CADERNOS CGI.br Referências

6.1

Internet & Jurisdição: Relatório de status global 2019

Dan Jerker B. Svantesson

INTERNET & JURISDICTION POLICY NETWORK

cgi.br
Comitê Gestor da Internet no Brasil

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

Núcleo de Informação
e Coordenação do Ponto BR

6.1
CADERNOS CGI.br **Referências**

Internet & Jurisdição: Relatório de status global 2019

Dan Jerker B. Svantesson

Comitê Gestor da Internet no Brasil
Maio 2021

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

Assessoria Administrativa
Alessandra Assis, Jaqueline Gonçalves Xavier e Salete Matias

Assessoria Técnica às Atividades do CGI.br
Alexandre Costa Barbosa, Andressa Bones Flores, Beatriz Rossi Corrales, Bruna Toso de Alcântara, Carlos Francisco Cecconi, Everton Teles Rodrigues, Gabriela Nardy de Vasconcellos Leitão, Hendrick Pereira, Isadora Perez Alves Peixoto, Jean Carlos Ferreira dos Santos, Juliano Cappi, Luiza Affonso Ferreira Mesquita, Marcelo Oliveira, Rodrigo Cardoso Silva e Vinicius Wagner Oliveira Santos

Coordenação Executiva e Editorial
Carlos Francisco Cecconi e Jean Carlos Ferreira dos Santos

Produção Editorial
Caroline D'Avo (Comunicação NIC.br) e Carolina Carvalho (Comunicação NIC.br)

Projeto Gráfico e Ilustrações
Pilar Velloso

Produção desta publicação

Tradução
Ana Zuleika Pinheiro Machado

Revisão da Tradução
Luiza Brandão

Revisão Técnica e Preparação
Carlos Francisco Cecconi, Everton Teles Rodrigues, Isadora Perez Alves Peixoto, Jean Carlos Ferreira dos Santos e Vinicius Wagner Oliveira Santos

Diagramação
Milena Branco

Fotos
Istockphoto

Título original
Internet & Jurisdiction Global Status Report 2019. Disponível em: <https://www.internetjurisdiction.net/publications/>

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

Dados Internacionais de Catalogação na Publicação (CIP)
(Câmara Brasileira do Livro, SP, Brasil)

Internet & jurisdição : relatório de status global 2019 [livro eletrônico] / Dan Jerker B. Svantesson ; [editor] Núcleo de Informação e Coordenação do Ponto BR ; tradução Ana Zuleika Pinheiro Machado. -- 1. ed. -- São Paulo : Comitê Gestor da Internet no Brasil, 2020.
PDF
ISBN 978-65-86949-31-5
1.Ciberespaço 2. Direito e tecnologia 3. Governança da Internet 4. Internet - Leis e legislação 5. Transnacionalização 6. Regulação I. Svantesson, Dan Jerker B. II. BR, Núcleo de Informação e coordenação do Ponto. III. Machado, Ana Zuleika Pinheiro. IV. Título.

20-49567 CDD-004.6

Índices para catálogo sistemático:
1. Governança digital : Tecnologia da informação : Relatórios 004.6
Aline Graziele Benitez - Bibliotacária - CRB-1/3129

Comitê Gestor da Internet no Brasil (CGI.br)

Composição em Maio de 2021

Integrantes

Representantes do Setor Governamental
Cláudio Benedito Silva Furtado
Evaldo Ferreira Vilela
Franselmo Araújo Costa
Heitor Freire de Abreu
Igor Manhães Nazareth
Leonardo Euler de Morais
Luis Felipe Salin Monteiro
Marcio Nobre Migon
Maximiliano Salvadori Martinhão

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

Coordenador
Marcio Nobre Migon

Secretário Executivo
Hartmut Richard Glaser

Apresentação à Edição Brasileira

por LUIZA BRANDÃO
Diretora do IRIS - Instituto de Referência em Internet e Sociedade

O relatório de status global Internet e Jurisdição é o resultado de um esforço de pesquisa robusto da Rede de Políticas Internet & Jurisdição, para responder às demandas sobre os aspectos transfronteiriços desencadeados ou potencializados pela Internet. Nesse contexto, o relatório fornece evidências sobre os temas em disputa, especialmente no que diz respeito aos atuais desenhos institucionais e à estrutura global da Internet. Além disso, procura estabelecer as bases para o avanço das discussões a níveis global, regional e local.

A estrutura multissetorial da Rede de Políticas Internet & Jurisdição se reflete no mapeamento das tendências dominantes para as três trilhas de discussão: dados, conteúdo e domínios. O relatório oferece para cada uma delas um retrato atualizado de conceitos, limitações e dinâmicas inseridas no cotidiano de milhares de atores e instituições por todo o mundo. Além de compilar situações práticas e precedentes relevantes para o avanço desses temas, encontram-se aspectos teóricos e definições centrais para a construção de soluções efetivas e tecnicamente viáveis.

A Rede de Políticas Internet & Jurisdição busca viabilizar espaços comuns, pontos de partida para colaboração sobre aspectos que envolvem os países, culturas e pessoas interligados pela internet global, seus eventuais conflitos e distintos interesses. Conforme o relatório global, os desafios da transnacionalidade que marcam as interações digitais compreendem desde a lacuna de formação sobre os desafios jurisdicionais, a concentração

das discussões no Norte Global e ainda barreiras linguísticas impostas pela predominância da língua inglesa. Nesse sentido, a iniciativa do Comitê Gestor da Internet no Brasil (CGI.br) de tradução é fundamental para expandir a representatividade não apenas do Brasil, mas de outros países lusófonos, nas esferas de discussão e de tomada de decisão sobre Internet e jurisdição.

A complexidade, inclusive terminológica, dos temas sobre jurisdição que envolvem a Internet demandou um trabalho rigoroso e dedicado de toda a equipe responsável por este caderno. Cada termo, gráfico, nota ou item da versão brasileira do Relatório de Status Global foi cuidadosamente escolhido, para ir além de uma tradução do inglês. Na verdade, busca-se refletir a importância do Brasil - e do envolvimento de diversos setores do país - nas discussões aqui apresentadas.

Para aqueles que há algum tempo se dedicam à jurisdição de dados, conteúdo e domínios, a versão brasileira do relatório oferece a possibilidade de expandir os campos de diálogo. Para quem inaugura o contato com essas trilhas, é um convite para dedicação, cada vez mais necessária, aos aspectos transnacionais da Internet. Poder revisar a versão brasileira do relatório foi, então, uma grande responsabilidade, mas também uma enorme alegria, por compreender a importância dos temas de jurisdição para a Internet contemporânea e futura. Espero que a leitura siga com a compreensão de que, ao enfrentarmos problemas globais e compartilhados, são essas também as características das soluções que precisamos construir.

Este Relatório foi encomendado pelo Secretariado da Rede de Políticas Internet & Jurisdição e é de autoria do Professor Dr. Dan Jerker B. Svantesson.

O Relatório de Status Global 2019, 1ª Edição, foi publicado pelo Secretariado da Rede de Políticas Internet & Jurisdição .

O autor deste Relatório envidou seus melhores esforços para mapear o ecossistema atual e as tendências com base em pesquisas documentais, consultas e entrevistas com as partes interessadas.

No entanto, a exaustividade das informações não pode ser garantida, uma vez que este Relatório constitui a primeira linha de referência global sobre jurisdição e Internet.

Além disso, a análise do autor não reflete necessariamente a visão do Secretariado da Rede de Políticas Internet & Jurisdição, das partes interessadas envolvidas com o trabalho da Rede de Políticas Internet & Jurisdição, ou daqueles que forneceram apoio financeiro à execução do Relatório.

Rede de Políticas Internet & Jurisdição, França

O Secretariado da Rede de Políticas Internet & Jurisdição agradece o apoio financeiro e institucional das seguintes entidades que permitiram a elaboração do relatório:

- *Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH*
- *Federal Ministry for Economic Cooperation and Development, Germany*
- *Ministry of Foreign Affairs of Denmark*
- *Republic of Estonia, Ministry of Foreign Affairs*
- *European Commission*

Citação do relatório — *Relatório de Status Global 2019. Internet & Jurisdiction Global Status Report 2019.*

Prefácios

BERTRAND DE LA CHAPELLE
e PAUL FEHLINGER
Diretor Executivo e Diretor Executivo Adjunto da Rede de Políticas Internet & Jurisdição

Saber lidar com a coexistência de leis heterogêneas na Internet transfronteiriça é um dos maiores desafios políticos do século XXI digital. No entanto, soluções políticas escaláveis e coerentes não podem ser desenvolvidas sem uma compreensão abrangente de um ecossistema altamente complexo e dinâmico composto por múltiplos atores, iniciativas e tendências em todos os silos políticos da economia digital, dos direitos humanos e da segurança. Este foi um chamamento claro feito por mais de 200 dos principais atores de 40 países durante a 2ª Conferência Global da Rede de Políticas Internet & Jurisdição em 2018. No entanto, mesmo décadas após a ascensão da Internet comercial, ainda não existem dados consolidados a esse respeito. O Secretariado da Rede de Políticas Internet & Jurisdição decidiu lançar o primeiro Relatório de Status Global: Internet e Jurisdição do mundo para fornecer este mapeamento e análise indispensáveis. Com base na experiência única dos principais atores envolvidos no trabalho de desenvolvimento de políticas da Rede de Políticas Internet & Jurisdição, esta edição inaugural do Relatório de Status Global fornece um primeiro retrato e uma linha de base. Este Relatório deve ser entendido como um importante conjunto de dados que nos permitirá proceder coletivamente e preencher as lacunas em futuras edições globais e regionais. Para este esforço ambicioso e crucial, convidamos todos os atores a contribuir com os seus conhecimentos e a compartilhar seus dados.

O esclarecimento da forma como as leis nacionais vigentes se aplicam ao ciberespaço e o desenvolvimento de novos regimes equilibrados para combater abusos viabilizarão a economia digital a proteger os direitos humanos e determinarão o formato da economia digital emergente. Para preservar o caráter aberto e transfronteiriço da Internet, é necessário estabelecer a coerência das políticas e a interoperabilidade jurídica entre múltiplos regimes. Isto requer comunicação, coordenação e, em última análise, cooperação entre todos os atores.

No entanto, a elaboração de políticas sólidas deve basear-se em evidências e dados confiáveis. A coerência das políticas em um nível transnacional só pode ser alcançada através de uma compreensão partilhada das questões em causa e da sensibilização para as várias iniciativas. A disponibilidade desta visão global e da análise das tendências e iniciativas traduzirá a natureza altamente complexa e muitas vezes técnica das questões substantivas para os tomadores de decisão.

Este Relatório representa o primeiro passo de um esforço contínuo do Secretariado da Rede de Políticas Internet & Jurisdição para tornar estas informações essenciais acessíveis a todos os atores, para ajudá-los a enfrentar coletivamente alguns dos desafios globais mais urgentes dos nossos tempos.

Estamos muito felizes com o lançamento desta edição completa do Relatório de Status Global: Internet e Jurisdição por ocasião do 14º Fórum de Governança da Internet, em Berlim, Alemanha. Gostaríamos de expressar a nossa gratidão aos pioneiros deste novo esforço global para fomentar a coerência das políticas através de capacitações e de inovação política baseada em evidências: os atores da Rede de Políticas Internet & Jurisdição, o autor, Professor Dan Svantesson, bem como a Alemanha, Dinamarca, Estônia e a Comissão Europeia, que tornam possível este importante esforço.

DRA. MARIA FLACHSBARTH
Secretária de Estado Parlamentar junto ao Ministério Federal para a Cooperação e o Desenvolvimento Econômico da Alemanha

A World Wide Web, a Internet como a maioria das pessoas a conhece, tem apenas 30 anos de idade. Neste curto período de tempo, a distinção entre o mundo on-line e off-line tornou-se sem sentido. Estamos on-line todos os dias. Usamos a Internet para receber notícias. Nós nos comunicamos com familiares, amigos e colegas de trabalho. Nossas casas e eletrodomésticos estão conectados através da Internet das Coisas. Encomendamos serviços e interagimos com autoridades locais e nacionais. Nossos celulares e laptops facilitam o acesso à Internet em casa ou em qualquer lugar.

