilização de uma língua ou de uma moeda de uso corrente num ou mais Estados-Membros, com a possibilidade de encomendar bens ou serviços nessa outra língua, ou a referência a clientes ou utilizadores que se encontrem na União, que podem ser reveladores de que o responsável pelo tratamento tem a intenção de oferecer bens ou serviços a titulares de dados na União". Ver: <<https://www.privacy-regulation.eu/pt/r23.htm>>. Acesso em: 10 mai 2021.

357 Comissão Europeia, Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece regras harmonizadas relativas à nomeação de representantes jurídicos para efeitos de recolha de provas em processo penal, n. COM(2018) 226 final, Strasbourg, 17 Abr 2018. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0226&from=EN>>. Acesso em: 10 mai 2021; Proposal for a regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters, No. COM(2018) 225 final, Strasbourg, 17 Abr 2018. Disponível em: <<https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52018PC0225&from=EN>>. Acesso em: 10 mai 2021.

358 Para uma visão geral sobre os casos de difamação, ver: <https://www.palermo.edu/cele/cele/pdf/english/Internet-Free-of-Censorship/Jurisdiction_Eduardo%20Bertoni.pdf>. Acesso em: 10 mai 2021.

seja, seu local habitual de residência.³⁵⁹ Do mesmo modo, no processo do *Centro Comercial Campanario*, o mesmo Supremo Tribunal decidiu que a jurisdição deveria ser atribuída ao local onde o dano ocorreu, ou seja, em caso de fraude on-line, o local onde a vítima se encontra.³⁶⁰

Seguindo um raciocínio semelhante, o Superior Tribunal de Justiça do Brasil³⁶¹ determinou, em vários casos, que a localização dos servidores é irrelevante quando se trata de determinar a jurisdição e que, em vez disso, ela deve ser atribuída ao local onde a vítima reside e trabalha, uma vez que é aí que a atividade ou o conteúdo nocivos terão o maior impacto e repercussões.³⁶²

Na Argentina, da mesma forma, várias decisões determinaram a jurisdição com base no local onde ocorreu o dano ou onde se encontra a vítima.³⁶³ Isso assume um aspecto diferente quando o suposto autor da ofensa é uma publicação de notícias que tem uma presença on-line e off-line. O raciocínio é que o local onde os “materiais são impressos” é o critério determinante. O princípio subjacente parece ser que, não obstante a presença on-line, o público-alvo é o leitor no local onde a edição impressa é distribuída.³⁶⁴

Na maioria dos casos na região, o principal critério para determinar a jurisdição é simplesmente o local onde o dano é sentido, como o local de residência ou de negócios da vítima. Essa

359 Ver: Supremo Tribunal de Justiça da Colômbia, Caso Jerónimo A. Uribe, nº 33.474/2010, Bogotá, 10 de fevereiro de 2010.

360 Ver: Supremo Tribunal de Justiça da Colômbia, Caso Centro Comercial Campanario, nº 34.564/2010, Bogotá, 25 de agosto de 2010.

361 Ver: Superior Tribunal de Justiça, Conflito de competência, nº 66.981, Brasília, 16 de fevereiro de 2009. Disponível em: <https://ww2.stj.jus.br/processo/revista/inteiroteor/?num_registro=200601611027&dt_publicacao=05/03/2009>. Acesso em: 10 mai 2021.

362 Ver: Superior Tribunal de Justiça, Conflito de competência, nº 66.981, Brasília, 16 de fevereiro de 2009; Conflito de competência, nº 107.938, Brasília, 27 de outubro de 2010; Agravo de instrumento, nº 1.375.009, Brasília, 15 de março de 2011.

363 Ver: Tribunal Federal de Recurso de Salta, J. G. R. v. Google Inc., Salta, 4 de julho de 2011; Tribunal Nacional de Recurso para Assuntos Penais e Correccionais da Cidade de Buenos Aires, NN. s/injurias, nº 1589/09, Buenos Aires, 21 de outubro de 2009.

364 Ver: Tribunal Nacional de Recursos Penais, Alifano, Roberto Francisco s/recurso de queja, nº 9375, Buenos Aires, 3 de março de 2009; Supremo Tribunal Federal de Justiça da Argentina, Verazay, Santos Justo s/querrela por calumnias e injurias, nº 1085, Buenos Aires.

abordagem direcionada também é vista em alguns textos legislativos, incluindo leis argentinas, brasileiras,³⁶⁵ colombianas,³⁶⁶ mexicanas³⁶⁷ e peruanas³⁶⁸ de proteção de dados. Outro exemplo é a Lei Especial contra o Crime Informático da Venezuela.

A principal dificuldade com essa abordagem de direcionamento é entender o perfil do alvo. O fato de um site estar disponível on-line, sem limitações geográficas, significa que ele tem como alvo o mundo inteiro, ou pelo menos que seus proprietários aceitam o risco de agir como se assim fosse? Será que uma mudança no idioma importa? Quais são os critérios precisos para determinar o público-alvo? Pode parecer relativamente fácil determinar a jurisdição no caso de um aplicativo de mensagens de ponta-a-ponta, mas o que mudaria se a mesma mensagem fosse enviada através de uma rede social aberta ao público?

O elemento controverso é a questão de saber se a jurisdição é justa para todas as partes envolvidas. Por um lado, limitar a jurisdição ao domicílio da pessoa que presta o serviço, vende seu produto ou realiza a publicação da mensagem deixaria a outra parte com muito pouco recurso. Por outro lado, se a parte potencialmente lesada receber muita proteção, o prestador de serviços, vendedor ou editor de conteúdo pode ter que se defender em tribunal de qualquer lugar do mundo sob uma lei cuja aplicação pode não ter esperado.

2. A EXPANSÃO DO ALCANCE JURISDICIONAL

Um número significativo de atores pesquisados observou que havia um desequilíbrio de poder e que, enquanto muitos países estavam implementando legislação de escopo extraterritorial,

365 Ver: <https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf>. Acesso em: 10 mai 2021.

366 Ver: Congresso da Colômbia, Ley Estatutaria 1581 de 2012, Bogotá, 2012. Disponível em: <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf>. Acesso em: 10 mai 2021.

367 Ver: Instituto Nacional de Desenvolvimento Social, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Cidade do México, 2010; Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Cidade do México, 2011; Secretaría de Economía, "Lineamientos del aviso de privacidad", Diario Oficial de la Federación, Cidade do México, 17 de janeiro de 2013.

368 Peru, Lei nº 29.733 de 2011, Lei de Proteção de Dados Pessoais.

nem todos os Estados eram capazes de executar tais leis. Alguns apontaram que regulações desse tipo poderiam ser mais eficazes se fizessem parte de acordos regionais, mas ainda é muito desafiador encontrar um terreno comum.

No contexto de uma Internet global neutra em que condutas e ações iniciadas em uma parte do mundo podem ter um impacto – e podem realmente causar danos – em outra, os países têm procurado estender seus poderes para além de seu próprio território. Eles tentaram unilateralmente fechar a lacuna internacional de governança e regulação para ações e condutas on-line, reivindicando uma jurisdição que vai além do que é tradicionalmente reconhecido como seu território, em alguns casos, independentemente de haver alguma perspectiva de execução real ou efetiva.

Um exemplo da região pode ser encontrado no artigo 11 do Marco Civil da Internet do Brasil. Afirma no caput que “[e]m qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira [...]”.³⁶⁹ O parágrafo 2 passa a abranger até “as atividades [que] sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil”.³⁷⁰

A tendência para reivindicar uma jurisdição expandida foi ainda mais reforçada pelo exemplo do artigo 3 do Regulamento Geral Europeu de Proteção de Dados (GDPR). Essa regulação teve um impacto na concepção de nova legislação nos países da América Latina e do Caribe. O Brasil, por exemplo, incluiu na sua Lei Geral de Proteção de Dados o artigo 3º, inspirado no seu homólogo europeu, afirmando que “[e]sta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado,

369 Ver: Internet & Jurisdiction Policy Network, “Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction”, Paris, 2014. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-5002_2014-04>. Acesso em: 10 mai 2021.

370 Ibidem.

independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que: I - a operação de tratamento seja realizada no território nacional; II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.” O parágrafo primeiro do artigo 3 da Lei Geral de Proteção de Dados do Brasil também estabelece que “[c]onsideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.”³⁷¹

Isso também se aplica a países como a Colômbia,³⁷² México³⁷³ e o Peru,³⁷⁴ que também estenderam suas regulações de proteção de dados para dar-lhes uma dimensão extraterritorial. Do ponto de vista de uma nação em desenvolvimento, essa abordagem pode ser vista como uma demonstração de força contra empresas estrangeiras com potencial para impactar os mercados domésticos de longe, especialmente quando as regulações são associadas a multas e sanções pesadas (discutido na seção V.A.4 abaixo). Parece haver aceitação internacional disso quando o que está sendo protegido são os direitos e valores fundamentais do país que aprova a lei.

No entanto, qualquer reivindicação jurisdicional, quer se trate de jurisdição prescritiva ou competência jurisdicional de um tribunal, “vive ou morre” pela possibilidade de ser executada. Quando falta a capacidade de realmente obrigar as partes ao cumprimento, a legitimidade da regulação pode ser diminuída. Essa abordagem também foi criticada por: (i) levar a uma aplicação arbitrária (demasiados sujeitos potencialmente não

371 Ver: <https://iapp.org/media/pdf/resource_center/Brazilian_General_Data_Protection_Law.pdf>. Acesso em: 10 mai 2021.

372 Colômbia, Lei nº 1581 de 2012. Ver: <https://www.defensoria.gov.co/public/Normograma%202013_html/Normas/Ley_1581_2012.pdf>. Acesso em: 10 mai 2021.

373 Ver: Instituto Nacional de Desenvolvimento Social, Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Cidade do México, 2010; Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, Cidade do México, 2011; Secretaría de Economía, “Lineamientos del aviso de privacidad”, Diario Oficial de la Federación, Cidade do México, 17 de janeiro de 2013.

374 Peru, Lei nº 29.733 de 2011, Lei de Proteção de Dados Pessoais.

conformes, fazendo com que as autoridades tenham de escolher quais perseguir); (ii) erosão da segurança jurídica (demasiados infratores não processados, dando a impressão de que a lei é letra morta); e (iii) criar potenciais conflitos de conformidade transfronteiriça (as normas de dois ou mais países podem exigir medidas diferentes para serem tomadas em relação à mesma conduta, levando a conflitos e obrigando os entes a escolher qual lei cumprir).

Um dos entrevistados mencionou que os tribunais superiores da América Latina tinham até agora mostrado contenção e não emitiram ordens com alcance global em questões relacionadas à Internet. Outro foi de opinião de que o escopo global potencial dos direitos individuais on-line ainda não havia sido determinado em muitos países da região.

A discussão vai além de se os tribunais têm jurisdição sobre determinadas pessoas ou tipos de assunto ou se a legislação se aplica a uma situação que pode ser entendida como estando fora do que é tradicionalmente entendido como território de um país. O que está em questão é o escopo dos efeitos da jurisdição: o escopo da jurisdição reparativa (*remedial jurisdiction*).³⁷⁵

O Ministro Alexandre de Moraes, do Supremo Tribunal Federal do Brasil, ordenou que as redes sociais Facebook e Twitter bloqueassem o acesso às contas de 16 indivíduos que estavam sendo investigados por supostamente propagarem desinformação e discurso de ódio on-line.³⁷⁶ O magistrado teria solicitado um bloqueio de alcance global (acesso seria bloqueado independentemente da origem do endereço IP do usuário) com base em um relatório policial que afirmava terem havido incidentes em que aqueles sob investigação tinham contornado a restrição imposta pela ordem anterior e continuaram a usar suas contas para publicar mensagens em descumprimento à atual ordem judicial, particularmente discurso de ódio.

375 Ver: D. Jerker, "Jurisdiction in 3D - 'scope of (remedial) jurisdiction' as a third dimension of jurisdictions", *Journal of Private International Law*, vol. 12, No. 1, Milton Park, Taylor & Francis, 2016.

376 Ver: <<https://www.reuters.com/article/us-facebook-brazil/facebook-puts-global-block-on-brazils-bolsonaro-supporters-idUSKCN24X3BN>>. Acesso em; 10 mai 2021.