A Internet aumentou a conectividade global, avançou nossas sociedades e economias, e ainda oferece enormes oportunidades. No entanto, não devemos esquecer que quase metade da população mundial não tem acesso à Internet. As mulheres, em especial, enfrentam desigualdades no que diz respeito ao acesso à Internet e à participação no setor das TI. O potencial da Internet ainda precisa ser destravado em áreas remotas e em países menos desenvolvidos. Esta é uma tarefa de extrema importância, e precisamos ter isso em mente quando falamos sobre o futuro e a evolução da Internet. Além disso, nem todos os países e atores têm sido capazes de contribuir igualmente para discussões sobre jurisdição e regulamentação da Internet. A Internet também estabeleceu novos desafios. A liberdade de expressão on-line tem de ser protegida e precisamos encontrar formas de lidar com o discurso de ódio, manipulação e desinformação. A segurança de dados e o direito à privacidade são da maior importância e exigimos uma defesa contra crescentes ameaças cibernéticas. Eventualmente, precisamos ter uma In-

ternet segura, mas aberta e confiável, que beneficie as pessoas e empresas em todo o mundo.

A Alemanha defende a neutralidade da rede, a liberdade de expressão e o acesso à Internet para todos. O Ministério Federal para a Cooperação e o Desenvolvimento Econômico coopera estreitamente com os países em desenvolvimento nos processos de digitalização e promove a inclusão dos países em desenvolvimento em todas as discussões relevantes. É por isso que apoiamos este primeiro Relatório de Status Global sobre Internet e Jurisdição.

Desejamos que o debate em curso sobre os desafios jurisdicionais enfrentados pela Internet aberta seja inclusivo, aberto a todas as regiões do mundo, e envolva todos os atores.

CASPER KLYNGE
Embaixador Tecnológico da Dinamarca
Ministério das Relações Exteriores da Dinamarca

A digitalização e a tecnologia definem parâmetros para a evolução das nossas sociedades no século XXI. Por um lado, a tecnologia tem potencial para retirar as pessoas da pobreza, melhorar os cuidados de saúde e outros setores-chave da sociedade, e impulsionar o crescimento econômico. Por outro lado, a tecnologia poderia exacerbar as desigualdades, minar os direitos fundamentais e corroer a confiança pública nas instituições democráticas. Para colher os benefícios e minimizar os riscos do desenvolvimento tecnológico, é necessária uma abordagem equilibrada. Isto exige o quadro político adequado. Precisamos, portanto, identificar os desafios que a tecnologia apresenta à governança, tanto no nível nacional como internacional. As tecnologias transfronteiriças, como a economia da Internet e das plataformas, trazem uma série desses desafios.

Por conseguinte, a Dinamarca congratula-se com o esforço da Internet & Jurisdiction Policy Network para mapear as principais tendências da sociedade digital. O Relatório de Status Global: Internet e Jurisdição é uma contribuição oportuna para uma melhor compreensão da era digital, um passo importante para nos proporcionar uma base sólida para o diálogo e cooperação internacionais construtivos. Há aproximadamente dois anos, o governo dinamarquês decidiu elevar a tecnologia e a digitalização a uma prioridade estratégica de política externa — através da TechPlomacy-initiative — nomeou o primeiro Embaixador de Tecnologia e da Digitalização da Dinamarca ("Embaixador Tecnológico"), e, na verdade, do mundo, e criou uma representação dedicada à tecnologia. A iniciativa é uma resposta à importância crescente que a tecnologia, a digita-

lização e a indústria têm para os indivíduos, as sociedades e as relações internacionais — e à necessidade de impulsionar o diálogo entre a indústria tecnológica, governos e organizações multilaterais. Estamos trabalhando no sentido de uma cooperação mais forte com vários atores para proteger valores e instituições fundamentais e promover uma abordagem de desenvolvimento tecnológico centrada no ser humano. Em suma, uma abordagem equilibrada em que os entes públicos e privados assumam a responsabilidade. Reconhecer a necessidade urgente de normas comuns e a preservação de uma ordem internacional baseada em regras para a era digital. Assegurar a regulamentação correta e proteger a democracia, os direitos humanos e o Estado democrático de direito.

A digitalização é de natureza internacional e transfronteiriça, criando uma série de novos desafios jurídicos, entre outros, às nossas sociedades e ao Estado democrático de direito na era digital — uma era que, pela mesma razão, exige mais, não menos, cooperação internacional.

HELI TIIRMAA-KLAAR
Embaixadora Extraordinária para Diplomacia Cibernética
Ministério de Relações Exteriores da Estônia

Em 2018, o mundo atingiu um marco importante, já que mais de 50% de sua população passou a ter acesso à Internet. Como demonstrado no Relatório de Status Global sobre Internet e Jurisdição, a Internet já revolucionou a forma como pessoas, empresas e governos interagem. O modelo de governança multissetorial da Internet proporcionou uma plataforma para um enorme desenvolvimento econômico e progresso político globalmente. Para que esse progresso continue, é fundamental que o modelo multissetorial responsável da Internet seja mantido, mesmo que a crescente interdependência no ciberespaço pareça criar desafios sem precedentes. Embora o ciberespaço aberto, livre e acessível seja, para muitos Estados, parte de sua identidade democrática, para alguns, a governança da Internet pode ser vista como mais uma ferramenta para executar o controle estatal. A Estônia sempre apoiou a Internet aberta e interoperável. O acesso não discriminatório e a acessibilidade da Internet são fundamentais para permitir e promover o direito à liberdade de expressão, reunião e associação. O acesso a fontes de meios de comunicação independentes, plataformas de redes sociais e uma Internet gratuita tornou-se parte integrante da boa governança e da sociedade democrática. Embora deva ser claro que a legislação internacional em vigor se aplica ao ciberespaço, é necessário desenvolver e implementar normas de comportamento estatal responsável para este campo dinâmico. Isto exige, evidentemente, comunicação, coordenação e cooperação entre todos os atores.

O Relatório de Status Global: Internet e Jurisdição concentra-se em tendências abrangentes e atuais, bem como em abordagens jurídicas e técnicas, e cria ligações entre diferentes iniciativas globais e regionais. Um dos incentivos para a elaboração deste relatório foi viabilizar melhor acesso a informações relevantes, em especial à legislação em vigor e à sua aplicação. No entanto, há ainda uma clara necessidade de uma coordenação significativa entre os múltiplos intervenientes da área e as iniciativas existentes. O Relatório fornece uma visão geral e documentação abrangentes das tendências passadas, atuais e emergentes. Contribui igualmente para o debate global sobre possíveis soluções para os principais desafios legais da política transfronteiriça. Como copatrocinadora do relatório, a Estônia espera criar pontes entre as diferentes iniciativas e jurisdições. Estamos certos de que este Relatório contribuirá para uma melhor coordenação entre as diferentes partes interessadas a fim de desenvolver e proteger uma Internet interoperável e segura para a comunidade multissetorial global.

PEARSE O'DONOHUE
Diretor para Redes Futuras
DG CONNECT, Comissão Europeia

A Internet já está em nossas vidas há décadas. Ela passou a ser um recurso crítico para a transformação de nossas economias e sociedades e a sua importância continuará a crescer. Portanto, é nossa responsabilidade garantir que a Internet continue sendo um ambiente centrado no ser humano, seguro e confiável.

A estratégia da UE para o mercado único digital avançou muito a este respeito. Deu aos cidadãos, às empresas e às administrações públicas europeias novas oportunidades de trabalho e de vida seguros e inclusivos, proporcionando um acesso equitativo aos bens, conteúdos e serviços digitais. A confiança digital tem sido reforçada pela aplicação do Regulamento Geral sobre a Proteção de Dados (GDPR, na sigla em inglês) e melhoria da resiliência da UE a incidentes cibernéticos através de um novo regime de segurança cibernética. Por meio do Mercado Único Digital (DSM, na sigla em inglês), a UE proporcionou benefícios concretos e tangíveis aos cidadãos europeus, mas também desempenhou um papel de liderança na definição de normas políticas de referência para a era digital.

A Internet é, naturalmente, um fenômeno global, e é nossa ambição impulsionar o debate político global na Internet com nossos parceiros e todos os atores que compartilham nossos valores, como parte da abordagem multissetorial de governança da Internet. Este debate, tradicionalmente centrado nas infraestruturas centrais da Internet, tem de ser expandido de modo a abranger questões como a governança da Inteligência Artificial, o livre fluxo de dados e a confiança na Internet. São igualmente importantes questões jurisdicionais, tais como a responsabilização no caso dos serviços oferecidos através da

Internet, a escolha da lei em eventual litígio ou o reconhecimento das legislações nacionais e o seu cumprimento. Ao abordar estas questões, não devemos permitir que as acusações de protecionismo desviem nosso propósito de manter um elevado nível de proteção ao indivíduo. O Relatório de Status Global: Internet e Jurisdição de 2019 oferece uma visão geral útil das tendências abrangentes que afetam a natureza transfronteiriça da Internet. Saudamos o esforço de acompanhar as iniciativas legislativas globais, as medidas não vinculantes (*soft law*) e melhores práticas na Internet. Este exercício de mapeamento certamente enriquecerá o debate sobre governança da Internet e estimulará a comunidade multissetorial a encontrar soluções para problemas jurisdicionais on-line. Esta é uma discussão importante se quisermos manter uma Internet global.

Sumário

Agradecimentos

Este Relatório foi encomendado pelo Secretariado da Rede de Políticas Internet & Jurisdição.
A produção deste Relatório foi possível graças ao apoio financeiro prestado pela Corporação Alemã de Cooperação Internacional (GIZ) em nome do Ministério Federal de Cooperação e Desenvolvimento Econômico da Alemanha (BMZ), do Ministério de Relações Exteriores da Dinamarca, do Ministério de Relações Exteriores da Estônia e ao apoio institucional prestado pela Comissão Europeia, Direção-Geral para Redes de Comunicações, Conteúdo e Tecnologia (DG CONNECT).

Equipe de autoria:

Autor:

Professor Dr. Dan Jerker B. Svantesson
Bond University
Gold Coast
Austrália

Assistência à pesquisa e entrevistas:

Rebecca Azzopardi
Doutoranda
Bond University
Gold Coast
Austrália

Coordenação do projeto:

Martin Hullin
Diretor de Operações e Parcerias
Secretariado da Internet & Jurisdiction
Policy Network

Equipe do projeto:

Bertrand de la Chapelle
Diretor Executivo
Secretariado da Internet & Jurisdiction
Policy Network
Paul Fehlinger
Diretor-Executivo Adjunto
Secretariado da Internet & Jurisdiction
Policy Network
Xavier Guyot de Camy
Gestor de Políticas
Secretariado da Internet & Jurisdiction
Policy Network
Ajith Francis
Encarregado de Políticas
Secretariado da Internet & Jurisdiction
Policy Network

Produção:

Secretariado da Internet & Jurisdiction Policy Network

Edição:

Emma Dann, Bond University, Gold Coast, Austrália

Design e layout:

Formas do Possível Creative Studio, Lisboa, Portugal

O Secretariado agradece imensamente o tempo e a contribuição de todos os participantes e entrevistados. Sem os seus valiosos conhecimentos, este relatório não poderia ter sido produzido.

Waiswa Abudu Sallam
Head Legal Affairs
Communications Commission
Uganda

Benedict Addis
Chair
Registrar of Last Resort (RoLR)
Reino Unido

Fiona Alexander
Associate Administrator for International Affairs
Department of Commerce
National Telecommunications and Information Administration (NTIA)
Estados Unidos

Chinmayi Arun
Assistant Professor of Law
National Law University Delhi
Índia

Karen Audcent
Senior Counsel
Department of Justice
Canadá

Greg Aaron
Vice-President
iThreat
Estados Unidos

Halefom Abraha
Research Officer
Information Policy and Governance
University of Malta
Malta

Bakhtiyor Avezdjanov
Program Officer
Columbia University, Global Freedom of Expression
Estados Unidos

Adriele Ayres Britto
Senior Counsel
Ayres Britto Consultoria Jurídica e Advocacia
Brasil

Kerry Ann Barrett
Cybersecurity Policy Specialist
Organization of American States (OAS)
Estados Unidos

Elizabeth Behsudi
Former General Counsel
Public Interest Registry (PIR)
Estados Unidos

Tijani Ben Jemaa
Executive Director
Fédération Méditerranéenne desbAssociations d'Internet (FMAI)
Tunísia

Eduardo Bertoni
Director
National Access to Public Information Agency
Argentina

Theo Bertram
Public Policy Manager
Google
Estados Unidos

Aparajita Bhatt
Assistant Professor
National Law University Delhi
Índia

Ellen Blackler
Vice President Global Public Policy
The Walt Disney Company
Estados Unidos

Marko Bošnjak
Judge
European Court of Human Rights (ECHR)
França

Maarten Botterman
Board Director
The Internet Corporation for Assigned Names and Numbers (ICANN)
Holanda

Andrew Bridges
Partner
Fenwick & West LLP
Estados Unidos

Lisl Brunner
Director
Global Public Policy
AT&T
Estados Unidos

Andre Caissy
Senior Policy Analyst
Canada, Department of Canadian Heritage
Canadá

Brent Carey
Domain Name Commissioner
Domain Name Commission for .nz
Nova Zelândia

Jordan Carter
Chief Executive
InternetNZ
Nova Zelândia

Mark Carvell
International Online Policy Senior Adviser
Department for Digital Culture, Media and Sport (DCMS)
Reino Unido

Adriana Castro Pinzón
Deputy Director
Business Law Department
Universidad Externado de Colombia
Colômbia

Eileen Berenice Cejas
Communications Director
Digital Grassroots
Argentina

Angelica Chinchilla-Medina
Director
Ministry of Science, Technology and Telecommunications
Costa Rica

Vivian Choy
Crime and Intelligence Analyst
Canada, Calgary Police Service
Canadá

Jose Clastornik
Executive Director
AGESIC - National eGovernment and Information Society Agency
Office of the President of Uruguay

Alexander Corbeil
Senior Research Analyst
Canada, Public Safety
Canadá

Alexander Corbeil
Research Advisor
Canada, Public Safety
Canadá

Jennifer Daskal
Associate Professor
American University
Washington College of Law
Estados Unidos

Bertrand De la Chapelle
Executive Director
Secretariat of the Internet & Jurisdiction Policy Network
França

Sissi Maribel De La Peña
Director of e-business and international organizations
ALAI - Asociación Latinoamericana de Internet
México

Jacques De Werra
Professor
University of Geneva
Suíça

Agustina Del Campo
Director
Center for Studies on Freedom of Expression and Access to Information (CELE)
Argentina

Steven Delbianco
President
NetChoice
Estados Unidos

Fernanda Domingos
Federal Prosecutor
Federal Prosecution Service
Brasil

Valensiya Dresvyannikova
Policy and Research Officer
International Federation of Library Associations and Institutions (IFLA)
Reino Unido

Salomé Eggler
Advisor
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
Alemanha

Shruttima Ehersa
Associate
Inttl Advocare
Índia

Brendan Eiffe
Head of Mutual Legal Assistance Division Department of Justice and Equality
Irlanda

Miriam Estrin
Policy Manager
Google
Reino Unido

Paul Fehlinger
Deputy Executive Director
Secretariat of the Internet & Jurisdiction Policy Network
França

Benedicto Fonseca Filho
Ambassador
Ministry of Foreign Affairs
Brasil

Nils Finder
Referent, Governance & Markets, Government Affairs
Siemens AG
Alemanha

Julia Fossi
Expert Advisor
eSafety Commissioner
Austrália

Gary Fowlie
Advisor
Geeks Without Frontiers
Estados Unidos

Jothan Frakes
Executive Director
The Domain Name Association
Estados Unidos

Eric Freyssinet
Chief Digital Strategy Officer
Gendarmerie nationale
França

Giancarlo Frosio
Senior Lecturer
University of Strasbourg
CEIPI
França

Lise Fuhr
Director General
European Telecommunications Network Operators' Association (ETNO)
Bélgica

Chawki Gaddes
Président
Instance Nationale de Protection des Données Personnelles (INPDP)
Tunísia

Michael Geist
Canada Research Chair in Internet and E-commerce Law
University of Ottawa
Canadá

Jan Gerlach
Senior Public Policy Manager
Wikimedia Foundation
Estados Unidos

Lorna Gillies
Senior Lecturer
Strathclyde University
Reino Unido

Grace Githaiga
Co-convenor
Kenya ICT Action Network (KICTANet)
Quênia

Hartmut Glaser
Executive Secretary
Brazilian Internet Steering Committee/CGI.br
Brasil

Tonei Glavinic
Director of Operations
Dangerous Speech Project
Espanha

Joaquín Gonzalez-Casanova
Director General for International Affairs
Instituto Nacional de Transparencia Acceso a la Información y Protección de Datos Personales
México

Luca Grandi
Legal Counsel
Ferrero
Luxemburgo

Robyn Greene
Privacy Policy Manager
Facebook
Estados Unidos

Nicole Gregory
Head Data and Online Harms, Foreign & Commonwealth Office
Reino Unido

Robert Guerra
CEO
Privaterra
Canadá

Devesh Gupta
Manager
Reliance Industries Limited (RIL)
Índia

Hiroki Habuka
Deputy Director, Digital Economy Division
Ministry of Economy, Trade and Industry (METI)
Japão

Statton Hammock
Vice-President
MarkMonitor
Estados Unidos

Sara Harrington
Vice President Legal
Chen Zuckerberg Foundation
Estados Unidos

Byron Holland
President and CEO
Canadian Internet Registration Authority (CIRA)
Canadá

Daniel Holznagel
Legal Officer
Federal Ministry of Justice and Consumer Protection
Alemanha

Martin Husovec
Assistant Professor
Tilburg University
Holanda

Erick Iriarte
Senior Partner
Iriarte & Associates
Peru

Manal Ismail
Executive Director
International Technical Coordination National Telecom Regulatory Authority (NTRA)
Egito

Pavlina Ittelson
Program Manager
DiploFoundation
Suíça

Sunali Jayasuriya
Legal Officer
Information and Communication Technology (ICT) Agency
Sri Lanka

Tarek Kamel
Senior Advisor
The Internet Corporation for Assigned Names and Numbers (ICANN)
Egito

Seb Kay
Policy Adviser
Foreign & Commonwealth Office
Reino Unido

Daniel Keck
Adviser
Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ)
Alemanha

Daphne Keller
Director of Intermediary Liability
Stanford Law School Center for Internet and Society
Estados Unidos

Gail Kent
Global Public Policy Lead on Law Enforcement and Surveillance
Facebook
Estados Unidos

Tshoganetso Kepaletswe
Chief Technology Officer
Communications Regulatory Authority
Botsuana

Matthias Kettemann
Co-Head
Research Focus Internet & Society
University of Frankfurt/Main
Alemanha

Gayatri Khandhadai
Asia Policy Regional Coordinator
Association for Progressive Communications (APC)
Índia

Jan Kleijssen
Director of Information Society and Action against Crime
Council of Europe
França

Wolfgang Kleinwächter
Professor
Global Commission on the Stability on Cyberspace (GCSC)
Alemanha

Casper Klynge
Tech Ambassador
Ministry of Foreign Affairs
Dinamarca

Monika Kopcheva
Political Administrator
Council of the EU
Brussels

Dominique Lazanski
Director
Public Policy and International Relations
GSMA
Reino Unido

Emmanuelle Legrand
Legal and Policy Officer
European Commission (EC)
Bélgica

May-Ann Lim
Executive Director
Asia Cloud Computing Association and Managing Director, TRPC Pte Ltd
Singapura

Rebecca Mackinnon
Director
Ranking Digital Rights
New America
Estados Unidos

Dinesh Mandagere
Managing Consultant
Wipro
Índia

Giacomo Mazzone
Head of Institutional Relations
European Broadcasting Union (EBU)
Suíça

Corynne McSherry
Legal Director
Electronic Frontier Foundation (EFF)
Estados Unidos

Christine Mackenzie
President
International Federation of Library Associations and Institutions (IFLA)
Holanda

Patricia Miranda
Senior Counsel
World Bank
Estados Unidos

Roudabeh Moghaddam
Executive Secretary to the Steering Committee
Child Dignity Alliance
Reino Unido

Doris Möller
Counsel
Association of German Chambers of Industry and Commerce
Alemanha

Francesca Musiani
Associate Research Professor (eq.)
Centre Nationale de la Recherche Scientifique (CNRS)
França

Vivek Narayanadas
Data Protection Officer
Shopify
Canadá

Victoria Nash
Senior Policy Fellow
University of Oxford
Reino Unido

Gonzalo Navarro
Chief Executive Officer
Latin American Internet Association (ALAI)
Chile

Paul Nemitz
Principal Adviser
European Commission (EC)
Bélgica

Michele Neylon
Chief Executive Officer
Blacknight Internet Solutions Ltd
Irlanda

Gregory Nojeim
Director
Freedom, Security & Technology Project
Center for Democracy & Technology (CDT)
Estados Unidos

Elliot Noss
Chief Executive Officer
Tucows
Canadá

Michael Oghia
Advocacy & Engagement Manager
Global Forum for Media Development
Sérvia

Seun Ojedeji
Chief Network Engineer
Federal University Oye-Ekiti
Nigéria

Phol Edward Paucar Aguirre
Universidad del Pacífico
Peru

Elena Perotti
Executive Director Public Affairs and Media Policy
World Association of Newspapers and News Publishers (WAN-IFRA)
França

Christian Perrone
Google Public Policy Fellow
Institute for Technology and Society of Rio de Janeiro (ITS Rio)
Brasil

Nick Pickles
Senior Public Policy Strategist
Twitter
Estados Unidos

Jason Pielemeier
Policy Director
Global Network Initiative (GNI)
Estados Unidos

Marc Porret
Legal and Criminal Justice Coordinator
United Nations Counter-Terrorism Committee Executive Directorate (UNCTED)
Estados Unidos

Frederic Potier
National Delegate
Délégation Interministérielle à la Lutte Contre le Racisme l'Antisémitisme et la Haine anti-LGBT (DILCRAH)
França

Rosanna Rafel-Rix
Digital Media Manager
Community Security Trust
Reino Unido

Rod Rasmussen
Principal
R2 Cyber
Estados Unidos

Chris Riley
Director
Public Policy
Mozilla
Estados Unidos

Beatriz Rodríguez
Adviser
Unidad Reguladora y de Control de Datos Personales (URCDP)
Uruguai

Jorge Rodríguez-Zapata
Justice
Supreme Court
Espanha

Elettra Ronchi
Head of Unit
Organization for Economic Co-operation and Development (OECD)
França

Kostas Rossoglou
Head of EU Public Policy
Yelp
Bélgica

Alexandre Roure
Senior Manager
Public Policy, Computer & Communication Industry Associations (CCIA)
Estados Unidos

Stefan Saatmann
Global Cybersecurity Policy Coordinator
Siemens AG
Alemanha

Nicolás Schubert
Digital Economy Coordinator
General Directorate of International Economic Affairs
Ministry of Foreign Affairs
Chile

Lori Schulman
Senior Director
Internet Policy
International Trademark Association
Estados Unidos

Jörg Schweiger
Chief Executive Officer
DENIC eG
Alemanha

Amy Shepherd
Legal and Policy Officer
Open Rights Group
Reino Unido

Toussi Simone
Researcher
South Lights 2030
Camarões

Tim Smith
General Manager
Canadian International Pharmacy Association
Canadá

Alissa Starzak
Head of Public Policy
Cloudflare
Estados Unidos

Christoph Steck
Director
Public Policy
Telefonica
Espanha

Blair Stewart
Assistant Commissioner
Office of the Privacy Commissioner
Nova Zelândia

Peter Swire
Professor
Georgia Tech Scheller College of Business
Estados Unidos

Ian Toon
Digital Examiner
London Metropolitan Police
Reino Unido

Stanislaw Tosza
Assistant Professor
Utrecht University
Holanda

Takahiko Toyama
Director for Information Policy Planning
Ministry of Economy, Trade and Industry (METI)
Japão

Lee Tuthill
Counsellor
World Trade Organisation (WTO)
Suíça

Kimmo Ulkuniemi
Chief Superintendent
National Police Board
Finlândia

Peter Van Roste
General Manager
CENTR
Bélgica

Mark Villiger
Retired Judge
Formerly Section President
European Court of Human Rights (ECtHR)
França

Ian Walden
Professor of Information and Communications Law
Queen Mary University of London
Reino Unido

Shota Watanabe
Researcher
Nomura Research Institute, Ltd.
Japão

Rolf H. Weber
Professor of International Business Law
University of Zurich
Suíça

Paul Wilson
Director General
Asia-Pacific Network Information Center (APNIC)
Austrália

Shinichi Yokohama
Chief Information Security Officer
Nippon Telegraph & Telephone (NTT)
Japão

Nicolo Zingales
Lecturer
Sussex University
Reino Unido

Sumário Executivo

Introdução

O Relatório de Status Global: Internet e Jurisdição de 2019 é o primeiro mapeamento abrangente das tendências políticas, atores e iniciativas relacionados a jurisdição na Internet. O Relatório baseia-se em uma contribuição sem precedentes em larga escala de dados fornecidos por 150 atores da Rede de Políticas Internet & Jurisdição, a saber: Estados, empresas de Internet, operadores técnicos, sociedade civil, academia e organizações internacionais.

Os atores consultados enviaram uma **mensagem muito forte de preocupação**:

- 95% preveem que os desafios jurídicos transfronteiriços da Internet se tornarão ainda mais cruciais nos próximos três anos[1];

EM RESUMO...