O evento teve uma maior repercussão, já que um dos 16 que tiveram suas contas bloqueadas globalmente foi capaz de usar outra conta para fazer uma declaração muito controversa contra o aborto. O comentário não só expressou opiniões sobre o assunto, mas também incluiu dados pessoais sobre uma menina de 10 anos que havia sido estuprada e que estava passando por um procedimento legal em um hospital. Outro juiz instruiu as mesmas redes sociais e o Google a remover as mensagens contendo as informações pessoais da menor.³⁷⁷ Um membro do congresso pediu que este incidente fosse acrescentado às investigações que levaram à ordem global emitida pelo Juiz Moraes, do Supremo Tribunal Federal.³⁷⁸

Os casos relativos ao chamado “direito ao esquecimento” têm tratado dos limites (escopo) da remoção ou desindexação da lista do buscador on-line em que a informação aparece, ou seja, discutem se é suficiente que a remoção ocorra no território do país (ou da Europa) ou deve ser global. O bloqueio geográfico (discutido na seção V.B.1 abaixo) está sendo considerado e tratado em termos de eficácia e precisão da técnica.³⁷⁹

A discussão sobre direitos de propriedade intelectual também avançou. A lógica é que existe um elevado grau de harmonização internacional nesse domínio (particularmente do direito autoral). Assim, uma ordem de um tribunal de um país pode ter um impacto global, a menos que se prove que regulações noutro país obrigam a plataforma a agir de forma diferente.³⁸⁰

A Rede de Políticas Internet & Jurisdição divulgou recentemente uma publicação que fornece orientações para governos e entidades privadas sobre como lidar com o escopo geográfico

377 Ver: <<https://www.bbc.com/news/world-latin-america-53820497>>. Acesso em: 10 mai 2021.

378 Ver: <<https://revistaforum.com.br/politica/alexandre-padilha-aciona-stf-contrasara-winter-por-incitar-fundamentalistas-contramenina-de-10-anos/>>. Acesso em: 10 mai 2021.

379 Ver: Court of Justice of the European Union, Google LLC, successor in law to Google Inc. v. Commission nationale de l'informatique et des libertés (CNIL), No. C-507-17, Luxembourg, 24 de setembro de 2019. Disponível em: <<http://curia.europa.eu/juris/liste.jsf?language=en&num=C-507/17>>. Acesso em: 10 mai 2021; Eva Glawischnig-Piesczek v. Facebook Ireland Limited, No. C-18/18, Luxemburgo, 3 de outubro de 2019. Disponível em: <<http://curia.europa.eu/juris/liste.jsf?num=C-18/18>>. Acesso em: 10 mai 2021.

380 Ver: Supremo Tribunal do Canadá, Google Inc. v. Equustek Solutions Inc., No. SCC 34, Out, 2017.

das restrições de conteúdo. Identifica quatro categorias de “coerência normativa internacional”, refletindo o grau de convergência entre diferentes partes da legislação relativa à ilegalidade de conteúdo. Essas categorias devem fornecer a base para uma escala com diferentes níveis de alcance geográfico para a remoção de conteúdo, desde os mais proporcionais e limitados aos mais globais.³⁸¹

Na região, a tendência de impor ordens globais de desindexação ainda não ganhou muita força. Isso não quer dizer que não tenham havido algumas ordens solicitando às plataformas a exclusão ou a desindexação global.³⁸² O escopo global previsto em algumas jurisdições também incentivou os cidadãos da região da América Latina e do Caribe a solicitar assistência internacional. Um cidadão paraguaio solicitou à Autoridade Espanhola de Proteção de Dados (AEPD) que ordenasse ao Google que desindexasse uma série de artigos da mídia nos quais ele apareceu. A AEPD negou seu pedido, mas isso demonstra o impacto de tais ordens com implicações globais.³⁸³ Os casos de desindexação fornecem alguma nuance para esse problema. No Tribunal de Justiça do Estado de São Paulo no Brasil, por exemplo, houve casos em que o tribunal ordenou ao Google Brasil que retirasse os resultados de busca de seu site ou que removesse vídeos do YouTube em decisões que poderiam afetar outras jurisdições. No caso do *Centro Espírita Beneficente União do Vegetal Versus Google Brasil Internet Ltda*, o juiz decidiu que o Tribunal não tinha jurisdição para determinar se o vídeo especificado nas alegações do requerente também estava disponível em outros países, como Colômbia e Alemanha, e se assim estivesse, excederia o âmbito de sua competência e constituiria uma violação da soberania de outros países.³⁸⁴

381 Ver: <<https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Policy-Network-20-102-Geographic-Scope-Content-Restrictions.pdf>>. Acesso em: 10 mai 2021.

382 Ver: Tribunal de Justiça do Estado de São Paulo, *Google Brasil Internet Ltda. v. Clóvis de Barros Filho*, São Paulo, 2019.

383 Ver: <<https://blog.cuatrecasas.com/propiedad-intelectual/derecho-al-olvido-audiencia-rechaza-aplicacion-extraterritorial/>>. Acesso em: 10 mai 2021.

384 Ver: Tribunal de Justiça do Estado de São Paulo, *Centro Espírita Beneficente União do Vegetal Google Brasil Internet Ltda.*, São Paulo, 11 de agosto de 2016. Disponível em: <<https://www.conjur.com.br/dl/justica-local-nao-obrigar-google2.pdf>>. Acesso em: 10 mai 2021.

3. ORDENS DE TRIBUNAIS PARA RETIRADA (TAKE-DOWN), MANUTENÇÃO [DA RETIRADA] (STAY-DOWN) E PERMANÊNCIA [DE CONTEÚDO] (STAY-UP)

A Internet possibilitou que o conteúdo fosse visto e compartilhado em todo o mundo em ambientes privados e públicos. Bilhões de mensagens são trocadas e milhões de fotos e horas de vídeos e músicas são carregadas todos os dias, com uma grande proporção sendo em plataformas globais acessíveis a pessoas em todas as partes do mundo. Essa abundância de informações certamente terá um impacto, afetando as pessoas e até mesmo causando danos. Apesar do alto valor estabelecido para a liberdade de expressão, é claro que alguns limites deverão ser impostos por exigências normativas, que podem variar de um país para outro.

Outra tendência global refletida na América Latina e no Caribe é a de tribunais pedirem às plataformas a retirada, a manutenção da retirada e permanência do conteúdo postado on-line. A disparidade de pontos de vista em relação às normas de proteção de diferentes direitos, particularmente a liberdade de expressão, é uma importante fonte de disputas transfronteiriças.

É bastante comum que tais pedidos tenham elementos transfronteiriços. A plataforma pode ser de origem estrangeira, a tecnologia utilizada pode vir do exterior, os dados podem ser mantidos em servidores *off-shore*; em suma, uma vasta gama de situações significa que muitas dessas ordens têm efeitos fora do território do país onde se originam.

Além disso, nem todos os países emitem esses pedidos por razões legítimas. Eles podem ser usados para restringir o conteúdo, perseguir opositores políticos ou com fins de discriminação, entre outras possíveis violações dos direitos humanos. Qualquer análise desses pedidos está inextricavelmente ligada ao assunto subjacente que se destinam a regular e ao direito material nacional e internacional que o abrange. O capítulo IV deste Relatório concentrou-se em algumas das questões mais importantes que levaram os tribunais a emitir ordens de retirada (e manutenção da retirada ou permanência) de conteúdo ou exigir que os provedores procedam à desindexação ou até mesmo apagamento, bloqueio ou remoção de conteúdo.

As ordens de retirada são as mais comuns e geralmente são emitidas em conexão com processos de indenização monetária.

A reparação consiste em proibir a exibição contínua do conteúdo. No entanto, pode haver outros objetivos específicos, como a remoção de informações enganosas ou que possam prejudicar a reputação de alguém.

Em 2012, durante uma campanha eleitoral, um juiz local no Brasil emitiu um pedido para que o Google retirasse de sua plataforma do YouTube um vídeo crítico a um candidato político. Enquanto o recurso estava pendente, o mesmo juiz emitiu um mandado de prisão ao diretor do Google Brasil por desrespeito a seu pedido judicial de retirada de conteúdo.³⁸⁵

Em janeiro de 2016, o Supremo Tribunal de Justiça do Chile ordenou a remoção de uma agência de distribuição de notícias que havia causado danos à reputação de um indivíduo e concedeu à empresa três dias para cumprir a ordem.³⁸⁶

As ordens de permanência [da retirada] também são emitidas em grande número na região. Elas lidam com um ponto débil das ordens de retirada: o fato de que praticamente não há custos para republicar um conteúdo que foi removido. As ordens de manutenção da retirada (do conteúdo), portanto, impõem a obrigação de que o conteúdo não reapareça. Isso cria dois problemas potencialmente desafiadores: (i) as plataformas são obrigadas a monitorar uploads futuros para avaliar se eles contêm o mesmo conteúdo ilegal; e (ii) para acelerar esse monitoramento e torná-lo menos intensivo em termos de recursos, assim, elas são induzidas a usar técnicas automatizadas, ou seja, filtros impulsionados por inteligência artificial.

Isso pode criar um regime privatizado de censura, com as plataformas sendo vistas como policiando conteúdos. Além disso, os filtros automatizados poderiam resultar em uma proibição geral de certos tipos de conteúdo, que, como resultado, nunca seriam publicados.

Arranjos deste tipo são mais fáceis de justificar em questões onde há pouca discussão sobre se o conteúdo deve ser

385 Ver: <<https://www.bbc.com/news/world-latin-america-19753158>>. Acesso em: 10 mai 2021.

386 Supremo Tribunal de Justiça do Chile, decisão de 21 de janeiro de 2016. Ver: <<https://bit.ly/2MbDW6m>>. Acesso em: 10 mai 2021.

considerado ilegal e o risco de “excesso de bloqueio” ou “excesso de filtragem” por plataformas provavelmente terá menos impacto no conteúdo protegido ou em termos de conteúdo que possa ser considerado legal. Um exemplo é o material sobre abuso infantil, já que existe um forte consenso de que é ilegal.

Há também uma discussão sobre se um indivíduo precisa identificar o endereço URL específico que deve ser retirado ou se é suficiente identificar o conteúdo. Neste último caso, cabe às plataformas identificarem onde o material foi publicado e depois retirá-lo.

Em 2007, um juiz brasileiro instruiu a plataforma YouTube a retirar um vídeo com conteúdo sexual de uma modelo famosa que havia sido postado sem o seu consentimento. Considerando que o vídeo foi repostado diversas vezes, o magistrado ordenou que o acesso ao site fosse bloqueado.³⁸⁷ A ordem foi alterada no dia seguinte, de modo a não restringir o acesso ao YouTube no país.

Em 2012, um tribunal argentino ordenou a remoção “permanente” de imagens sexuais de um modelo de um motor de busca. O tribunal declarou que a plataforma tinha os meios para fazer isso.³⁸⁸

Em 2017, o Tribunal Constitucional da Colômbia instruiu o Google a excluir um blog anônimo de sua plataforma Blogger porque o blog estaria violando o direito ao desenvolvimento pessoal e à privacidade.³⁸⁹

As decisões para a permanência do conteúdo (*stay-up*) ainda não são tão comuns, sendo que muito poucos países as emitiram. O entendimento sobre a liberdade de expressão on-line é que as plataformas

387 Ver: <https://www.nytimes.com/2007/01/05/business/worldbusiness/05fobriefs-JUDGEBLOCKSY_BRF.html>. Acesso em: 10 mai 2021.

388 Ver: <<https://www.internetjurisdiction.net/uploads/pdfs/Papers/Internet-Jurisdiction-Synthesis-2-Dec-2012.pdf>>. Acesso em: 10 mai 2021.

389 Ver: Tribunal Constitucional da Colômbia, Acción de tutela interpuesta por John William Fierro Caicedo, contra Google Inc. y otros, No. T-063A/17, Bogotá, 9 Mai 2018. Disponível em: <<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", Paris, 2017. Disponível em: <<https://www.internetjurisdiction.net/publications/retrospect#eyJ0byl6ljlwMjAtMDgifQ==>>. Acessos em: 10 mai 2021.

devem respeitar a liberdade de expressão. No entanto, elas têm uma margem de manobra para impor certas restrições, principalmente com base em seus termos de serviço e diretrizes de comunidade.

Entretanto, alguns países como a Alemanha e, na região, o Brasil, julgaram que existem circunstâncias em que o conteúdo é protegido e não deve ser restringido por plataformas. Assim, os tribunais ordenaram que o conteúdo retirado fosse novamente disponibilizado.³⁹⁰

Em um exemplo recente, em dezembro de 2019, o Tribunal de Justiça do Distrito Federal e Territórios do Brasil concedeu uma liminar contra o Facebook exigindo que ele mantivesse on-line um post de um deputado, Eduardo Bolsonaro, no qual ele criticou jornalistas por causa de um artigo publicado na imprensa sobre sua esposa. O Facebook declarou que os jornalistas haviam denunciado o uso não autorizado de suas imagens, o que constituía uma violação dos termos de serviço da plataforma.³⁹¹ Uma decisão de fevereiro de 2020 julgou o mérito do caso a favor do Facebook, considerando que não houve interferência indevida na liberdade de expressão do deputado.³⁹²

Em conjunto, tais ordens podem ter importantes consequências para a moderação do conteúdo da plataforma em diferentes países. Os denominadores comuns mínimos entre as normas de diferentes países são difíceis de encontrar quando alguns tribunais podem ordenar que determinados conteúdos sejam retirados, enquanto outros podem ordenar que o mesmo conteúdo seja mantido. Há, portanto, um potencial real para conflitos jurisdicionais. As plataformas são chamadas a serem as guardiãs do equilíbrio e não devem pecar por excesso ou por falta com relação à remoção de conteúdo.

390 Ver: D. Keller, "Why DC Pundits' must-carry claims are relevant to global censorship", Stanford, Center for Internet and Society (CIS), 13 Set 2018. Disponível em: <<http://cyberlaw.stanford.edu/blog/2018/09/why-dc-pundits-must-carry-claims-are-relevant-global-censorship>>. Acesso em: 10 mai 2021.

391 Ver: <<https://www.uol.com.br/tilt/noticias/redacao/2019/12/03/posts-de-novo-no-ar-facebook-perde-para-eduardo-bolsonaro-na-justica.htm>>. Acesso em: 10 mai 2021.

392 Ver: <<https://www.migalhas.com.br/quentes/323429/facebook-nao-indenizara-eduardo-bolsonaro-por-remover-posts-que-violaram-regras-da-rede-social>>. Acesso em: 10 mai 2021.

A Rede de Políticas Internet & Jurisdição, através de seu programa temático Conteúdo e Jurisdição, propôs uma série de estruturas e soluções que permitem tanto aos governos quanto às plataformas alcançar um equilíbrio e gerenciar conteúdo, levando em consideração a diversidade de leis, costumes e culturas ao redor do mundo, e especificamente na América Latina e no Caribe.³⁹³

4. MULTAS E SANÇÕES

As sanções administrativas impostas pelas autoridades locais constituem um instrumento importante para as execuções da regulação relacionada à Internet. As autoridades envolvidas podem variar dependendo do assunto em questão, como consumidor, antitruste, ambiental ou proteção de dados. As sanções geralmente variam de advertências e multas até a suspensão ou término de uma determinada atividade.

Como descrito nas seções anteriores, muitas das regulações de proteção de dados na região foram inspiradas pelo quadro legal europeu, que prevê severas sanções administrativas. Uma diferença notável, no entanto, é que os regulamentos europeus preveem a cooperação internacional entre países, enquanto na América Latina e no Caribe a maioria das regras relativas à responsabilidade administrativa é de âmbito nacional.

As sanções administrativas por violação da privacidade de dados pessoais na região incluem multas de até 100.000 pesos (aproximadamente US\$ 1.500) na Argentina³⁹⁴ e até 10.000 balboas (aproximadamente US\$ 10.000) no Panamá. Em Trinidad e Tobago, as penalidades legais baseiam-se no faturamento anual de uma empresa, podendo ser aplicada uma multa de até 10% deste valor.³⁹⁵ No Brasil, existem disposições específicas que exigem que as autoridades considerem a receita total da empresa em questão,³⁹⁶ o que poderia significar multas menores para empresas menores.

393 Ver: <<https://www.internetjurisdiction.net/news/content-jurisdiction-program-outcomes>>. Acesso em: 10 mai 2021.

394 Lei nº 25326, artigo 31. Ver: <<https://www.argentina.gob.ar/normativa/nacional/ley-25326-64790/actualizacion>>. Acesso em: 10 mai 2021.

395 Data Protection Act, 2011, seção 96. Ver: <<http://www.tparliament.org/legislations/a2011-13.pdf>>. Acesso em: 10 mai 2021.

396 Brasil, Lei nº 13.709, artigo 52.4. Ver: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em: 10 mai 2021.

Embora a legislação nacional preveja a cooperação entre as autoridades de proteção de dados,³⁹⁷ é justo dizer que sanções e/ou ordens estão sendo impostas em um contexto doméstico. As agências reguladoras competentes são geralmente confrontadas com a escolha de jurisdição por empresas que armazenam dados em um país diferente daquele onde as pessoas a quem os dados se referem estão localizadas ou residem (e onde a lei está sendo executada). Em 1º de abril de 2020, a Superintendência da Indústria e Comércio da Colômbia reafirmou sua autoridade para impor ordens administrativas não somente ao Facebook Colômbia, mas também ao Facebook Inc., localizado nos Estados Unidos, e ao Facebook Irlanda, baseado na Irlanda.³⁹⁸

Um especialista entrevistado afirmou que as recentes regulações de proteção de dados estavam se tornando cada vez mais uma espécie de lei extraterritorial, pois produziam efeitos em outros países, ao mesmo tempo em que promoviam uma espécie de “reconceitualização da soberania”. Esse efeito extraterritorial se torna evidente quando agências reguladoras impõem sanções que explicitamente exigem ações de uma empresa sediada em outro lugar. Para garantir um ecossistema regulatório que preserve o aspecto transnacional da Internet, as autoridades devem exercer suas competências de cooperação internacional e considerar acordos bi ou multilaterais. A cooperação internacional é uma das principais linhas de ação para fazer valer a privacidade³⁹⁹ e deve ser tratada como tal.

Outra situação presente em alguns países da região é a incerteza sobre quais órgãos são competentes para aplicar sanções administrativas. No Brasil, onde a Autoridade Nacional de Proteção de Dados ainda não está totalmente operacional, procedimentos administrativos e ordens relacionadas à proteção de dados já foram executados pela Secretaria Nacional do Consumidor (SENACON), incluindo multas tanto para Facebook Inc. quanto para Facebook Serviços Online do Brasil

397 Ver, por exemplo, Nicarágua, Lei nº 787 de 2012, artigo 29.i.

398 Superintendência da Indústria e Comércio, resolução nº 12.192 de 2020. Ver: <<https://www.sic.gov.co/sites/default/files/files/2020/Res%2012192%20011V2020%20SIC%20Facebook%20Inc.pdf>>. Acesso em: 10 mai 2021

399 Ver: A. Brian, “Data protection and enforcement in Latin America and in Uruguay”, *Enforcing Privacy: Regulatory, Legal and Technological Approaches*, D. Wright and P. de Hert (eds.), Berlin, Springer, 2016.

Ltda.⁴⁰⁰ É verdade que as regulações sobre dados, consumidores e concorrência criam espaço para impor sanções, mas ainda não está claro em que medida elas são necessárias. Assim, em alguns casos, são necessárias mais cooperação e coesão não apenas no contexto internacional, mas também internamente.

Muitos países da região adotaram legislação impondo severas sanções pelo não cumprimento de normas setoriais que poderiam se aplicar às atividades da Internet, a maioria inspirada nas regulações europeias. Isso é particularmente prevalente no campo da proteção de dados.

5. OS TERMOS DE SERVIÇO ESTÃO INTERLIGADOS COM AS LEIS NACIONAIS

Os termos de serviço criados por empresas multinacionais têm se interligado de alguma forma com a legislação nacional, servindo como uma importante fonte de orientação sobre o que é permitido ou não em tais plataformas. Por um lado, as empresas enfrentam o desafio de equilibrar a liberdade de expressão contra um conteúdo potencialmente prejudicial. Por outro lado, elas estão tendo que lidar com mudanças significativas no cenário jurídico em áreas como propriedade intelectual, privacidade de dados, limitações de responsabilidade e proteção ao consumidor.

Os termos de serviço e as diretrizes de comunidades implementam obrigações legislativas (particularmente no que diz respeito ao procedimento), mas complementam-nas com a visão das próprias empresas sobre como deve ser o ambiente da plataforma. Várias das questões apresentadas neste relatório decorrem de conflitos entre as regulações domésticas e os termos de serviço dos fornecedores e/ou diretrizes de comunidades.

Um aspecto transfronteiriço importante é que tais plataformas tendem a ser construídas sobre uma arquitetura mundial ou, pelo menos, regional. Assim, muitos elementos dos termos de serviço que suportam essas arquiteturas têm um núcleo comum. As normas desenvolvidas pelas plataformas cobrem vastas áreas do globo e são proporcionalmente influentes. Os padrões nacionais regulatórios e consuetudinárias podem

400 Ver: Ministério da Justiça e Segurança Pública, "MJSP multa Facebook em R\$ 6,6 milhões", Brasília, 30 Dez 2019. Disponível em: <<https://www.gov.br/mj/pt-br/assuntos/noticias/mjssp-multa-facebook-em-r-6-6-milhoes>> . Acesso em: 10 mai 2021.

entrar em conflito com tais termos e diretrizes, levando a uma necessidade de acomodação.

O problema é mais agudo nos casos em que as entidades por trás das plataformas têm menos recursos ou são *start-ups*. O crescimento rápido pode ser particularmente perturbador e levar a choques regulatórios e culturais. Estes podem resultar de um excesso de autorregulação, quando os termos são mais intrusivos do que as leis do país ou fornecem soluções diferentes (ou, na maioria das vezes, são mais liberais ou menos desenvolvidos), ou têm lacunas ou deficiências, não conseguindo lidar com tipos de comportamentos que deveriam ser contemplados, seja por exigências regulatórias, seja por necessidades culturais.

Uma questão intimamente relacionada diz respeito à moderação do conteúdo. Os termos de serviço e os padrões de comunidade desempenham um papel muito importante. O ambiente da plataforma é impactado pelos tipos de conteúdo que são permitidos e incentivados. Os serviços de Internet que atendem crianças devem restringir certos tipos de conteúdo que podem ser legais, mas não são apropriados para crianças. Na outra ponta do espectro, os serviços que visam uma clientela mais adulta podem ser mais liberais em relação aos tipos de conteúdo permitidos, mas devem levar em consideração as normas relativas ao conteúdo sexual on-line; situações como pornografia infantil e pornografia de vingança (como discutido na seção IV.A.4) geralmente exigem uma resposta rápida.

Os termos e os padrões servem para determinar o conteúdo que deve permanecer e ser removido. Os governos tendem a confiar nessas ferramentas com o objetivo de pressionar as empresas a manter certos padrões morais ou alcançar determinados objetivos (como a implementação de leis). Para equilibrar essas necessidades, certas plataformas sugeriram a existência de órgãos de supervisão capazes de sugerir cursos de ação em casos particularmente espinhosos.⁴⁰¹

Isso também se aplica à propriedade intelectual. A União Europeia atualizou sua Diretiva sobre Direitos Autorais no Mercado

401 Ver: The Economist, "Facebook unveils details of its content-oversight board", London, 30 Janeiro 2020. Disponível em: <<https://www.economist.com/business/2020/01/30/facebook-unveils-details-of-its-content-oversight-board>>. Acesso em: 10 mai 2021.

Único Digital, criando incentivos para que as plataformas ofereçam mecanismos de moderação de conteúdo antes mesmo de sua publicação. A Diretiva teve um impacto sobre os países da região. Alguns poucos lançaram procedimentos para reformar sua legislação sobre propriedade intelectual. O Brasil, por exemplo, iniciou uma consulta e um amplo estudo sobre uma nova estratégia nacional para a propriedade intelectual. Um dos tópicos, os mecanismos de proteção contra a pirataria on-line, se baseia fortemente nos últimos desenvolvimentos da legislação europeia.⁴⁰²

Alguns governos da América Latina e do Caribe têm pressionado ou mesmo firmado acordos com plataformas de comércio eletrônico para melhorar as medidas que tomam contra a pirataria e a venda de produtos contrafeitos. Essas ações levaram muitas plataformas de comércio eletrônico a autorregular e adicionar meios não judiciais de resolução de disputas aos seus termos e condições. Elas utilizam métodos internos (automáticos na maioria das vezes) para encontrar e derrubar violações percebidas (contrafação ou pirataria). Esses mecanismos alternativos de resolução de disputas geralmente oferecem uma oportunidade para que tanto o titular quanto o suposto infrator expressem seus pontos de vista.