- Os desafios jurídicos transfronteiriços na Internet são cada vez mais graves.
- A pluralidade normativa no ciberespaço está aumentando.
- O risco de uma corrida armamentista legal é muito elevado.
- Estão em jogo importantes direitos humanos.
- Estão em jogo importantes interesses econômicos e sociais.
- O ciberespaço corre o risco de ser fragmentado ao longo das fronteiras nacionais.
- Os abusos on-line correm o risco de não serem endereçados de forma eficiente se não houver cooperação.
- Os países em desenvolvimento e as PME enfrentam barreiras regulatórias significativas.
- A agenda regulatória é definida por um pequeno número de Estados e outros atores dominantes.
- O ecossistema de governança é caracterizado por agendas e valores concorrentes.
- A complexidade normativa está aumentando, conduzindo à insegurança jurídica.
- Os conceitos jurídicos centrais estão ultrapassados e impedem o progresso.
- Os agentes privados estão cada vez mais desempenhando funções regulatórias e judiciais quase públicas.
- Os atores reivindicam a adoção de instituições, regimes e normas políticas adequadas.
- Os atores reivindicam uma maior coordenação internacional.
- Os atores reivindicam inclusão e capacitações.
- Os atores destacam o valor do multilateralismo.

- Apenas 15% acreditam que já dispomos das instituições certas para enfrentar estes desafios[2]; e
- 79% consideram que a coordenação internacional é insuficiente[3].

Cinquenta anos após a criação da Internet, o Relatório apresenta fortes indícios de uma **tendência perigosa**: a multiplicação mundial descoordenada de iniciativas de políticas públicas e privadas terá consequências negativas. Mesmo quando visam legitimamente abordar questões fundamentais de política transnacional, a adoção rápida de medidas corretivas sob a pressão da urgência frequentemente conduz a uma corrida armamentista legal e a conflitos adicionais. Garantir a preservação dos atributos fundamentais da Internet requer medidas ativas sob a forma de **esforços inovadores de coordenação e cooperação**.

Proliferação de problemas e iniciativas

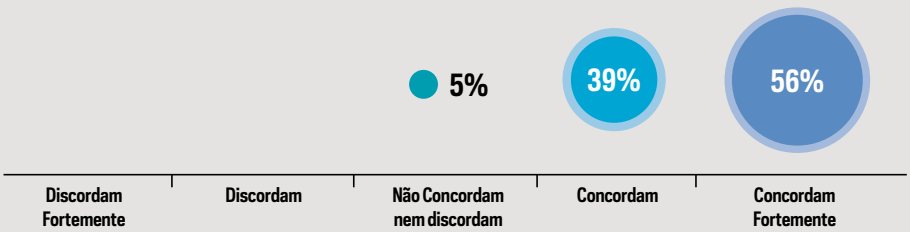
Os atores manifestaram sua dificuldade em acessar informações abrangentes sobre os numerosos e complexos desafios políticos, bem como em acompanhar a proliferação de iniciativas que procuram enfrentá-los. No entanto, dados consolidados e acessíveis constituem um pré-requisito para a tomada de decisão com base em evidências e para a manutenção da coerência entre as políticas.

Assim sendo, o relatório documenta extensivamente um número crescente de temas preocupantes que demandam atenção, sejam eles relacionados à expressão, segurança ou economia digital. Os desafios jurisdicionais surgem em todas as instâncias de regulamentação on-line, entre elas:

- Extremismo violento, ódio, violação de privacidade de dados e outras formas de abuso que podem se tornar tão prevalentes a ponto de o ambiente on-line tornar-se "inabitável", ao mesmo tempo em que um elevado grau de desinformação, seja ele real ou percebido, pode gerar uma crise de confiança;
- Crimes e ataques cibernéticos que possam minar de forma duradoura a confiança no ambiente on-line e ameaçar a sua infraestrutura; e
- Atividades comerciais cuja complexidade aumenta o custo da conformidade e pode criar barreiras à entrada de pequenas e médias empresas, limitando a concorrência, inovação e o acesso ao mercado transfronteiriço.

INFOGRÁFICO 1

OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET SE TORNARÃO CADA VEZ MAIS GRAVES NOS PRÓXIMOS TRÊS ANOS?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

O relatório também documenta as abordagens **jurídicas ou técnicas** cada vez mais diversas adotadas pelos governos e agentes privados para abordar essas questões, incluindo:

- Afirmação extraterritorial de jurisdição;
- Termos de serviço privados e diretrizes de comunidade;
- Localização obrigatória dos dados; e
- Bloqueio geográfico.

O relatório aponta para vários desafios fundamentais ao abordar questões jurídicas transfronteiriças, que **colocam em jogo atributos fundamentais da Internet transfronteiriça**, tais como:

- A falta de acordo comum sobre valores substantivos entre os agentes, ou a compreensão compartilhada dos principais conceitos jurídicos e do vernáculo;
- O risco de um "nivelamento por baixo" [*race to the bottom*][A] se a extraterritorialidade não for implementada com cautela;
- Desconfiança entre os usuários da Internet que não sabem quais são as leis aplicáveis às suas atividades on-line;
- A fragmentação voluntária ou involuntária, tanto no sentido técnico quanto regulamentar, pode desenvolver-se

A Para fins desta publicação, optamos por utilizar "nivelamento por baixo" como tradução que se aproxima do sentido da expressão em inglês "race to the bottom" empregada na publicação original, que não possui uma tradução amplamente reconhecida no português. [N.E.]

a tal ponto que será impossível falar da Internet como uma rede global; e

- A ausência de um equilíbrio adequado nas obrigações impostas aos intermediários da Internet pode resultar numa perda considerável de liberdade de expressão on-line e disponibilidade de serviços, ao ponto de afetar até mesmo a própria natureza da atual Internet transfronteiriça.

A insegurança jurídica domina

Muito do que foi feito até o momento buscou resolver problemas globais através de um olhar nacional. No entanto, o fluxo constante de inovação digital e a natureza transnacional da Internet tornam cada vez mais desafiador combater os abusos on-line com instrumentos jurídicos nacionais tradicionais.

Além disso, à medida que as interações transnacionais se tornam o novo normal, as pessoas e entidades são muitas vezes incapazes de determinar o seu "ambiente jurídico contextual", isto é: todas as leis dos Estados e outras normas que se aplicam à sua atividade on-line em determinado momento.

Devido às afirmações extraterritoriais de jurisdição, em algumas regiões, indivíduos, organizações e até Estados estão preocupados com a sua sujeição a regras on-line desenvolvidas sem a sua participação em um país distante.

Uma espiral perigosa

Uma corrida armamentista legal de iniciativas de políticas públicas e privadas descoordenadas, reativas e rápidas, que são propensas a serem incompatíveis, cria uma espiral perigosa, prejudicial em vários níveis, pois:

- Cria afirmações de jurisdição concorrentes em que o cumprimento da lei de um Estado resulta inevitavelmente em violação direta das leis de outros Estados;
- Impede efetivamente que os agentes enfrentem eficazmente os abusos on-line;
- Dificulta a inovação digital e o crescimento da economia da Internet, especialmente nos países em desenvolvimento e para as PME; e
- Favorece a regra dos mais fortes.

Isso poderá tornar potencialmente impossíveis os espaços e as atividades transfronteiriços on-line no futuro.

A coordenação é fundamental

As apostas são altas: a Internet impacta profundamente todas as sociedades e economias e novas fronteiras regulatórias estão constantemente emergindo, variando desde a criptografia até a inteligência artificial. Assim como o meio ambiente está enfrentando uma mudança climática, o ambiente legal on-line também está passando por uma transformação sistêmica.

Muita coisa precisa mudar para que os desafios jurídicos transfronteiriços sejam superados. Os atores consultados apontaram especificamente para a necessidade de:

- Maior coordenação para assegurar a coerência entre as políticas;
- Maior interoperabilidade jurídica, através de normas materiais e processuais desenvolvidas em conjunto;
- Inclusividade e capacitações, incluindo a abordagem de questões práticas, como a falta de acesso a informações relevantes devido a barreiras linguísticas e culturais, bem como a sobrecarga de informações;
- Maior clareza e compreensão comum dos conceitos jurídicos pertinentes;
- Levar em conta os respectivos papéis dos setores privado e público, incluindo a necessidade clara de reexaminar e definir de forma mais clara os papéis dos intermediários;
- Transparência e *accountability*[B];
- Buscar soluções para cada problema específico ou conjunto de problemas;
- Adesão contínua, ou ampliada, a uma abordagem multissetorial; e
- Reconhecer que nenhum Estado, empresa ou organização pode abordar essas questões sozinho, e que os atores do ecossistema simplesmente não podem optar por não colaborar.

B Para fins desta publicação, optamos por manter o uso da palavra accountability em sua forma original em inglês, seja pela falta de uma tradução amplamente aceita, pelas limitações conhecidas, ou mesmo pela circulação frequente desse termo em textos em português. [N.E.]

Moldar o futuro da sociedade digital

Os atores da Rede de Políticas Internet & Jurisdição enfatizaram que, por fim, não abordar os desafios jurisdicionais teria um custo elevado: a questão agora não é se a regulamentação deve ser feita, mas sim como e por quem ela deve ser feita. Como apontado por um especialista consultado, a Internet não é o problema nem a causa do problema. Com efeito, a Internet corre o risco de ser uma vítima da nossa falta de mecanismos de governança adequados.

A tarefa que se coloca diante de todos nós exige inovação de governança: envolve o desenvolvimento de normas de interoperabilidade legal e a coordenação de políticas para que estejamos dotados de métodos e ferramentas que sejam tão transnacionais, distribuídos, escaláveis e resilientes como a própria Internet. O que está em jogo é nada menos do que o futuro da sociedade digital que queremos coletivamente — para nós e para as futuras gerações.

Metodologia

Embarcar em um exercício de mapeamento e análise destinado a facilitar uma compreensão abrangente de um ecossistema altamente complexo e dinâmico - composto por múltiplos atores, iniciativas e tendências em todos os silos políticos da economia digital, direitos humanos e segurança constitui tarefa ousada. Tal empreendimento apresenta vários desafios. O mais óbvio é a dificuldade em facilitar uma compreensão suficientemente profunda das questões complexas associadas à coexistência de leis heterogêneas na Internet transfronteiriça — um dos maiores desafios políticos do século XXI.

Além disso, há desafios associados à tentativa de compreender plenamente e representar de forma justa os diversos pontos de vista e os multifacetados interesses envolvidos. Outro desafio considerável são os "fatos desconhecidos"; em qualquer tarefa que envolva grande diversidade setorial e geográfica corre-se o risco de perder algo importante sem sequer perceber que está faltando.

O reconhecimento desses desafios moldou a metodologia deste relatório e levou à adoção de um projeto de pesquisa flexível e qualitativo que permita uma exploração aprofundada dos assuntos pesquisados. Para superar os desafios citados acima, este projeto de redação adotou um método de pesquisa multifacetado que incorpora uma contribuição colaborativa e um

processo de revisão sem precedentes e inovador. Esse processo aproveitou a experiência combinada dos principais atores envolvidos na Rede de Políticas Internet & Jurisdição através de entrevistas semiestruturadas, feedback de revisão por pares e procedimentos de coleta de dados, combinados com investigação documental detalhada e abrangente.

Pesquisa documental

A pesquisa documental adotou métodos convencionais de pesquisa jurídica e consistiu principalmente de um estudo abrangente e da análise da jurisprudência relevante, de legislações e outras iniciativas regulatórias, bem como da literatura — incluindo livros, artigos de revistas, artigos publicados em conferências e publicações do setor. Essa pesquisa foi complementada por um estudo detalhado de diversos relatórios valiosos e outros materiais de várias organizações publicados nos últimos anos.

A pesquisa documental se beneficiou muito da vasta coleção de documentos relevantes da Rede de Políticas Internet & Jurisdição, disponíveis na base de dados I&J Retrospect Database.[4] A Retrospect Database é a principal coleção de acesso aberto da Rede de Políticas Internet & Jurisdição, com registros sobre avanços políticos, decisões judiciais, acordos internacionais e outros casos que reflitam tensões jurisdicionais na Internet transfronteiriça.

Esta importante coleção forneceu informações atualizadas sobre as principais tendências, atitudes, avanços e iniciativas.

Os materiais contidos na Retrospect Database também forneceram percepções importantes sobre as atuais abordagens legais e técnicas voltadas para as soluções, e também sobre aquilo que este Relatório define como "meta-tendências" abrangentes.