Além dos sistemas de resolução de disputas criados pelo setor privado, os governos da região têm promovido iniciativas de correção. Essas iniciativas são inspiradas no Memorando de Entendimento sobre a venda de produtos contrafeitos na Internet, facilitado pela Comissão Europeia e acordado por várias plataformas, titulares de direitos e associações.⁴⁰³

Em muitos casos, os termos de serviço identificam a jurisdição a ser usada para resolver disputas além da lei aplicável. Eles são considerados como sendo contratos (embora sejam contratos de adesão) que regulam a relação com os usuários e tais assuntos como autonomia das partes. Na região, entretanto, a tradição de proteção ao consumidor é robusta e há uma percepção de que a autonomia

402 Ver: <<http://cultura.gov.br/ministerio-da-cidadania-abre-consulta-publica-sobre-reforma-da-lei-de-direitos-autorais/>>; <<http://www.mdic.gov.br/index.php/ultimas-noticias/3948-grupo-interministerial-de-propriedade-intelectual-inicia-atividades>>. Acessos em: 10 mai 2021.

403 Ver: <https://ec.europa.eu/growth/industry/policy/intellectual-property/enforcement/memorandum-understanding-sale-counterfeit-goods-internet_en>. Acesso em: 10 mai 2021.

das partes deve ser limitada, particularmente em circunstâncias em que um consumidor está envolvido e não pode negociar as cláusulas do contrato. Isso reflete uma tendência emergente identificada no *Relatório de Status Global 2019* de que os tribunais não apoiam cláusulas de escolha do foro e do direito aplicável nos termos de serviço das plataformas internacionais da Internet.

B. Principais abordagens técnicas

A América Latina e o Caribe não são exceção à regra de que algumas das mais importantes questões legais relacionadas à Internet e à jurisdição tendem a ser vistas através da lente das soluções técnicas. Alguns países seguiram linhas semelhantes às soluções encontradas em outros países do mundo, mas outros acabaram com um sabor regional muito particular. Esta seção se propõe a apresentar e analisar as abordagens técnicas mais significativas que se apresentaram na região e destacar as peculiaridades que se desenvolveram entre os países da América Latina e do Caribe. A análise foi realizada a partir da perspectiva dos impactos transfronteiriços que eles podem ter e suas implicações práticas e legais.

A maioria das abordagens técnicas aqui apresentadas tem como objetivo abordar a questão de como controlar e limitar o acesso ao conteúdo. Ela tem sido fonte de grandes disputas na Internet durante a última década. Em certa medida, os países começaram adotando uma abordagem mais liberal do *laissez-faire* na produção e distribuição de conteúdo. Os intermediários eram obrigados a se autorregular e os produtores de conteúdo eram responsáveis pelo conteúdo que disponibilizaram. Na metade da década, alguns países da região começaram a desafiar essa visão, desenvolveram e implantaram as técnicas discutidas neste relatório.

As tecnologias de geolocalização, que raramente faziam parte da arquitetura dos serviços de Internet no passado, passaram a ser vistas como mais relevantes. O *Relatório de Status Global 2019* apontou, e a pesquisa para este Relatório confirmou, que existem opiniões contrastantes sobre a conveniência de introduzir tais técnicas em maior escala. Talvez a divergência mais importante esteja relacionada à filtragem de conteúdo. Várias iniciativas nacionais consideraram a conveniência de exigir tecnologias de filtragem para partes específicas da Internet, particularmente grandes redes de mídia social.



O bloqueio de serviços e aplicações (aplicativos) da Internet é uma questão importante. Em vários casos, os próprios governos, tribunais e empresas impediram o acesso a serviços e aplicativos específicos, com diferentes graus de transparência e devido processo. Em muitos casos, isso foi feito para cumprir uma lei local ou uma ordem judicial de outra natureza. Também ocorreram paralisações de toda a Internet, mas geralmente foram temporárias e restritas a áreas específicas.

Outras abordagens técnicas que foram implantadas incluem restrições ao Sistema de Nomes de Domínio (DNS) impostas sob ordens judiciais que exigem suspensão, exclusão, não resolução, apreensão e transferência, ou bloqueio/roteamento de endereço IP e bloqueio de URL. Finalmente, alguns países discutiram e, em certa medida, implementaram, a localização obrigatória de dados. Todas essas técnicas restringem o funcionamento da Internet como originalmente previsto e estão mudando rapidamente o cenário regulatório. As abordagens técnicas podem ser úteis para lidar com os desafios legais transfronteiriços; entretanto, é necessário entender suas consequências e buscar consenso sobre a adequação da sua implantação.

1. TECNOLOGIAS DE GEOLOCALIZAÇÃO

Se houvesse um mapa da Internet, a versão original não teria fronteiras. Os protocolos que controlam a Internet foram concebidos para desconsiderar as fronteiras dos países, conferindo-lhe, assim, um caráter sem fronteiras. Entretanto, as tecnologias de geolocalização têm servido para trazer de volta um grau de geografia para a Internet. Em termos gerais, essas tecnologias são capazes de determinar a posição geográfica dos usuários, permitindo, assim, aos provedores de serviços adaptar alguns atributos às peculiaridades daquele lugar, mudando características como a linguagem padrão, fornecendo resultados mais precisos (por exemplo, mostrando onde fica o restaurante mais próximo) e até mesmo limitando o acesso a certos componentes ou conteúdos com base em costumes e normas culturais, sociais ou legais.

A tecnologia por trás da geolocalização não é uniforme, mas depende de vários aspectos como endereços IP, GPS, a linguagem padrão do dispositivo ou as atividades para as quais ele está sendo usado (corrida, caminhada, navegação), triangulação de torres de telefonia móvel e até mesmo sinais wi-fi e Bluetooth. O grau

de certeza e precisão com que o dispositivo está localizado varia de acordo com isso. Outro aspecto que pode afetar sua precisão é o uso de uma tecnologia de ocultação, como uma rede virtual privada (VPN), empregando técnicas que bloqueiam ou informam erroneamente a localização da pessoa ou dispositivo.

Em muitos lugares do mundo, o debate sobre o uso de tecnologias de geolocalização amadureceu nas últimas duas décadas. Na Europa especialmente, o debate começou com uma discussão sobre se tais técnicas poderiam ser empregadas, dado seu nível de precisão, e evoluiu para focalizar sua adequação e a extensão de seu uso. Paralelamente às políticas de constituição de um Mercado Único Digital Europeu, a União Europeia emitiu até mesmo uma regulação (No. 2018/302) relativo ao geobloqueio, uma das funções potenciais das tecnologias de geolocalização.

Esta regulação restringe o uso de tais tecnologias em casos de “bloqueio geográfico injustificado”, que é entendido como ocorrendo em três circunstâncias: (i) a venda de bens sem entrega física (os clientes têm o direito de comprar produtos vendidos por lojas em países diferentes daquele em que estão); (ii) a venda de serviços prestados por via eletrônica (um cliente pode optar por utilizar um serviço prestado por um prestador de outro país e não deve ser obrigado a pagar taxas adicionais); (iii) a venda de serviços prestados num local físico específico (por exemplo, preços com desconto para pessoas num local específico).

Na América Latina e no Caribe, a discussão sobre o geobloqueio ainda não tem a especificidade regulatória que tem em outros países e regiões. No entanto, há um debate político e jurídico crescente sobre as implicações das tecnologias de geolocalização em relação à proteção do consumidor e dos dados, especialmente o bloqueio geográfico e a geoprecificação.

No Brasil, por exemplo, a empresa de viagens on-line Decolar foi multada por sujeitar seus clientes ao bloqueio geográfico e à geoprecificação. O caso dizia respeito à discriminação entre clientes do Brasil e da Argentina, já que alguns hotéis listaram preços médios mais elevados para clientes brasileiros do que para os argentinos. Além disso, a empresa bloquearia o acesso a certos hotéis e serviços (o aluguel de certos carros) para clientes de um país e não do outro.⁴⁰⁴

404 Ver: Secretaria Nacional do Consumidor, Nota Técnica, nº 92/2018, Brasília, 16 de junho de 2018.

As leis de privacidade de dados preveem o direcionamento das atividades de processamento de dados para um país ou local específico. Isso implica algum grau de georreferenciamento e o uso de tecnologias de geolocalização. O Regulamento Geral de Proteção de Dados (GDPR), por exemplo, entra em ação sempre que as empresas direcionam suas atividades para o mercado comum [europeu]. O mesmo pode ser visto na Lei Geral de Proteção de Dados brasileira.

Como no *Relatório de Status Global 2019*, os pontos levantados pelos entrevistados centraram-se em três temas: (i) essas tecnologias podem ser facilmente contornadas e podem não ser particularmente eficazes; (ii) podem impactar a liberdade de expressão e o acesso à informação; e (iii) podem ser utilizadas em determinadas circunstâncias comerciais. A semelhança entre os pontos apontados pelos entrevistados globais e regionais é impressionante, embora especialistas da região pareçam ser da opinião de que essas tecnologias podem ser mais úteis em um ambiente comercial do que em um ambiente mais público. Um especialista mencionou que as tecnologias de geolocalização podem não ser apropriadas para processos democráticos. A preocupação na região parece ser sobre o acesso à informação. Assim, há uma visão de que as tecnologias de geolocalização podem impedir o acesso a informações armazenadas fora do país.

À medida que a luta contra a pandemia do COVID-19 continua, os países da região estão tentando fazer maior uso dos dados para lidar melhor com a propagação do vírus. As tecnologias de geolocalização estão cada vez mais desempenhando um papel na determinação do grau de distanciamento social adotado por grupos maiores ou mapeando rotas e contatos dos indivíduos infectados.

As preocupações com a privacidade e a proteção de dados estão crescendo, uma vez que a natureza transfronteiriça da Internet facilita o armazenamento de dados confidenciais num país estrangeiro. Além disso, países com uma história recente de regimes autoritários estão enfrentando manifestações públicas de pessoas afirmando que o uso de dados de geolocalização para combater a pandemia é uma desculpa para introduzir uma supervisão sem precedentes dos cidadãos.

A expectativa deve ser que um debate mais informado sobre o uso de tecnologias de geolocalização, combinado com

preocupações políticas, legais e técnicas, se desenvolva na região como legado da luta contra o COVID-19.

INFOGRÁFICO 11

Quão apropriada é uma ferramenta de filtragem de conteúdo geolP para abordar o escopo geográfico dos direitos nacionais?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

2. A FILTRAGEM DE CONTEÚDO ESTÁ CRESCENDO À MEDIDA QUE OS PAÍSES COMBATEM DISCURSO DE ÓDIO E DESINFORMAÇÃO

Quase nenhum país da América Latina e do Caribe organizou suas redes a priori para bloquear (ou filtrar) o conteúdo recebido ou para policiar o conteúdo produzido localmente. Tais restrições não foram instaladas como parte integrante da rede na infraestrutura dos países da região (também conhecida como espinha dorsal da Internet). No entanto, muitos governos têm procurado impor uma obrigação aos fornecedores de acesso ou provedores de serviços de Internet de monitorar, filtrar ou derrubar certas categorias de conteúdo em um curto período de tempo. Em determinadas circunstâncias, tais regulações podem ter objetivos legítimos e serem aplicadas com limites e controles razoáveis. Em outros, elas podem ter um impacto semelhante à censura e podem até moldar o conteúdo político e cultural, impactando inadvertidamente a liberdade de expressão ou mesmo estendendo as proteções de direitos autorais sem justificativa.

Quanto à filtragem embutida na espinha dorsal da Internet, há relatos de que o governo de Cuba tem em vigor medidas técnicas capazes de filtrar o conteúdo da Internet.⁴⁰⁵ Os relatos

405 Ver: A. Shahbaz e A. Funk, Freedom on the Net 2019: The Crisis of Social Media, Washington, D.C., Freedom House, 2019. Disponível em: <<https://www.freedomonthenet.org/country/cuba/freedom-on-the-net/2019#B1>>. Acesso em: 10 mai 2021.

afirmam que mensagens contendo palavras específicas como “democracia” ou “ditadura” nunca chegam ao seu destino e que certos serviços de Internet considerados inconsistentes com os valores do Estado cubano não estão disponíveis on-line.