A primeira pesquisa com os atores

O primeiro método para obter a participação dos atores consistiu em uma pesquisa on-line composta por 17 perguntas sobre diversos tópicos relevantes para os assuntos pesquisados. Ao considerar a melhor forma de reunir os dados coletados para embasar as perguntas da pesquisa, houve um cuidado especial para formular perguntas que pudessem ser respondidas por todos os 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 identificou participantes da pesquisa representando todos os seus setores — ou seja, academia, sociedade civil, governos, organizações internacionais, plataformas de Internet e a comunidade técnica — e os participantes foram selecionados especificamente para garantir diversidade geográfica. Para esse efeito, regiões geográficas específicas foram direcionadas para capturar o máximo de variação possível. Além disso, a escolha dos participantes da pesquisa foi proposital, na medida em que foram especificamente orientados com base na sua experiência e conhecimentos consideráveis. No total, foram recebidas contribuições de 100 participantes entre o outono de 2018 e a primavera de 2019. Os participantes apresentaram seus pontos de vista pessoais, e não como representantes de qualquer organização específica. Além disso, as contribuições obtidas com as pesquisas só foram utilizadas sem atribuição.

A pesquisa obteve uma inestimável contribuição dos especialistas. Além de chamar a atenção para as principais tendências atuais, apresentar abordagens para soluções, meta-tendências abrangentes e preocupações geralmente mantidas no ecossistema, os resultados da pesquisa ajudaram a fornecer tanto o contexto quanto uma compreensão mais sutil dos ambientes operacionais enfrentados pela sociedade civil, governos, organizações internacionais, plataformas de Internet e a comunidade técnica.

Os resultados da pesquisa são usados ao longo do Relatório para mostrar, em números, as preocupações e atitudes do ecossistema dos atores da Rede de Políticas Internet & Jurisdição. Além disso, os comentários dos especialistas consultados são utilizados para destacar argumentos, observações e preocupações particularmente importantes.

Entrevistas com os atores

Foram organizadas entrevistas semiestruturadas com uma ampla gama de atores, a fim de complementar as percepções obtidas com as respostas à pesquisa e com a investigação documental. Tal como ocorre com as questões, o Secretariado da Rede de Políticas Internet & Jurisdição teve o cuidado de garantir a inclusão e a diversidade, inclusive geográfica, dos entrevistados, incluindo especialistas da academia, sociedade civil, governos,

organizações internacionais, plataformas de Internet e comunidade técnica. Esses atores foram identificados tanto de dentro como de fora da Rede de Políticas Internet & Jurisdição.

Cada entrevista durou, em média, mais de 30 minutos. As entrevistas foram realizadas em sigilo e, como tal, não foram gravadas. Notas detalhadas foram reunidas e as observações foram registradas de forma estruturada, facilitando o cruzamento e a análise detalhada. As entrevistas semiestruturadas permitiam uma flexibilidade considerável, possibilitando perguntas complementares, baseadas nas discussões com o entrevistado. Isto — combinado com a garantia de sigilo — proporcionou um ambiente em que os especialistas entrevistados puderam destacar questões que consideravam importantes no âmbito dos temas discutidos. Em muitos casos, os entrevistados também puderam fornecer perspectivas, percepções e informações que, de outra forma, não poderiam ter sido obtidas pelos pesquisadores. Dessa forma, parte do objetivo das entrevistas foi diminuir lacunas regionais e temáticas da pesquisa documental. No total, foram realizadas 63 entrevistas entre o outono de 2018 e a primavera de 2019. Os especialistas entrevistados forneceram seus pontos de vista pessoais e não como representantes de qualquer organização específica. Além disso, as contribuições obtidas com as entrevistas foram utilizadas sem atribuição.

Tal como os comentários feitos pelos especialistas pesquisados, os comentários dos especialistas entrevistados foram vitais e são utilizados ao longo do relatório para destacar argumentos, observações e preocupações particularmente importantes.

Avaliações dos atores

Além das pesquisas e entrevistas, buscou-se a participação dos atores mediante o compartilhamento de uma versão avançada do Relatório com os contribuintes antes da 3ª Conferência Global da Rede de Políticas Internet & Jurisdição, realizada de 3 a 5 de junho de 2019, na qual quase 300 dos principais atores de mais de 50 países se reuniram em Berlim. Uma versão mais curta — Principais conclusões — deste Relatório foi lançada durante a 3ª Conferência Global da Rede de Políticas Internet & Jurisdição.

As contribuições obtidas com esta revisão foram extremamente valiosas para garantir a qualidade deste Relatório, nomeadamente minimizando as lacunas regionais e tópicas.

> **A pesquisa obteve uma inestimável contribuição dos especialistas. Além de chamar a atenção para as principais tendências atuais, apresentar abordagens para soluções, meta-tendências abrangentes e preocupações geralmente mantidas no ecossistema, os resultados da pesquisa ajudaram a fornecer tanto o contexto quanto uma compreensão mais sutil dos ambientes operacionais enfrentados pela sociedade civil, governos, organizações internacionais, plataformas de Internet e a comunidade técnica.**

A segunda pesquisa com os atores

Uma segunda pesquisa com os atores foi realizada durante o terceiro trimestre de 2019. Essa pesquisa assumiu a forma de um chamamento público às partes interessadas para que fornecessem contribuições gerais para o Relatório.

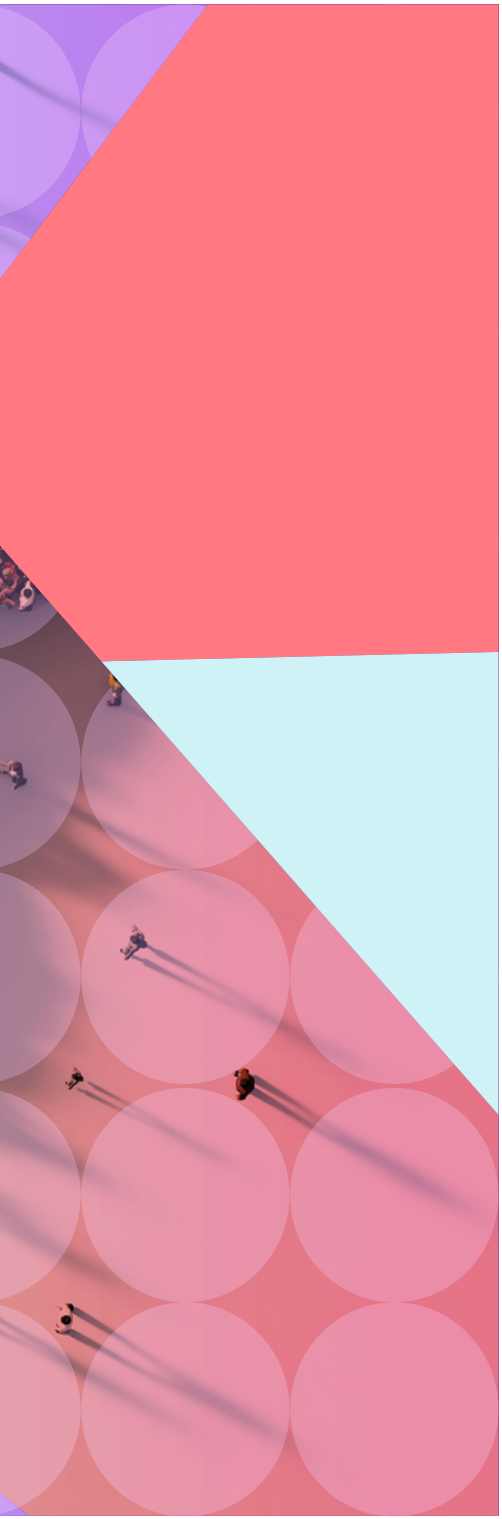
Além disso, a pesquisa buscou contribuições específicas para complementar as listas de iniciativas e progressos atuais coletados através da pesquisa documental, da primeira pesquisa e das entrevistas.

A segunda pesquisa gerou uma valiosa contribuição de mais de 50 colaboradores. Essa contribuição ajudou ainda mais a garantir a qualidade deste Relatório, particularmente ao minimizar as lacunas regionais e tópicas.

Limitações do estudo

Um estudo baseado em pesquisa desta natureza tem certas limitações. Em primeiro lugar, o âmbito do Relatório é delineado por referência ao mandato da Rede de Políticas Internet & Jurisdição. Assim, não se trata de um relatório de situação global sobre a Internet em geral, mas sim de um relatório centrado especificamente em questões jurídicas transfronteiriças relacionadas com a Internet. Em segundo lugar, apesar das medidas acima descritas, deve-se reconhecer o inevitável risco de lacunas. A relevância estatística da pesquisa exploratória que se baseia, em parte, num número limitado de participantes da pesquisa e de especialistas entrevistados não deve ser exagerada. Além disso, a maioria dos formatos de pesquisas documentais pode ser acusada de vieses que são difíceis de eliminar por completo.

À luz do que foi acima exposto, este Relatório representa uma tentativa, com base nos melhores esforços, de fornecer documentação e um panorama geral, porém abrangente, das tendências passadas, atuais e emergentes, dos agentes relevantes e das propostas de soluções para os principais desafios relacionados às políticas de direito transfronteiriço que a nossa sociedade conectada enfrenta até 1 de julho 2019. Como tal, é um retrato oportuno do ambiente político e cria uma primeira linha de referência sobre a qual poderão ser realizados estudos futuros.



01.

Por que um relatório de status global, e o que está em jogo?

- Expressão
- Segurança
- Economia

1.1. Respondendo ao chamamento da Rede de Políticas Internet & Jurisdição

O Relatório de Status Global da Internet & Jurisdição de 2019 é o primeiro relatório desse tipo. É produzido em resposta ao apelo urgente de mais de 280 atores de alto nível, de 50 países, durante a 2ª e 3ª Conferências Globais da Rede de Políticas Internet & Jurisdição, realizadas em 2018 e 2019.

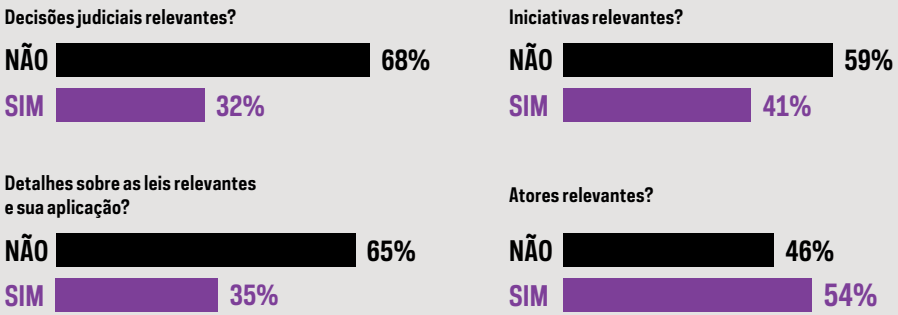
O principal objetivo do Relatório de Status Global é fornecer um panorama atual e refletir o pensamento, as preocupações, tendências e propostas atuais de diversos atores da Rede de Políticas Internet & Jurisdição. Assim, busca-se fornecer uma avaliação objetiva do que este ecossistema de atores enfrenta hoje e antecipar os avanços relevantes, destacando, por exemplo, tendências abrangentes que impactarão a evolução no futuro próximo.

O objetivo secundário é que o Relatório de Status Global seja um recurso útil para o desenvolvimento de capacitações e para criar uma maior compreensão sobre as complexas questões envolvidas — questões que podem afetar profundamente todo o ecossistema. Em certa medida, o Relatório também pode fornecer uma linha de base muito necessária para futuros estudos de tendências legais e regulatórias a nível global e servir de ponto de partida para os futuros relatórios regionais da Rede de Políticas Internet & Jurisdição.

Perguntamos aos especialistas se eles atualmente dispõem de fácil acesso a informações suficientes sobre os atores relevantes, iniciativas, leis e decisões judiciais. Embora a pesquisa tenha salientado algumas diferenças regionais e setoriais, identificou igualmente uma necessidade clara de um melhor acesso às informações relevantes.

INFOGRÁFICO 2

NO QUE SE REFERE AOS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET, VOCÊ ATUALMENTE TEM FÁCIL ACESSO A INFORMAÇÕES SUFICIENTES SOBRE:



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Com ficou claro a partir desses resultados, o acesso a informações suficientes sobre os atores e iniciativas relevantes[5] é consideravelmente maior do que a informação sobre os detalhes das leis pertinentes e da sua aplicação ou a decisões judiciais pertinentes. Os atores de países não membros da OCDE indicaram um grau consideravelmente inferior de acesso fácil à informação sobre atores e iniciativas relevantes, o que sugere a necessidade de capacitação e sensibilização para facilitar as atuais e futuras conversações.

Quando perguntados se existe acesso fácil a informações suficientes sobre detalhes de leis relevantes e sua aplicação, a resposta foi um retumbante "não" em todas as regiões e grupos de atores, a não ser no meio acadêmico. Não menos que 50% dos entrevistados do meio acadêmico indicaram ter acesso fácil a tais informações, o que significa que o problema não é a ausência de informação, mas sim a acessibilidade de tais informações. Isso pode ser explicado em parte pelo fato de que algumas informações importantes estão atrás de *paywalls* em bancos de dados que são comumente acessíveis a atores da academia, mas menos acessíveis para outros setores. No entanto,

existem também inúmeros bancos de dados on-line gratuitos que fornecem fácil acesso a vastas informações sobre os detalhes de leis relevantes e sua aplicação.[6] Em última análise, este aspecto dos resultados da pesquisa destaca, em parte, a necessidade de capacitação.