O Relator Especial para a Liberdade de Expressão da Comissão Interamericana de Direitos Humanos (CIDH) analisou a arquitetura institucional que restringe e filtra o conteúdo disponível on-line em Cuba.⁴⁰⁶ Também observou alguns trechos de regulação particularmente relevantes. Merecem destaque as resoluções 127/2007, que trata da segurança da tecnologia da informação e 179/2008, uma regulação para provedores de serviços de Internet que trata do acesso público à Internet. A primeira proíbe a circulação de dados ou informações contrárias ao “interesse social ou moral e aos costumes públicos”. A outra cria uma obrigação para os provedores de serviços de Internet (PSIs) de monitorar e “regular” o conteúdo on-line e estabelece um regime de responsabilidade direta para os intermediários.⁴⁰⁷ Esses trechos da regulação são considerados impactantes à liberdade de expressão e à liberdade de acesso à informação.⁴⁰⁸

Na República Bolivariana da Venezuela, a Lei de Responsabilidade Social na Rádio, Televisão e Mídia Eletrônica estabelece que os PSIs podem ser responsabilizados pelas informações que disponibilizam e que geram ansiedade entre os cidadãos, impedem o reconhecimento das autoridades legitimamente constituídas, perturbam a ordem pública, incitam ou encorajam o não cumprimento das leis.⁴⁰⁹

No início de 2019, a Assembleia Nacional Constituinte da República Bolivariana da Venezuela apresentou um projeto de lei chamado Lei Constitucional do Ciberespaço da República Bolivariana da Venezuela. Foi noticiado que foram previstos amplos poderes para o governo regular a Internet no país, inclusive com

406 Ver: Special Rapporteur for Freedom of Expression, Special Report on the Situation of Freedom of Expression in Cuba, Washington, D.C., 2019.

407 Ibidem.

408 Ibidem.

409 Ver: <<http://www.leyresorte.gob.ve/wp-content/uploads/2012/07/Ley-de-Responsabilidad-Social-en-Radio-Television-y-Medios-Electr%C3%B3nicos.pdf>>. Acesso em: 10 mai 2021

a filtragem obrigatória de conteúdo.⁴¹⁰ Esse é um tipo de cenário regulatório no qual provedores e PSIs em geral têm incentivos para filtrar conteúdo.

Além disso, em novembro de 2017, a República Bolivariana da Venezuela aprovou uma Lei contra o Ódio que autoriza as autoridades a revogarem licenças e bloquearem serviços de Internet se os PSIs exibirem conteúdo (inclusive conteúdo de terceiros) considerado pelo governo como sendo incitadores de ódio ou intolerância.⁴¹¹ A Lei não requer por si só a aplicação de filtros de conteúdo, mas a severidade das sanções cria um ambiente que incentiva a implantação dessas tecnologias.

Outros países da região têm se preocupado com a disseminação da desinformação, particularmente durante as eleições. O escândalo envolvendo a Cambridge Analytica, uma empresa acusada de usar dados pessoais para criar campanhas de desinformação personalizadas, levou muitos países da América Latina e do Caribe a revisar suas leis referentes ao papel dos intermediários da Internet.

Alguns países pressionaram por uma legislação que exigiria que os prestadores de serviços implantassem mecanismos para identificar e, em certos casos, retirar discursos contendo desinformação, particularmente durante as eleições. O Relator Especial para a Liberdade de Expressão declarou que, sob as normas do Sistema Interamericano para a proteção dos direitos humanos, qualquer regulação que exija que os PSIs implementem bloqueio ou filtragem de conteúdo deve ser restrita a casos excepcionais, como pornografia infantil, propaganda de guerra e discursos de ódio que constituam incitamento à violência ou incitação ao genocídio, com a proteção adicional de que um juiz independente deve determinar a ilegalidade do conteúdo.

410 Ver: <<https://www.accessnow.org/a-bill-in-venezuela-seeks-to-give-the-government-absolute-control-over-the-internet/>>. Acesso em: 10 mai 2021.

411 Ver: <<https://www.bloomberg.com/news/articles/2017-11-08/venezuela-passes-anti-hate-law-threatening-media-censorship>>. Acesso em: 10 mai 2021.

3. O SISTEMA DE NOMES DE DOMÍNIO: SUSPENSÕES E BLOQUEIOS RESULTANTES DE NOTIFICAÇÕES E ORDENS JUDICIAIS E ADMINISTRATIVAS

O Sistema de Nomes de Domínio (DNS) está na raiz da Internet, operando como um sistema de endereçamento que ajuda os usuários a encontrar o seu caminho em torno da rede. Cada dispositivo conectado à rede tem um endereço exclusivo, uma série de números chamada endereço IP. O DNS permite que estas cadeias de números sejam transformadas em conjuntos de letras, facilitando, assim, sua memorização pelos usuários.

Como mencionado no *Relatório de Status Global 2019* da Rede de Políticas Internet & Jurisdição, os pedidos transfronteiriços de suspensão de nomes de domínio estão sendo cada vez mais enviados a operadores técnicos em relação a conteúdos ou atividades supostamente abusivas nos sites subjacentes.⁴¹² Essa abordagem é atraente para os solicitantes porque a suspensão de um nome de domínio tem um efeito global direto e imediato.

Os efeitos de longo alcance da adulteração do Sistema de Nomes de Domínio justificam uma análise cautelosa das supostas violações e uma reflexão sobre a proporcionalidade da medida. Suspender ou bloquear um nome de domínio inteiro significa que todo o conteúdo de um determinado site fica indisponível. Os operadores devem, portanto, considerar a interferência no DNS como uma medida de último recurso a ser usada somente se não houver outra maneira de lidar com a conduta ou conteúdo alegadamente infrator.

Como eles têm o efeito prático de rapidamente tirar do ar o conteúdo em todo o mundo, as suspensões e os bloqueios no nível do DNS têm sido usados para lidar com questões muito diferentes, desde violações de propriedade intelectual até conteúdos nocivos. A decisão de retirar um nome de domínio específico pode ser desencadeada simplesmente por uma notificação da vítima de uma alegada violação, mas também pode ser determinada por ordens administrativas e judiciais.

Avisos para suspender ou bloquear nomes de domínio podem naturalmente ter um impacto transfronteiriço. O nome de domínio “ldmx.org” foi registrado a fim de hospedar um site que protestava

412 Ver: D. Jerker, Internet & Jurisdiction Global Status Report 2019, Paris, Internet & Jurisdiction Policy Network, 2019.

contra o uso excessivo da força pela polícia no México. O nome de domínio foi uma referência ao dia em que Enrique Peña Nieto fez o juramento como presidente em dezembro de 2012. Uma série de protestos irrompeu naquele dia e foi reprimida pela polícia. Dezenas de estudantes e manifestantes foram detidos e um manifestante morreu. Um ano depois, o site foi encerrado após um pedido de suspensão do nome de domínio recebido pelo GoDaddy, o registrador do nome de domínio, do Departamento de Segurança Nacional dos Estados Unidos. A razão para a retirada foi que o site era “parte de uma investigação policial em andamento”⁴¹³ e que seu conteúdo violava os termos de serviço da empresa.⁴¹⁴

Alguns governos da região são conhecidos por sua prática de bloqueio DNS, embora a medida não seja generalizada na região. Recentemente, o governo venezuelano bloqueou a rede Tor, uma ferramenta que permite aos usuários navegar na Internet de forma anônima. O bloqueio foi executado pelo provedor de Internet CAN-TV, o maior PSI do país.⁴¹⁵ Para acessar a ferramenta bloqueada, os usuários venezuelanos tiveram que contar com redes privadas virtuais (VPNs), para contornar as regulações governamentais.

Em “parknets” cubanos (nome dado aos lugares públicos dos quais a Internet pode ser acessada), vários sites foram bloqueados, inclusive pontos de venda de mídia.⁴¹⁶

Seguindo uma tendência global, as ordens judiciais para o bloqueio ou suspensão de nomes de domínio estão aumentando na América Latina e no Caribe. Na Argentina, por exemplo, a Câmara Argentina de Produtores de Fonogramas e Videogramas e outras empresas de gestão de direitos autorais entrou com uma ação judicial e recebeu uma liminar⁴¹⁷ para bloquear o Pi-

413 Ver: <<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>>. Acesso em: 10 mai 2021.

414 Ver: 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. Disponível em: <<https://itsrio.org/wp-content/uploads/2018/01/digital-rights.pdf>>. Acesso em: 10 mai 2021.

415 Ver: <<https://www.accessnow.org/venezuela-blocks-tor/>>. Acesso em: 10 mai 2021.

416 Ver: <<https://blog.torproject.org/measuring-internet-censorship-cubas-parknets>>. Acesso em: 10 mai 2021.

417 Ver: <https://www.scribd.com/fullscreen/232015119?access_key=key-2j7jKJaMaBADeV4XpAOw&allow_share=true&escape=false&view_mode=scrollar>. Acesso em: 10 mai 2021.

rate Bay, um site popular de compartilhamento de arquivos.⁴¹⁸ A liminar ordenou que os PSIs bloqueassem vários nomes de domínio associados ao site de compartilhamento de arquivos, como thepiratebay.org e thepiratebay.se.⁴¹⁹

Como observado pela organização não-governamental (ONG) Derechos Digitales, em vez de bloquear links para obras que são suspeitas de infração, para o trabalho de um determinado artista ou grupo de artistas ou para obras musicais ou fonográficas em geral, a decisão tomada proibiu o acesso a todo o site.⁴²⁰

Vários defensores da liberdade de expressão lembraram recentemente que “o bloqueio de sites inteiros, endereços IP, portas ou protocolos de rede providenciados pelo Estado é uma medida extrema que só pode ser justificada quando estipulada por lei e necessária para proteger um direito humano ou outro interesse público legítimo, ou seja, deve ser proporcional, e não deve haver medidas alternativas menos invasivas que possam preservar esse interesse e respeitar as garantias mínimas do devido processo”.^{421 422}

4. BLOQUEIO DE SITES E APLICATIVOS

A paralisação do acesso à Internet ou de serviços ou bloqueio de aplicativos são medidas aplicadas em muitos países do mundo. *O Relatório de Status Global 2019* da Rede de Políticas Internet & Jurisdição mencionou essa tendência e destacou suas implicações transfronteiriças. Na maioria das vezes, os provedores de serviços são empresas estrangeiras e as paralisações dificilmente são localizadas.

418 Ver: <<https://www.derechosdigitales.org/7608/internet-bajo-censura-bloquean-pirate-bay-en-argentina/>>. Acesso em: 10 mai 2021.

419 Ver: <<https://www.lanacion.com.ar/tecnologia/la-comision-nacional-de-comunicaciones-ordena-el-bloqueo-de-the-pirate-bay-en-la-argentina-nid1705910/>>. Acesso em: 10 mai 2021.

420 Ver: <<https://www.derechosdigitales.org/7608/internet-bajo-censura-bloquean-pirate-bay-en-argentina/>>. Acesso em: 10 mai 2021.

421 Ver: Organization for Security and Cooperation in Europe (OSCE) and others, Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade, Vienna, 2019. Disponível em: <<https://www.osce.org/representative-on-freedom-of-media/425282?download=true>>. Acesso em: 10 mai 2021.

422 Ver: <http://www.oas.org/en/iachr/expression/publications/Guia_Desinformacion_VF%20ENG.pdf>. Acesso em: 10 mai 2021.

Devido à arquitetura da Internet e sua natureza interligada, uma paralisação em um lugar pode prejudicar o acesso ou a usabilidade em outro. Se a paralisação for implementada na camada de infraestrutura da Internet, é ainda mais provável que tenha repercussões além do território originalmente pretendido. Os usuários não podem limitar-se a um país e os serviços podem ser prestados através de um sistema transnacional.

Os países da América Latina e do Caribe não são diferentes. Um dos entrevistados observou que a infraestrutura de Internet da região é compartilhada por muitos países e empresas. Uma ação em um local pode ter repercussões sobre os outros, mesmo em diferentes Estados. Governos, tribunais e empresas muitas vezes bloquearam certos serviços e aplicativos da Internet, com consequências que foram sentidas além da área ou serviço pretendido. Outro entrevistado mencionou que o que antes era uma tática de último recurso tornou-se uma prática comum.