Os comentários dos especialistas pesquisados e entrevistados deixaram claro que eles têm algum acesso às informações relevantes, mas não de forma consistente ou abrangente. A falta de uma única fonte oficial, a dependência de múltiplos boletins informativos (setoriais), a falta de transparência, a falta de acesso on-line, a utilização de jargão legal e a sobrecarga de informações foram todos mencionados como preocupações. A ampla abrangência do assunto também pode ser um motivo. Como ficou claro no Capítulo III, que examina as tendências atuais, os desafios jurídicos transfronteiriços na Internet surgem numa gama tão diversificada de domínios importantes que é extremamente oneroso e desafiador manterem-se atualizados.

Vale ressaltar que os especialistas consultados não fizeram referência específica aos trabalhos acadêmicos como fonte de informação, sugerindo que o trabalho dos acadêmicos não chega efetivamente aos demais grupos de atores. Seria muito valioso explorar as opções para melhorar esta atual falta de transferência de conhecimento. Ao permitir a inovação política baseada em evidências, o presente Relatório procura fornecer a todos os atores as informações necessárias para desenvolver quadros e normas políticas para a sociedade e a economia digitais. O Relatório visa a fornecer uma visão geral abrangente e regionalmente equilibrada e uma documentação global de tendências passadas, atuais e emergentes dos atores relevantes e das soluções propostas para os principais desafios da política legal transfronteiriça que a sociedade conectada enfrenta. Ao fazê-lo, o Relatório explica o fato de que a Internet pode ser vista como: (a) uma infraestrutura técnica física (ou seja, hardware, roteadores, servidores, computadores, satélites, cabos de fibra óptica, etc.); (b) uma estrutura lógica (ou seja, protocolos técnicos que regem as interações on-line); e (c) uma construção social composta pelos conteúdos disponíveis e atividades cibernéticas. O Relatório complementa o processo de desenvolvimento de políticas em curso facilitado pelo Secretariado da Rede de

Políticas Internet & Jurisdição. Assim, baseia-se nos achados e nas questões abordadas nos três Programas temáticos da Rede de Políticas Internet & Jurisdição, a saber:

1. Programa de Dados e Jurisdição;
2. Programa de Conteúdo e Jurisdição;
3. Programa de Domínios e Jurisdição.

A abrangência dos assuntos tratados no Relatório foi determinada, sendo limitada pelo foco da Rede de Políticas Internet & Jurisdição na governança da Internet e no cruzamento de três áreas: economia digital, direitos humanos e segurança cibernética. Portanto, a abrangência não se limita a questões de jurisdição da Internet *per se*, mas abrange um vasto leque de questões processuais e materiais incluídas no amplo tema dos desafios jurídicos transfronteiriços que a Internet enfrenta. No entanto, a abrangência é claramente limitada a estes desafios jurídicos transfronteiriços e não pretende abordar questões gerais relacionadas à Internet.

“A abrangência não se limita a questões de jurisdição da Internet *per se*, mas abrange um vasto leque de questões processuais e materiais incluídas no amplo tema dos desafios jurídicos transfronteiriços que a Internet enfrenta.

Alinhado com as áreas prioritárias da Rede de Políticas Internet & Jurisdição, o Relatório não aborda mais amplamente guerras ou conflitos cibernéticos. Paralelamente, nem sempre é possível distinguir, no ambiente on-line, atividades que se encaixam ou não no campo do conflito cibernético. Por exemplo, a espionagem cibernética é realizada para fins militares e econômicos, e quando é direcionada aos setores de defesa ou infraestruturas críticas, diferenciar a espionagem militar e não militar pode ser praticamente impossível; ao contrário, tais atividades de espionagem são simultaneamente militares e não militares. Do mesmo modo, nem sempre é possível traçar uma linha precisa entre o compartilhamento de informações de segurança nacional e o de informações no contexto do cumprimento da lei.

Um número significativo de atores pediu um compêndio em tempo oportuno com as atividades globais. Espera-se que este Relatório — tornado possível pelo forte apoio que a Rede de Políticas Internet & Jurisdição goza de seus atores — possa

satisfazer esta demanda e servir como um instrumento crucial para ajudar a fomentar a coerência de políticas entre todas as iniciativas em curso.

Assim, o Relatório pretende contribuir para a mitigação de conflitos jurisdicionais graves, apoiar o desenvolvimento de soluções operacionais concretas e preservar os benefícios da Internet aberta, interoperável e transfronteiriça.

1.2. Transnacional como o novo normal

O mundo é composto por quase 200 países, alguns industrializados e outros em desenvolvimento. Todos esses países têm a sua própria história, economia e culturas. Possuem diferentes estruturas sociais, sistemas políticos e leis. Muitos têm grande diversidade cultural e alguns têm um leque diversificado de leis. As pessoas que povoam esses países são de etnias diferentes e falam línguas diferentes. Elas possuem valores, crenças religiosas e opiniões políticas diferentes. De fato, mesmo onde as pessoas consideram importantes os mesmos valores, elas frequentemente têm visões diferentes sobre como tais valores compartilhados devem ser equilibrados em casos específicos em que eles conflitam uns com os outros. Esta diversidade impressionante contrasta com o fato de que todos — até agora — essencialmente compartilhamos uma Internet.

Durante as entrevistas realizadas em apoio à elaboração do Relatório, o Regulamento Geral de Proteção de Dados (GDPR, na sigla em inglês) da União Europeia, introduzido em 2018, foi de longe a iniciativa legal mais mencionada. Poucas, se houver, iniciativas legislativas anteriores ganharam um grau semelhante de atenção internacional. Então, por que é possível conversar com pessoas de qualquer lugar do mundo e descobrir que elas não só estão cientes, mas têm conhecimento detalhado do GDPR — uma lei promulgada por legisladores na Europa, longe de países como Austrália, Brasil, China e República Democrática do Congo? Quando a União Europeia introduziu sua Diretiva relativa à proteção de dados em meados da década de 90, obteve apenas atenção internacional limitada e setorial. O que então mudou no mundo para fazer do GDPR um tema praticamente onipresente de discussão?

A resposta provavelmente tem duas partes. Primeiro, a globalização mudou o mundo desde meados da década de 1990 e o ecossistema está agora mais alerta para como as leis de uma jurisdição

podem impactar pessoas em outras partes do mundo. Esta é uma consequência inevitável do aumento da interconexão. Além disso, os Estados olham mais frequentemente para outros Estados ao tentar moldar suas próprias respostas jurídicas aos desafios que os atores enfrentam. A Internet contribuiu fortemente para estes avanços. Em segundo lugar, há agora um reconhecimento consideravelmente maior do papel que os dados — e, portanto, a privacidade de dados — têm em nossas vidas. Esta mudança também tem sido predominantemente impulsionada pela Internet.

> **Os assuntos que antes foram determinados internamente são agora de natureza transnacional, exigindo uma mentalidade diferente entre os tomadores de decisão em todos os níveis.**

O GDPR é apenas uma das muitas leis que impactam indivíduos além da sua jurisdição original. Na verdade, a maioria das leis dos países têm um impacto desse tipo em algum nível. Como muitos especialistas entrevistados observaram, isso contribui para um ambiente regulatório cada vez mais complexo.

A observação de que o ambiente on-line é em grande parte transnacional pode parecer pouco mais do que um truísmo; mas esta tendência tem implicações profundas, dando origem a problemas e impactando abordagens para sua solução. Vários especialistas entrevistados e pesquisados observaram que os assuntos que antes foram determinados internamente são agora de natureza transnacional, exigindo uma mentalidade diferente entre os tomadores de decisão em todos os níveis. As apostas são altas e a diversidade é grande.

A importância da comunicação (incluindo as comunicações transfronteiriças) está bem estabelecida e nenhum outro meio pode facilitar a comunicação transfronteiriça tão fluidamente como a Internet. O ambiente on-line presta-se ao tipo de comunicação transfronteiriça que as comunidades on-line nos países industrializados e em desenvolvimento esperam, e que pode levar a disputas transfronteiriças. A resolução de questões transnacionais não é, por conseguinte, facultativa, e as regras necessárias em matéria de jurisdição da Internet devem ser capazes de fazer face a um elevado volume de disputas.

Enquanto ambiente internacional, as questões de regulação da Internet também exigem soluções orientadas internacional-

mente; sejam elas pretendidas a nível internacional ou nacional, as soluções devem ter em conta o contexto internacional em que irão operar. Tanto as abordagens úteis quanto as nocivas são suscetíveis a implicações transfronteiriças e podem difundir-se internacionalmente. O "imperativo categórico" de Kant vem à mente, levando à busca de soluções universais.

Infelizmente, o clima político internacional mudou recentemente. Há um afastamento significativo nos esforços colaborativos internacionais e objetivos comuns, à medida que mais Estados adotam políticas voltadas internamente e colocam seus próprios interesses imediatos em primeiro lugar. A confiança está sendo substituída pela desconfiança, a colaboração pela regra dos mais fortes. Tais tendências representam um obstáculo substancial à coordenação eficaz da regulamentação da Internet. No entanto, continua a ser incontornável o fato de que os desafios jurídicos transfronteiriços na Internet só podem ser enfrentados por meio de esforços colaborativos internacionais e da busca de objetivos comuns; nenhum Estado, empresa ou organização pode fazê-lo sozinho e o ecossistema simplesmente não pode se dar ao luxo de não colaborar.

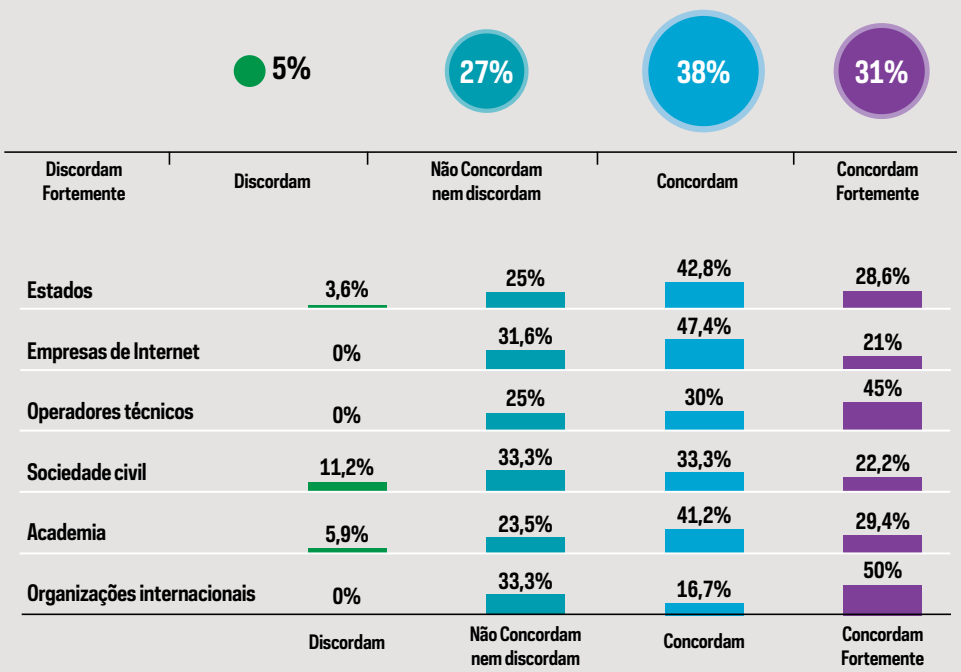
> **A confiança está sendo substituída pela desconfiança, a colaboração pela regra dos mais fortes.**

1.3. Preocupação crescente com abusos

Existe um sentimento geral entre as partes interessadas da Rede de Políticas Internet & Jurisdição de que o abuso on-line está aumentando. Uma clara maioria — 69% dos especialistas pesquisados — ou "concordaram" ou "concordaram fortemente" que os abusos on-line (por exemplo, sob a forma de discurso de ódio, assédio, pirataria, violações de privacidade ou fraude) estão aumentando. Vinte e sete por cento (27%) "não concordaram nem discordaram", e apenas 4% "discordaram" ou "discordaram fortemente".

INFOGRÁFICO 3

OS ABUSOS ON-LINE, POR EXEMPLO, SOB A FORMA DE DISCURSO DE ÓDIO, ASSÉDIO, PIRATARIA, VIOLAÇÕES DE PRIVACIDADE OU FRAUDE, ESTÃO AUMENTANDO?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Apesar de concordarem que os abusos on-line (por exemplo, discurso de ódio, assédio, pirataria, violações de privacidade ou fraude) estão aumentando, a porcentagem de entrevistados que "nem concordaram nem discordaram" foi substancial e muitos especialistas pesquisados disseram que a falta de provas empíricas dificultou a resposta a esta pergunta.