Em dezembro de 2015, um juiz brasileiro ordenou que o aplicativo de serviço de mensagens instantâneas WhatsApp fosse bloqueado por 48 horas por causa da recusa em entregar dados de comunicação para investigações criminais em andamento. Esse não foi um caso isolado, pois duas outras ordens judiciais com o mesmo pedido de bloqueio seguiram-se em diferentes estados do país. Todas as ordens judiciais foram rapidamente revertidas, mas o assunto está pendente de decisão em dois casos constitucionais perante o Supremo Tribunal Federal do Brasil. Esses casos dizem respeito à extensão dos poderes dos juízes para ordenar que os serviços sejam bloqueados desta forma e ao argumento de que os dados são tecnicamente impossíveis de acessar por causa da criptografia de ponta-a-ponta usada pelo serviço de mensagens.

A ordem de bloqueio se aplicava às operadoras de telecomunicações, que a cumpriram, bloqueando o acesso no nível da infraestrutura. Usuários do aplicativo na Argentina e no Chile também foram afetados e não puderam acessar o serviço.⁴²³

Um especialista entrevistado mencionou uma liminar de um juiz eleitoral em Santa Catarina (Brasil) exigindo o bloqueio do Facebook por desobedecer a uma ordem judicial a respeito de um perfil supostamente falso que zombava de um prefeito.

423 Ver: <<https://www.nytimes.com/2015/12/18/world/americas/brazil-whatsapp-facebook.html>>. Acesso em: 10 mai 2021.

O Facebook teria argumentado que havia cumprido a ordem original e, portanto, a liminar não foi executada.⁴²⁴

Em outros casos, os juízes brasileiros solicitaram a remoção de aplicativos das lojas de aplicativos Google e Apple. No caso do aplicativo Secret, a justificativa era de que se tratava de um “santuário para o *cyberbullying*”.⁴²⁵ Em um caso semelhante, um juiz ordenou que a Microsoft removesse o aplicativo Cryptic dos telefones Windows, uma vez que ele oferecia um serviço de mensagens anônimas semelhante.⁴²⁶

Em outubro de 2019, coincidindo com os protestos em Quito sobre a publicação do decreto nº 883 do Presidente Lenin Moreno, que introduziu medidas de austeridade, certos serviços de compartilhamento de mensagens e multimídia como o Facebook e o WhatsApp não estavam disponíveis no Equador.⁴²⁷

Em 13 de abril de 2016, uma ordem judicial na cidade de Buenos Aires, na Argentina, exigiu que a plataforma de compartilhamento de carros Uber suspendesse suas atividades naquela cidade. Os provedores de serviços de Internet (PSIs) foram instruídos a encerrar o aplicativo móvel e a plataforma on-line da Uber.⁴²⁸ Não só o serviço da multinacional foi interrompido na cidade de Buenos Aires, mas áreas além da capital também foram afetadas.

Em 20 de dezembro de 2019, a Superintendência Colombiana de Indústria e Comércio se pronunciou contra o aplicativo de

424 Ver: <<https://olhardigital.com.br/noticia/juiz-manda-bloquear-facebook-em-todo-o-brasil-por-24-horas/62909>>. Acesso em: 10 mai 2021.

425 Ver: Internet & Jurisdiction Policy Network, “Blocking apps: Brazil orders Apple, Google to remove Secret from stores and devices”, Paris, 2014. Disponível em: <<https://www.internetjurisdiction.net/publications/retrospect#eyJ0byl6ljwMTktMTlifQ==>>>. Acesso em: 10 mai 2021.

426 Ver: <<https://www.sfgate.com/business/article/Brazil-wants-no-Secret-on-app-stores-5701537.php>>. Acesso em: 10 mai 2021.

427 Ver: <<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 Out 2019. Disponível em: <<https://www.elespectador.com/opinion/ecuador-restringe-redes-sociales-durante-las-protestas-de-esta-semana-columna-885505/>>. Acesso em: 10 mai 2021.

428 Ver: Internet & Jurisdiction Policy Network, “Argentina: Uber faces blocking order and investigation by the DPA”, Paris, 2016. Disponível em: <<https://www.internetjurisdiction.net/publications/retrospect#eyJ0byl6ljwMTktMTlifQ==>>>. Acesso em: 10 mai 2021.

compartilhamento de carros Uber, afirmando que a empresa havia violado as leis de concorrência e antitruste no país.⁴²⁹ A decisão instruiu os PSIs a bloquearem o acesso ao aplicativo. Os atores argumentaram que esta ordem violava o princípio da neutralidade da rede.⁴³⁰

Em 2019, foi noticiado que a República Bolivariana da Venezuela havia sofrido algum tipo de restrição de serviço que durou 171 horas e afetou mais particularmente o Twitter, WhatsApp, YouTube e Periscope.⁴³¹ Também foi amplamente divulgado que a enciclopédia on-line Wikipédia tinha sido bloqueada após o que se dizia ser uma “guerra de edição” sobre se Juan Guaidó ou Nicolás Maduro era o presidente legítimo do país.⁴³²

Em 14 de novembro de 2019, o Ministério dos Transportes e Comunicações do Peru emitiu o Decreto nº 035/2019,⁴³³ que o autoriza a bloquear unilateralmente e sem uma ordem judicial aplicativos de transporte que supostamente ofereçam serviços ilegais (inclusive bicicletas, táxis e patinetes elétricos). Foi noticiado que o Ministério instruiu PSIs a bloquearem determinados aplicativos de transporte e as lojas de aplicativos da Apple e Google foram instruídas a parar de exibi-los.⁴³⁴

5. PARALISAÇÕES DE SERVIÇO

As paralisações da Internet são uma disrupção deliberada do acesso à Internet ordenada por autoridades locais por curtos períodos, geralmente em situações em que há uma ameaça,

429 Ver: <<https://www.sic.gov.co/slider/superindustria-ordena-cese-de-la-prestacion-del-servicio-de-transporte-uber>>. Acesso em: 10 mai 2021.

430 Ver: <<https://www.elespectador.com/tecnologia/que-tiene-que-ver-la-neutralidad-de-red-y-la-orden-de-suspender-uber-en-colombia-articulo-898079>>

431 Ver: S. Woodhams and S. Migliano, *The Global Cost of Internet Shutdowns in 2019*, London, Top10VPN, 2020. Disponível em: <<https://www.top10vpn.com/cost-of-internet-shutdowns/>>. Acesso em: 10 mai 2021.

432 Ver: <<https://netblocks.org/reports/wikipedia-blocked-in-venezuela-as-internet-controls-tighten-XaAwR08M>>; A. Azpúrua e outros, "From the blocking of Wikipedia to social media: Venezuela's political crisis", *VesinFiltro*, Caracas, 29 de janeiro de 2019. Disponível em: <<https://vesinfiltr.com/noticias/report-jan-2019/>>. Acessos em: 10 mai 2021.

433 Ver: <<https://busquedas.elperuano.pe/normaslegales/decreto-supremo-que-precisa-disposiciones-sobre-el-servicio-decreto-supremo-n-035-2019-mtc-1826768-5/>>. Acesso em: 10 mai 2021.

434 Ver: <<https://www.accessnow.org/blocking-apps-by-ministerial-decree-enables-illegal-content-takedowns-in-peru/>>. Acesso em: 10 mai 2021.

real ou alegada, à ordem pública. Elas podem ter consequências desestabilizadoras, pois impedem não apenas a comunicação, mas também o acesso à informação. Sem acesso à Internet, a capacidade de uma população realizar muitas atividades diárias é obstruída. As pessoas se veem incapazes de se comunicar on-line, realizar pesquisas e até mesmo acessar serviços básicos, alguns deles públicos.

Com as transações financeiras migrando cada vez mais para a Internet, o acesso ao dinheiro e a diferentes recursos também pode ser interrompido. Consequências mais duradouras dizem respeito à confiança dos consumidores e à necessidade de as empresas migrarem para alternativas mais dispendiosas, tendo em conta a instabilidade da rede.

Os efeitos das paralisações da Internet não se limitam à dimensão doméstica. Uma série de serviços internacionais é impedida de funcionar, o que pode dificultar os planos de investir no país e até mesmo deixar os serviços completamente indisponíveis, pois as empresas podem decidir sair [do país]. As comunicações com o mundo exterior também são restritas. Os membros da família podem não conseguir entrar em contato uns com os outros. Isso pode ser particularmente preocupante, uma vez que as paralisações da Internet tendem a acontecer em situações de agitação civil ou política. Em vista de um passado no qual os desaparecimentos forçados eram uma prática não rara em muitos países da região, a incapacidade de contatar um ente querido pode ter um impacto social perturbador e consequências duradouras.

Na República Bolivariana da Venezuela, por exemplo, não só os aplicativos e os serviços de Internet foram bloqueados, mas também houve paralisações na Internet ou interrupção de conectividade em áreas inteiras por curtos períodos de tempo. Esses eventos tendem a ser associados a eventos políticos significativos. Em 2019, foi relatada a ocorrência de paralisações da Internet ou grandes interrupções na conectividade várias vezes, particularmente com o provedor de Internet estatal. Elas geralmente coincidem com atividades políticas de Juan Guaidó (Presidente da Assembleia Nacional da Venezuela e autoproclamado Presidente do país). Um exemplo notável de uma paralisação da Internet ocorreu durante uma reunião de Juan Guaidó com o Presidente da Colômbia na fronteira entre os dois países.

Da mesma forma, em 2018, em meio a protestos em diferentes partes da Nicarágua, foi noticiado que a Internet foi paralisada ou interrompida em diferentes áreas da capital, Manágua.⁴³⁵ O governo não reconheceu a paralisação da Internet, mas foi noticiado que havia uma correlação entre as ações tomadas pelas forças governamentais e as regiões onde a Internet foi interrompida.⁴³⁶

Instituições regionais de direitos humanos, como o Sistema Interamericano de Direitos Humanos, agindo através de seu Relator Especial para a Liberdade de Expressão, condenaram as paralisações e interrupções da Internet. Tais ações, quando tomadas por governos ou sob ordens governamentais, são vistas como “medidas extremas análogas à proibição de um jornal ou uma estação de rádio ou televisão. Tais bloqueios ou restrições não podem ser justificados, nem mesmo por razões de ordem pública ou de segurança nacional, e não podem ser usados como medidas de censura ou como mecanismos para impedir o acesso à informação da população.”⁴³⁷

O mesmo relator se uniu a outras organizações internacionais para lamentar “paralisações e interrupções arbitrárias para restringir o acesso às redes de telecomunicações e à Internet”.⁴³⁸ De acordo com algumas organizações da sociedade civil que monitoram o assunto, o número dessas medidas aumentou de um para 14 na região entre 2018 e 2019 em países que incluíam Nicarágua, República Bolivariana da Venezuela e Equador, apesar de tais condenações.⁴³⁹

435 Ver: <<https://netblocks.org/reports/nicaragua-regional-internet-disruptions-amid-protests-gdAmMvA9>>. Acesso em: 10 mai 2021.

436 Ver: <<https://www.accessnow.org/cms/assets/uploads/2019/07/KeepItOn-2018-Report.pdf>>. Acesso em: 10 mai 2021.

437 Ver: Relatoria Especial para a Liberdade de Expressão, “The office of the Special Rapporteur condemns closure of Radio Caracas Radio 750 AM, the censorship of television channels, restrictions on the Internet, and the arrest of journalists in Venezuela”, Comunicado à Imprensa, No. R116/19, Washington, DC, 15 Maio 2019. Disponível em: <<http://www.oas.org/en/iachr/expression/showarticle.asp?artid=1140&lid=1>>. Acesso em: 10 mai 2021.

438 Ver: Organization for Security and Cooperation in Europe (OSCE) and others, Twentieth Anniversary Joint Declaration: Challenges to Freedom of Expression in the Next Decade, Vienna, 2019. Disponível em: <<https://www.osce.org/representative-on-freedom-of-media/425282?download=true>>. Acesso em: 10 mai 2021.

439 Ver: <<https://www.accessnow.org/cms/assets/uploads/2020/02/KeepItOn-2019-report-1.pdf>>. Acesso em: 10 mai 2021.

6. LOCALIZAÇÃO FORÇADA DE DADOS

É da natureza dos dados serem facilmente transmissíveis e acessíveis em todo o mundo. No entanto, o fato de que eles são acessíveis em qualquer lugar, mas devem ser armazenados em algum lugar, torna difícil supervisionar os acordos de segurança para armazená-los e garantir o acesso contínuo a eles.

Vários países da região têm debatido e alguns exigiram o armazenamento local de dados. Os argumentos mais importantes para essa localização forçada de dados tendem a se relacionar com a segurança nacional, proteção nacional e acesso à execução da lei aos dados relevantes. A lógica é que os dados armazenados em servidores dentro do território sob a jurisdição do Estado estão mais prontamente disponíveis, proporcionando, assim, mais segurança e controle.