Esta observação é válida, importante e reflete a sofisticação do ecossistema. Ela direciona a atenção para o fato de que há atualmente uma falta de dados confiáveis, o que, por sua vez, está ligado à necessidade de padronizar métodos e iniciativas para coletar dados confiáveis para informar decisões políticas.

Um tema recorrente nos comentários feitos por especialistas pesquisados é que, da mesma forma que os abusos on-line estão aumentando, o uso geral da Internet também tem aumentado — em outras palavras, tanto abuso quanto uso normal estão aumentando (possivelmente em proporção). Um especialista consultado apontou corretamente que se trata de uma questão de porcentagens versus números absolutos. Com mais pessoas on-line e mais camadas de serviços e plataformas, o volume absoluto de abusos on-line e de pessoas afetadas por eles aumenta. No entanto, esta é uma questão em separado para saber se há um aumento na porcentagem de pessoas que se comportam mal no conjunto de usuários da Internet. Alguns especialistas pesquisados também observaram que, à medida que a conscientização sobre os abusos on-line aumentou, a disposição para denunciar abusos também aumentou.

Ambos os fatores podem contribuir para a percepção de que os abusos on-line estão aumentando. Uma tendência fundamental é que a conscientização e a sensibilidade a estes abusos resultam numa pressão política crescente para combatê-los. Esta pressão política corre o risco de desencadear descoordenação, reações unilaterais que não atingem efeitos desejáveis no longo prazo.

Alguns especialistas entrevistados afirmaram que a Internet meramente espelha a conduta off-line. Um especialista pesquisado sugeriu que o abuso está aumentando tanto off-line quanto on-line por causa do atual ambiente político e econômico e que as plataformas on-line simplesmente refletem a sociedade. No entanto, diferentes tipos de abusos também surgem on-line. A Internet dá maior visibilidade a coisas que antes eram largamente restritas à esfera privada e, portanto, facilita a sua disseminação.

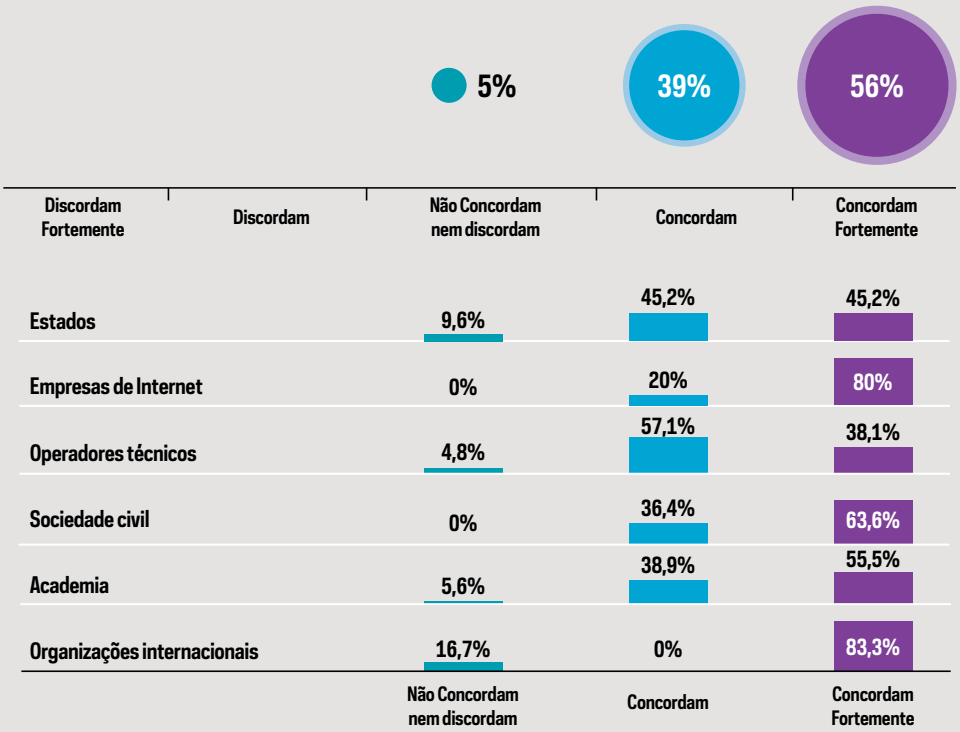
Outro especialista entrevistado enfatizou que essas dinâmicas diferem entre culturas e que há diferenças crescentes no que é visto como assédio, violações de privacidade e discurso de ódio.

> **“Como apontou um especialista consultado, nisso tudo, a Internet não é o problema nem a causa do problema. Ao contrário, a Internet é a vítima.**

A maioria (56%) dos especialistas consultados “concordou fortemente” que os desafios jurídicos transfronteiriços na Internet se tornarão cada vez mais graves nos próximos três anos. Outros 39% “concordaram” e nenhum dos especialistas entrevistados “discordou” ou “discordou fortemente”, enquanto 5% responderam que não tinham opinião sobre esta pergunta.

INFOGRÁFICO 4

OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET SE TORNARÃO CADA VEZ MAIS GRAVES NOS PRÓXIMOS TRÊS ANOS?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Os comentários apresentados pelos especialistas consultados salientaram uma opinião amplamente defendida segundo a qual a combinação de três fatores tornará cada vez mais graves os desafios jurídicos transfronteiriços na Internet:

1. O mundo está cada vez mais interligado através da Internet, aumentando, assim, a diversidade on-line;
2. A Internet está afetando profundamente as sociedades e as economias, o que significa que as apostas são altas; e
3. Os Estados-nações com visões diferentes procuram aumentar seu controle sobre a Internet, principalmente

através da utilização de instrumentos nacionais, em vez de cooperação e coordenação transnacionais.

Como apontou um especialista consultado, nisso tudo, a Internet não é o problema nem a causa do problema. Ao contrário, a Internet é a vítima.

1.4. Interesses legítimos conflitantes precisam ser reconciliados

Existe um "verdadeiro desafio regulatório" quando há interesses legítimos conflitantes difíceis de reconciliar. No contexto da jurisdição da Internet, existem inúmeros casos de interesses legítimos conflitantes. Por exemplo, pode ser difícil conciliar a proteção da liberdade de expressão do Estado A com as restrições do Estado B sobre o discurso de ódio.

Os verdadeiros desafios regulatórios com os quais o ecossistema se depara podem resumir-se à necessidade de conciliar, ou pelo menos equilibrar, as três dimensões de:

1. combate aos abusos;
2. proteção dos direitos humanos; e
3. promoção da economia digital.

Todas essas três dimensões são fortemente afetadas por dois fatores complicadores de importância fundamental:

1. os interesses individuais são buscados em detrimento do bem comum; e
2. existem lógicas/visões concorrentes para o que é o bem comum.

Em grande medida, as dificuldades em encontrar soluções para os desafios jurídicos transfronteiriços na Internet resultam do fato de que os verdadeiros desafios regulatórios são numerosos e envolvem noções jurídicas fundamentais para a identidade de cada Estado. No entanto, isso não explica completamente a complexidade da situação enfrentada pelo ecossistema. Alguns dos desafios resultam, em vez disso, da inadequação dos conceitos jurídicos utilizados.

1.5. Os conceitos jurídicos existentes estão sob pressão

A maioria dos conceitos jurídicos com os quais trabalhamos - como o foco sobre a localização das provas - foi desenvolvida no contexto off-line.

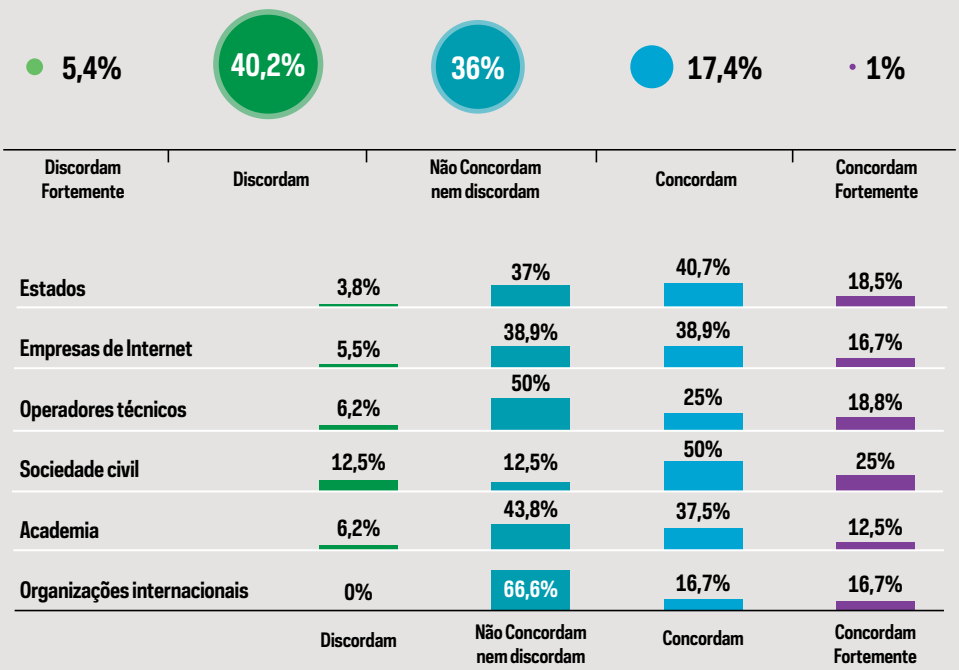
A aplicação online de conceitos legais pré-Internet frequentemente envolve decisões sobre as analogias e metáforas apropriadas. O impacto de tais decisões foi notavelmente destacado em meados da década de 1990 durante o debate sobre a constitucionalidade do US Communication Decency Act (CDA)[7], e voltou à tona na audiência do Supremo Tribunal do Canadá de 2016 durante o processo *Equustek*[8]. Representando a Google Inc., McDowell sugeriu que a pesquisa do Google era semelhante a um bibliotecário que gerenciava um dos vários catálogos de fichas. Em contraste, o juiz Karakatsanis sugeriu uma analogia diferente, comparando a pesquisa do Google com a pessoa atrás do balcão de uma livraria. A escolha da analogia claramente teria impacto na questão da responsabilidade.

Vários especialistas entrevistados enfatizaram a preocupação de que, no campo da jurisdição, os conceitos jurídicos são antiquados e desatualizados. Isto cria "desafios regulatórios artificiais", na medida em que os quadros e os conceitos aplicados são insuficientes para resolver as questões; em outras palavras, a inadequação dos instrumentos pode causar desafios regulatórios. Isso impede, ou pelo menos limita, o progresso.

Talvez o principal conceito sob pressão seja a distinção binária entre territorial e extraterritorial. Embora — da mesma forma que outras simplificações binárias, como a distinção entre dia e noite — possa funcionar para certos fins, elas são inadequadas para outros fins importantes. Tal como a distinção dia/noite não leva em conta o anoitecer e o amanhecer e, na verdade, as muitas nuances entre os dois, analisar a força das reivindicações jurisdicionais a partir da perspectiva binária de territorial versus extraterritorial não reflete adequadamente as nuances envolvidas.

INFOGRÁFICO 5

JÁ ESTAMOS APLICANDO OS CONCEITOS JURÍDICOS ADEQUADOS PARA FAZER FACE AOS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

PREOCUPAÇÕES COM OS CONCEITOS JURÍDICOS

Uma das perguntas feitas pela pesquisa apresentava a alegação de que já aplicamos os conceitos jurídicos corretos para fazer face aos desafios jurídicos transfronteiriços na Internet. Entre os especialistas pesquisados, 46% discordaram ou discordaram fortemente, 36% indicaram que não concordaram nem discordaram, e 18% concordaram ou concordaram fortemente. Os comentários dos especialistas consultados esclarecem a forma como estas estatísticas devem ser compreendidas e quais são as preocupações. Por exemplo, um especialista consultado

explicou sua concordância com a alegação acima, destacando que, embora os conceitos jurídicos básicos sejam sólidos e pertinentes, sua aplicação ao ambiente on-line continua sendo um desafio. Essa preocupação também é recorrente na literatura.

Outro especialista consultado observou que existem várias lacunas nos conceitos legais e outro enfatizou, ainda, que há um desafio categoricamente novo em fundir a Internet global com as fronteiras nacionais e que nós não possuímos os conceitos ou princípios jurídicos adequados para esta tarefa. Este último especialista também salientou que este desafio é mais complexo do que outros desafios transfronteiriços, como a regulamentação das transações financeiras ou do espaço aéreo.

Essas respostas à pesquisa correspondem a observações comumente feitas na literatura. Por exemplo, de que a mobilidade de dados prejudica a utilidade de vários pontos âncoras tradicionais da jurisdição.

Uma preocupação correlata é que, possivelmente, grande parte da discussão em torno de desafios jurídicos transfronteiriços na Internet depende de conceitos jurídicos envolvendo abstrações imprecisas que são difíceis de operacionalizar. Em parte, isso ocorre devido a diferentes entendimentos de conceitos jurídicos fundamentais. Um exemplo disso é encontrado no termo "cortesia" (*comity*), que tem um significado bastante específico no direito norte-americano, mas continua sendo um conceito vago e controverso no direito internacional. Devido às variações nos sistemas jurídicos ao redor do mundo, um especialista consultado observou que pode ser difícil até mesmo afirmar quais são os "conceitos jurídicos corretos". Outro especialista consultado apontou que, embora algumas regiões do mundo trabalhem com os conceitos legais "corretos", não o fazemos em nível global.

Um especialista consultado observou que os tribunais não possuem uma estruturação jurídica clara e inequívoca. No entanto, o mesmo especialista também acrescentou que chegar a uma legislação clara e inequívoca não seria tão difícil e não exigiria qualquer reinvenção importante da lei.

Neste contexto, um obstáculo potencial é o grau em que os tribunais compreendem e acompanham devidamente os desenvolvimentos tecnológicos. Este desafio já foi abertamente reconhecido pelos tribunais. No caso mais famoso, em 1997, o

Tribunal Distrital dos EUA para o Distrito Sul de Nova York observou que: "Juízes e legisladores confrontados com a adaptação dos padrões legais existentes ao novo ambiente do ciberespaço lutam com termos e conceitos que a criança média [...] de cinco anos de idade encara com natural familiaridade"[9]. Hoje em dia, raramente se veem tais confissões abertamente. No entanto, embora a competência geral de TI do judiciário tenha, sem dúvida, aumentado ao longo dos anos, pode-se sugerir que a complexidade das tecnologias relevantes aumentou em um ritmo ainda mais rápido. Assim, a pergunta se estamos ou não numa posição melhor do que em 1997, quando o Tribunal Distrital dos EUA para o Distrito Sul de Nova Iorque fez a sua observação, não tem resposta óbvia.

Seja como for, devido à complexidade envolvida, poucas áreas são tão atormentadas por desafios regulatórios artificiais como o debate sobre desafios jurídicos transfronteiriços na Internet. Basta considerar a complexidade conceitual envolvida na análise de uma questão legal transfronteiriça padrão, como uma reivindicação de jurisdição sobre uma conduta que ocorre em outro Estado, mas que afeta o Estado requerente. Em tal situação, a tradição ditaria começar perguntando se a matéria é do âmbito do direito internacional público ou privado – uma questão que nem sempre tem uma resposta óbvia[10]. Se a matéria for do âmbito do direito internacional privado, há necessidade de considerar outras matérias, tais como se existem fundamentos para reivindicar jurisdição pessoal e jurisdição temática. Em seguida, é necessário identificar a lei aplicável e determinar se há motivos para que o tribunal em questão se recuse a exercer jurisdição. Só então a questão pode ser analisada. Uma vez emitida uma sentença, surgem novas questões em torno do reconhecimento e da execução.

Por outro lado, se a questão for abrangida pelo direito internacional público, a tradição aponta para, pelo menos, três tipos diferentes de jurisdições — jurisdição prescritiva, adjudicativa e de execução, à qual foi recentemente acrescentada uma quarta jurisdição (jurisdição de investigação). Cada um desses tipos de jurisdição está associado a critérios pouco claros e vagos, e nem sempre é óbvio a que categoria uma determinada matéria pertenceria. Para a jurisdição prescritiva, existe um conjunto de princípios de referência comumente conhecidos

como Harvard Draft Principles,[11] com a inclusão da chamada "doutrina dos efeitos". Estes princípios foram originalmente elaborados para um propósito mais estreito comparado à forma como eles são frequentemente tratados hoje. Os critérios são menos claros para as jurisdições adjudicativa e de execução, enquanto os critérios detalhados da jurisdição de investigação ainda carecem de definição.

Se a reivindicação de jurisdição ultrapassar esses obstáculos, existem ainda inúmeras outras considerações, tais como:

- A reivindicação de jurisdição violaria a soberania de outro Estado (pressupondo que a soberania permanece vista como um direito por si só que pode ser violado)?[12]
- A reivindicação de jurisdição seria contrária ao dever de não intervenção?
- A reivindicação de jurisdição seria contrária à cortesia?
- A reivindicação de jurisdição a está, de fato, autorizada pelo princípio da devida diligência?[13]

A complexidade conceitual funciona como uma barreira, impedindo que os "não iniciados" contribuam para o debate, e corre o risco de tornar este campo o domínio exclusivo de um pequeno grupo de advogados especializados. Também regularmente resulta em mal-entendidos e erros de comunicação. Além disso, cria um ambiente em que as discussões se caracterizam por reivindicações excessivamente amplas e simplistas, levando a posições travadas; frequentemente os conceitos jurídicos não são debatidos de forma sistemática. Em vez disso, há uma tendência para escolher conceitos que suportam qualquer posição.

Um proponente de uma reivindicação de jurisdição pode, por exemplo, defender a "doutrina dos efeitos" (ignorando todos os demais princípios), ao passo que um oponente à mesma reivindicação pode defender o "princípio da cortesia" (ignorando todos os demais princípios). A complexidade pode ocultar as falhas em suas respectivas abordagens, e uma vez que ambos se sentem apoiados por lei, a probabilidade de acordo — ou mesmo de uma discussão construtiva — é baixa. Isto sublinha a necessidade clara de um quadro jurídico mais simples com princípios fundamentais para ancorar a discussão. O relatório aponta para um possível quadro jurisprudencial para a jurisdição, no qual a atenção é dirigida a três critérios:

1. se existe uma ligação substancial entre a matéria e o Estado que pretende exercer a jurisdição;
2. se o Estado que pretende exercer a jurisdição tem um interesse legítimo na matéria; e
3. se o exercício da jurisdição é razoável dado o equilíbrio entre os interesses legítimos do Estado e outros interesses.

Esses critérios estão ganhando crescente reconhecimento[14] e transcendem a lacuna percebida entre o direito público e o privado. Além disso, eles incorporam tanto a doutrina de efeitos e a cortesia, bem como outros conceitos relevantes de direito internacional público e privado. Como tal, constituem uma base adequada para construir normas jurídicas mais detalhadas para contextos específicos.

As atuais discussões sobre os desafios jurídicos transfronteiriços na Internet centram-se predominantemente na resolução das questões mais prementes do dia-a-dia (ou seja, alguns dos verdadeiros desafios regulatórios), à custa de se concentrar na complexidade conceitual subjacente (isto é, o desafio da regulamentação artificial). Isto é natural, dado o impacto que estes desafios têm para a sociedade. No entanto, só será possível fazer verdadeiros progressos se o ecossistema também enfrentar os desafios regulatórios artificiais. Com efeito, os desafios regulatórios artificiais devem ser primeiramente enfrentados a fim de abordar de forma adequada os verdadeiros desafios regulatórios. Espera-se que este Relatório possa contribuir para esta importante tarefa.

Para este fim, os capítulos a seguir deste Relatório têm o cuidado de não apenas envolver e delinear os desafios regulatórios genuínos, mas também de fazê-lo de forma que possa mitigar alguns dos desafios regulatórios artificiais aqui referidos.

“As atuais discussões sobre os desafios jurídicos transfronteiriços na Internet centram-se predominantemente na resolução das questões mais prementes do dia-a-dia (ou seja, alguns dos verdadeiros desafios regulatórios), à custa de se concentrar na complexidade conceitual subjacente (isto é, o desafio da regulamentação artificial).

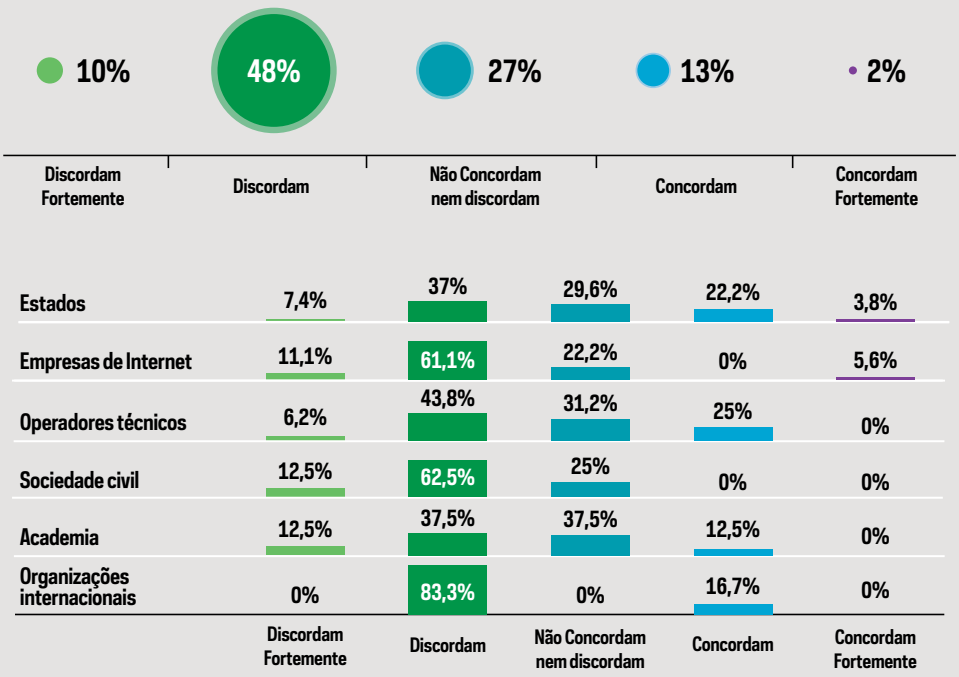
1.6. Faltam regimes e instituições adequadas

Os atores da Rede de Políticas Internet & Jurisdição chamaram a atenção para a atual falta de instituições adequadas para enfrentar os desafios jurídicos transfronteiriços na Internet.

A maioria (58%) dos especialistas consultados "discordou" ou "discordou fortemente" de que já dispomos de instituições adequadas para enfrentar os desafios jurídicos transfronteiriços na Internet. Apenas 15% dos especialistas consultados declaram que "concordaram" ou "concordaram fortemente", enquanto 27% indicaram que não "concordaram, nem discordaram".

INFOGRÁFICO 6

TEMOS AS INSTITUIÇÕES CERTAS PARA LIDAR COM OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET?



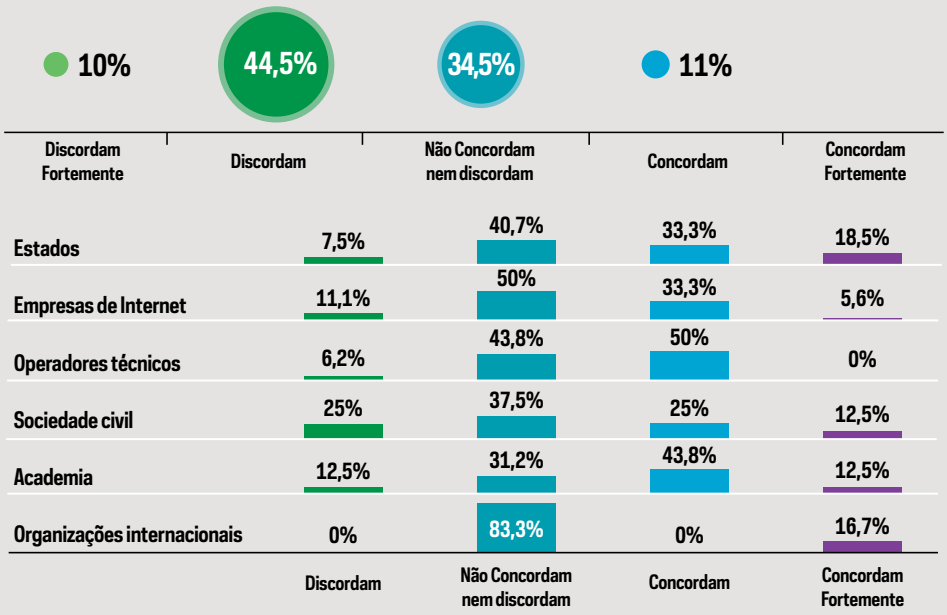
FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Alguns especialistas consultados comentaram que a sensibilização para a importância dos desafios jurídicos transfronteiriços na Internet é frequentemente baixa nas atuais instituições — tanto em nível internacional quanto nacional — e que estas precisam