Esses possíveis benefícios devem ser ponderados em relação às limitações potenciais das transações de comércio eletrônico que dependem de prestadores de serviços financeiros estrangeiros, por exemplo, ou de empresas que operam através da nuvem ou mesmo de pequenas e médias empresas (PMEs), que não podem prontamente cumprir com os requisitos de localização para entrar em novos mercados. Podem também dificultar a criação de mercados digitais unificados e restringir a prestação de serviços transfronteiriços, com desvantagens particulares para as empresas que implementam uma estratégia centralizada.⁴⁴⁰

A localização dos dados não precisa ser explicitamente autorizada, mas pode ser um resultado *de facto* de uma política. Pode haver exigências que dificultem as transferências de dados transfronteiriças: isso tem sido chamado de localização condicional ou *soft*, em oposição à localização obrigatória.⁴⁴¹ Exigências sob as leis de privacidade que condicionam as transferências a um procedimento que garanta os direitos daqueles sobre os quais os dados são mantidos podem ser colocadas nessa categoria. A maioria da legislação de proteção de dados na América Latina e no Caribe tende a seguir o modelo europeu e exige ou uma decisão sobre a

440 Ver: Economic Commission for Latin America and the Caribbean (ECLAC), "Regional digital market: strategic aspects", Project Documents (LC/TS.2018/30), Santiago, 2018.

441 Ver: <<https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf>>. Acesso em: 10 mai 2021.

adequação, ou um procedimento, ou mecanismos que garantam a intenção da outra parte de cumprir com os mesmos padrões de proteção que são concedidos dentro do país. Isso não restringe diretamente o fluxo de dados, mas pode criar obstáculos.

Desde o escândalo das revelações de Snowden, em 2013, quando dados relativos a altos funcionários em muitos países foram acessados, vazados ou entregues à Agência Nacional de Segurança dos Estados Unidos,⁴⁴² vários governos da região consideraram a possibilidade de exigir que pelo menos alguns dados particularmente sensíveis fossem armazenados em servidores dentro de seu território.

Um exemplo muito significativo foi uma proposta de emenda ao chamado Marco Civil da Internet do Brasil, destinada a impor a localização de dados de uma forma muito geral.⁴⁴³ A emenda foi redigida da seguinte forma: "O Poder Executivo, por meio de Decreto, poderá obrigar os provedores de conexão e de aplicações de Internet previstos no art.11 que exerçam suas atividades de forma organizada, profissional e com finalidades econômicas a instalarem ou utilizarem estruturas de armazenamento, gerenciamento e disseminação de dados em território nacional, considerando o porte dos provedores, seu faturamento no Brasil e a amplitude da oferta do serviço ao público brasileiro".⁴⁴⁴

A proposta foi rejeitada, mas a lei aprovada determina que a lei brasileira é aplicável quando empresas, mesmo estrangeiras, oferecem serviços ao público brasileiro.⁴⁴⁵

442 Ver: G. Greenwald, "NSA collecting phone records of millions of Verizon customers daily", *The Guardian*, London, 6 Jun 2013. Disponível em: <<http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order>>. Acesso em: 10 mai 2021; G. Greenwald, R. Kaz and J. Casado, "EUA espionaram milhões de e-mails e ligações de brasileiros", *O Globo*, Brasília, 7 Dez 2013. Disponível em: <<http://oglobo.globo.com/mundo/eua-espionaram-milhoes-de-mails-ligacoes-de-brasileiros-8940934#ixzz2lEHZqYwh>>. Acesso em: 10 mai 2021.

443 Ver: <https://itsrio.org/wp-content/uploads/2018/02/v5_com-capa_pages_miolo_Brazil-Internet-Bill-of-Rights-A-closer-Look.pdf>. Acesso em: 10 mai 2021.; <<https://igarape.org.br/marcocivil/en/>>. Acesso em: 10 mai 2021; e Internet & Jurisdiction Policy Network, "Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction", Paris, 2014.

444 Ver: National Congress, "Substitutive Bill Proposal to Bill No. 2126 from 2011", 2013. Disponível em: <<http://infojustice.org/wp-content/uploads/2013/11/Marco-Civil-English-Translation-November-2013.pdf>>. Acesso em: 10 mai 2021.

445 Ver: <<https://www.camara.leg.br/noticias/429574-camara-aprova-projeto-do-marco-civil-da-internet/>>. Acesso em: 10 mai 2021.

Às vezes, não há legislação clara exigindo a localização de dados, no entanto, ainda são levantadas questões sobre a disponibilidade ou a conveniência de permitir que certos dados sejam armazenados em servidores em um território diferente. Um exemplo diz respeito aos dados judiciais. Em 21 de fevereiro de 2019, o Conselho Nacional de Justiça (CNJ) suspendeu o processo de aquisição de serviços de computação em nuvem da Microsoft por temer que os bancos de dados dos tribunais brasileiros mantivessem “informações sobre a vida, economia e sociedade do Brasil [...] que poderiam colocar em risco a segurança e os interesses nacionais do Brasil”.⁴⁴⁶ Embora não houvesse nenhuma ordem que exigisse o armazenamento de dados judiciais em território brasileiro, a suspensão teve a consequência indireta de bloquear o serviço por causa da localização transfronteiriça dos servidores.

Da mesma forma, o Ministério das Tecnologias de Informação e Comunicação da Colômbia expressou preocupação com os riscos de confiar no armazenamento em nuvem para a implantação de serviços básicos. Como medida de mitigação, a autoridade solicitou ao Gabinete do Conselho Geral que impusesse requisitos de localização de dados para a aquisição de serviços na nuvem por agências governamentais.⁴⁴⁷

No que diz respeito às autorizações indiretas de localização de dados, a Direção Nacional de Proteção de Dados Pessoais da Argentina emitiu a disposição nº 18/2015, que trata o armazenamento em nuvem como uma transferência internacional de dados, o que significa que os aplicativos executados em um serviço de computação em nuvem devem estar em conformidade com a Lei de Proteção de Dados Pessoais.⁴⁴⁸ Isso pode constituir uma barreira ao fluxo de dados e restringir esse tipo de aplicação. Ser obrigado a obter uma autorização expressa adicional do usuário também constitui um obstáculo. As aplicações que

446 Ver: <<https://www.conjur.com.br/dl/cnj-proibe-tj-sp-contratar-microsoft.pdf>>. Acesso em: 10 mai 2021. Esta decisão foi interpelada e confirmada em 25 de junho de 2019. Ver: <<https://www.conjur.com.br/dl/voto-schiefler-contrato-tj-sp-microsoft.pdf>>. Acesso em: 10 mai 2021.

447 Colombia, Basic Digital Services project. Ver: <<https://estrategia.gobiernoenlinea.gov.co/623/w3-article-18756.html>>. Acesso em: 10 mai 2021.

448 Ver: <<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>>. Acesso em: 10 mai 2021

utilizam servidores dentro do país têm uma vantagem sobre aquelas que utilizam computação em nuvem.

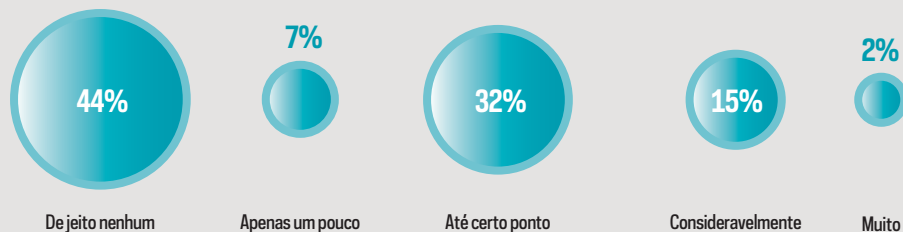
Noticiou-se que a República Bolivariana da Venezuela também fez exigências relativas à localização de dados. Elas parecem ser particularmente importantes no que diz respeito à infraestrutura de pagamento eletrônico e de processamento de pagamentos, uma vez que os dados de pagamento devem ser processados localmente.⁴⁴⁹

Na outra ponta do espectro, o México assinou um acordo com os Estados Unidos e Canadá (Acordo entre os Estados Unidos, México e Canadá (USMCA)), cujas cláusulas de comércio digital incluem uma proibição de qualquer legislação que exigisse que os servidores estivessem localizados dentro da jurisdição de um país membro.⁴⁵⁰

Mais de 70% dos entrevistados concordaram ou concordaram fortemente que a localização obrigatória dos dados restringiu o livre fluxo de informações e o comércio internacional.

INFOGRÁFICO 12

Você concorda com a afirmação de que a localização obrigatória de dados restringe o livre fluxo de informações e comércio internacional?



FONTE: INTERNET & JURISDICTION POLICY NETWORK AND ECONOMIC COMMISSION FOR LATIN AMERICA AND THE CARIBBEAN (ECLAC).

449 Ver: <<https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost>>. Acesso em: 10 mai 2021.

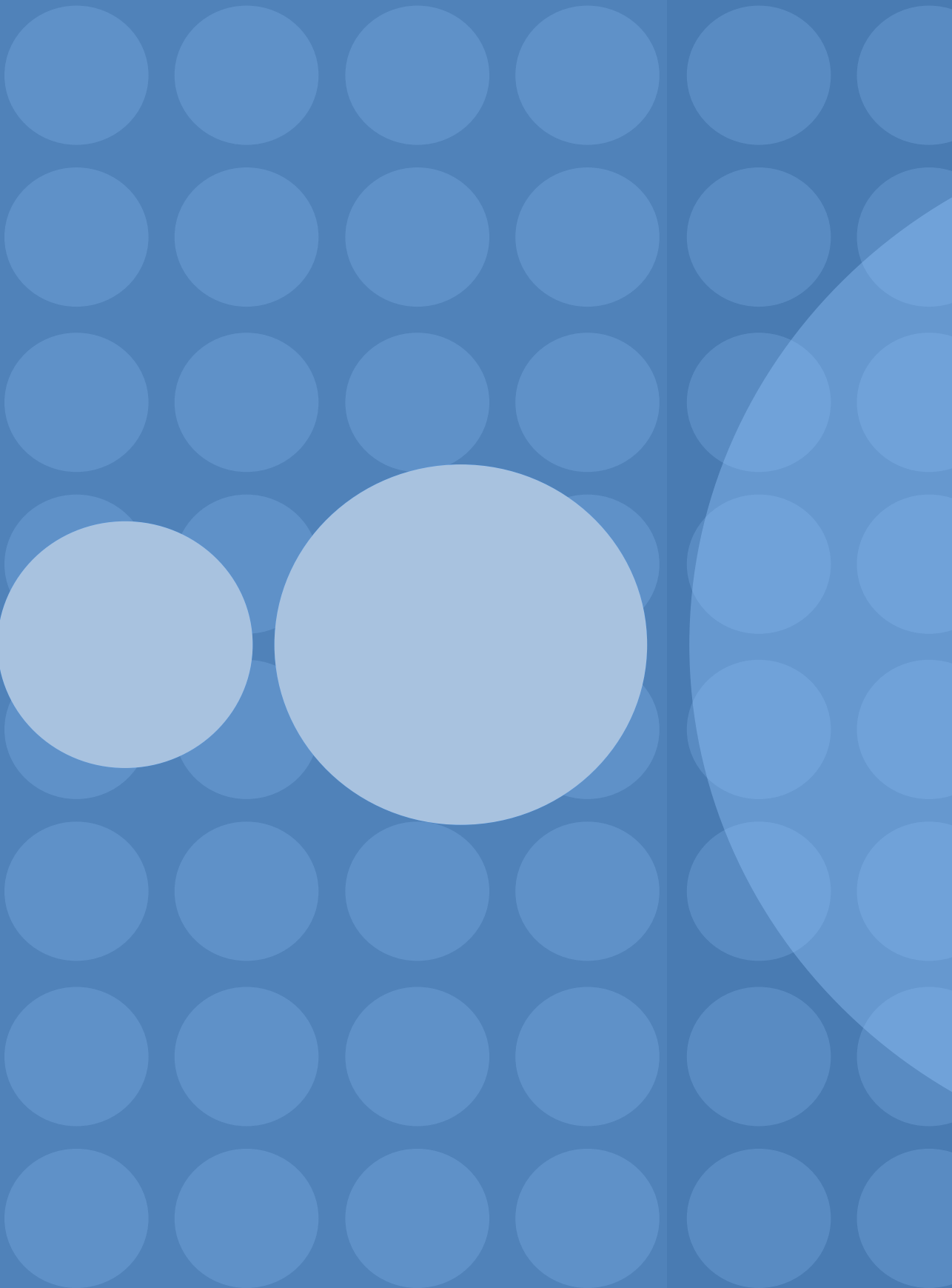
450 Acordo entre os Estados Unidos, México e Canadá (USMCA) (30 de novembro de 2018), artigo 19.12, localização das instalações de informática: "Nenhuma Parte exigirá que uma pessoa amparada use ou localize instalações de informática no território dessa Parte como condição para a realização de negócios nesse território". Ver: <<https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>>. Acesso em: 10 mai 2021.

Diversos atores mencionaram em seus comentários que é natural que uma economia global em rede tivesse dados circulando através das fronteiras sem obstáculos e que a localização obrigatória de dados restringe e concentra a Internet. Do ponto de vista técnico, um dos atores chamou a atenção para como a localização obrigatória de dados poderia impactar a velocidade da rede e a qualidade do serviço. Pode haver custos não só em termos de preços mais elevados, mas também no potencial de inovação. Um dos entrevistados expressou a preocupação de que tais obrigações restringiam a escala a que os atores menores poderiam aspirar, pois somente as empresas maiores poderiam arcar com os custos de infraestrutura para manter servidores em diferentes países.

Alguns dos atores apontaram que o armazenamento interno de dados poderia ser justificado em certos casos, quando envolverem informações confidenciais, dados pertencentes à administração pública e dados de segurança nacional. Houve algumas preocupações sobre a computação em nuvem e sugestões de que ela deveria ser objeto de regulação. Um ator observou, entretanto, que se tratava de cumprir as leis locais. Outro observou que nem todos os países tinham recursos e ferramentas para fazer cumprir as suas leis internas, especialmente quando a execução tem uma componente extraterritorial.

Deve-se notar que, apesar da tendência global, a localização voluntária de dados domésticos ocorre com mais frequência na América Latina e no Caribe. Há muitos fatores possíveis por trás disso, mas a percepção de controle e o desejo de melhor satisfazer as exigências locais podem ser os mais comuns. As escolhas nacionais e as políticas públicas podem favorecer indiretamente o armazenamento local de dados.

A coerência política necessária para construir um ecossistema digital regional próspero e integrado exige a mesma coerência nas definições que moldam o debate. A Internet foi criada há mais de 50 anos e a World Wide Web já comemorou seu trigésimo aniversário.



Glossário

Alguns conceitos se consolidaram ao longo dos anos, servindo como pontos de entrada consagrados para a discussão política, mas outros, que procuram captar os aspectos essenciais das novas tendências tecnológicas, ainda são muito controversos. Este pequeno glossário visa familiarizar os leitores com os conceitos-chave mencionados no Relatório, e assim ajudar a esclarecer as tendências e soluções jurídicas e tecnológicas mencionadas.

1. **Internet** é o sistema global de redes de computadores interconectados que depende do conjunto de protocolos da Internet (Transmission Control Protocol (TCP) / Internet Protocol (IP)) para a comunicação entre redes e dispositivos.
2. **IP (Internet Protocol)** é “o protocolo de comunicação subjacente à Internet, que permite que redes de dispositivos se comuniquem através de uma variedade de links físicos. Cada dispositivo ou serviço na Internet tem pelo menos um endereço IP que o identifica e distingue de outros dispositivos ou serviços na Internet.”⁴⁵¹
3. **A World Wide Web (WWW)** é um sistema de informação em que documentos e outros recursos estão interligados por hipertexto e são acessíveis através da Internet, fazendo com que “qualquer pessoa possa perambular, navegar e contribuir com facilidade”.⁴⁵²
4. **O Sistema de Nomes de Domínio**, mais conhecido pela nomenclatura em inglês, DNS (*Domain Name System*), é o sistema de nomenclatura que “ajuda os usuários a se orientar pela Internet”. Cada computador na Internet tem um endereço único, constituído por uma sequência de números (o endereço IP) e o DNS facilita o uso da Internet, permitindo o uso de uma sequência familiar de letras (o nome do domínio, como www.internetjurisdiction.net) em vez do endereço IP.⁴⁵³
5. **Jurisdição** tem diferentes significados no direito internacional. Neste relatório é usado para designar uma

451 Ver: <<https://www.icann.org/resources/en/glossary>>. Acesso em: 10 mai 2021.

452 Ver: <<https://www.w3.org/WWW/>>. Acesso em: 10 mai 2021.

453 Ver: <<https://www.icann.org/resources/en/glossary>>. Acesso em: 10 mai 2021.

autoridade ou um órgão legal formalmente constituído para ouvir e/ou tomar decisões relativas a um assunto específico. Geralmente está relacionado à ideia de território, mas os dois conceitos nem sempre estão associados. Isso é particularmente verdadeiro quando se trata de temas relacionados à Internet, devido à natureza transfronteiriça da Internet.⁴⁵⁴

Como já foi apontado no *Relatório de Status Global 2019* da Rede de Políticas Internet & Jurisdição :

É frequentemente estabelecida uma distinção entre jurisdição pessoal e jurisdição temática. A jurisdição pessoal diz respeito a um tribunal competente sobre uma determinada pessoa física ou jurídica. A jurisdição temática diz respeito à questão de saber se um tribunal é competente para julgar o tipo de litígio em causa.

Recentes litígios, no entanto, têm chamado a atenção para um terceiro tipo de jurisdição: 'alcance da jurisdição'. O alcance da jurisdição diz respeito ao âmbito geográfico das decisões proferidas por um tribunal com jurisdição pessoal e temática. Esta questão — que se sobrepõe ao direito dos recursos — tem surgido recentemente com os tribunais que realizam ordens globais de bloqueio, cancelamento de referência ou remoção de conteúdo.

Considerações sobre o alcance de jurisdição adequado são intrinsecamente ligadas à força da reivindicação pertinente de jurisdição pessoal, bem como à escolha da lei. Por exemplo, quando um tribunal tem uma reivindicação relativamente fraca de jurisdição pessoal, pode não estar em posição de optar por um alcance de jurisdição expandido. Um tribunal que opte por um alcance de jurisdição expandido também poderá não ter poder para aplicar apenas a sua própria lei, dado o impacto que a sua decisão terá no estrangeiro.⁴⁵⁵

454 Ver: D. Svantesson, *Solving the Internet Jurisdiction Puzzle*, Oxford, Oxford University Press, 2017.

455 Ver: <<https://www.internetjurisdiction.net/news/release-of-worlds-first-internet-jurisdiction-global-status-report>>. Acesso em: 10 mai 2021. [Versão em português do *Relatório de Status Global 2019*: <<https://cgi.br/publicacao/cadernos-cgi-br-internet-jurisdicao-6-1/>>]

6. **A escolha da lei [aplicável]** é a capacidade das partes contratuais de escolher qual lei regerá qualquer disputa entre as partes e a interpretação de um contrato. O Relatório abordou esse conceito quando se refere à cláusula de escolha da lei [aplicável] geralmente incluída nos termos de serviço e diretrizes de comunidade das plataformas internacionais da Internet. Em acordos on-line desse tipo, a “autonomia das partes” na escolha da lei é geralmente questionável, uma vez que o usuário é apresentado a termos contratuais unilateralmente predeterminados.
7. **Criptografia** é “o processo de codificação de dados para que possam ser interpretados somente pelos destinatários previstos”⁴⁵⁶ É usada como um importante recurso de segurança e privacidade por vários aplicativos populares, desde o comércio eletrônico, transações bancárias via Internet, mensagens instantâneas, até aplicativos de comunicação por vídeo.
8. **Blockchain** é “um registro de transações compartilhado entre as partes em uma rede, não controlado por uma única autoridade central”. O *blockchain* funciona como um livro-razão, uma vez que “registra e armazena todas as transações entre usuários em ordem cronológica. Em vez de uma autoridade controlar este livro-razão (como um banco), uma cópia idêntica dele é mantida por todos os usuários na rede, chamados de ‘nodos’”.⁴⁵⁷
9. **Tecnologia financeira** (abreviada como *fintech*) refere-se à tecnologia utilizada pelas entidades especializadas na prestação de serviços financeiros, principalmente através de plataformas on-line tecnologicamente habilitadas.⁴⁵⁸
10. **As sanboxes regulatórias** são espaços previstos para que as empresas experimentem a operação de produtos ou serviços inovadores de forma limitada com regras menos

456 Ver: <https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x25702>

457 Ver: <<https://www.oecd.org/finance/OECD-Blockchain-Primer.pdf>>. Acesso em: 10 mai 2021.

458 Para mais informações, ver: W. Magnuson, "Regulating fintech", College Station, Texas A&M University, 2018. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3027525>. Acesso em: 10 mai 2021.

rigorosas, sob a supervisão de uma autoridade reguladora governamental.⁴⁵⁹

11. Fake News é um termo usado na última década como um rótulo com forte conotação política para se referir a qualquer “informação falsa e enganosa, dissimulada e divulgada como notícia”.⁴⁶⁰ O debate acadêmico sobre um termo mais apropriado ainda está em curso, com autores sugerindo o uso de definições como “desinformação” ou “má informação”. A desinformação pode ser definida como informação falsa que é deliberadamente criada ou disseminada com o propósito expresso de causar danos. Os produtores de desinformação normalmente têm motivações políticas, financeiras, psicológicas ou sociais. A má informação, por outro lado, é informação falsa, mas não se destina a causar danos. Por exemplo, indivíduos que não sabem que uma informação é falsa podem espalhá-la nas mídias sociais em uma tentativa de ser útil.⁴⁶¹

12. Deepfake é um termo usado atualmente para descrever mídias produzidas com inteligência artificial. Ao processar elementos de arquivos de vídeo ou áudio existentes, esses elementos podem ser usados para criar novos conteúdos, nos quais os indivíduos falam palavras e realizam ações sem nenhuma base na realidade.⁴⁶² À medida que a tecnologia evolui, é provável que a *deepfake* seja cada vez mais utilizada em campanhas de desinformação.⁴⁶³

459 Ver: <<https://publications.iadb.org/publications/english/document/Regulatory-Sandboxes-in-Latin-America-and-the-Caribbean-for-the-FinTech-Ecosystem-and-the-Financial-System.pdf>>. Acesso em: 10 mai 2021.

460 Ver: <https://en.unesco.org/sites/default/files/journalism_fake_news_disinformation_print_friendly_0.pdf>. Acesso em: 10 mai 2021.

461 Ver: C. Wardle and H. Derakshan, Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making, Strasbourg, Council of Europe, 2017. Disponível em: <<https://rm.coe.int/information-disorder-toward-an-interdisciplinaryframework-for-research/168076277c>>. Acesso em: 10 mai 2021.

462 Ver: <https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x25702>. Acesso em: 10 mai 2021. Para mais informações, ver: Y. Li, M. Chang and S. Lyu, “In ictu oculi: exposing AI generated fake videos by detecting eye blinking”, 2018. Disponível em: <<https://arxiv.org/pdf/1806.02877.pdf>>. Acesso em: 10 mai 2021.

463 Para mais informações, ver: <<https://www.lawfareblog.com/deepfakes-looming-crisis-national-security-democracy-and-privacy>>. Acesso em: 10 mai 2021.

13. A Internet das Coisas é um sistema de dispositivos inter-relacionados capazes de coletar e transferir dados através de uma rede sem a necessidade de interação humana contínua. Em um cenário mais complexo, a Internet das Coisas pode ser definida como “uma rede autoconfigurável, adaptativa e complexa que interconecta ‘coisas’ à Internet através do uso de protocolos de comunicação padrão. As coisas interconectadas têm representação física ou virtual no mundo digital, capacidade de sensoriamento/atuação, características de programabilidade e são identificáveis de forma única. A representação contém informações que incluem a identidade, status, localização ou qualquer outra informação comercial, social ou privada relevante. As ‘coisas’ oferecem serviços, com ou sem intervenção humana, através da exploração de identificação única, captura e comunicação de dados e capacidade de atuação. O serviço é explorado através do uso de interfaces inteligentes e é disponibilizado em qualquer lugar, a qualquer momento e para qualquer coisa que leve em consideração a segurança”.⁴⁶⁴

464 Ver: <https://iot.ieee.org/images/files/pdf/IEEE_IoT_Towards_Definition_Internet_of_Things_Revision1_27MAY15.pdf>. Acesso em: 10 mai 2021.

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR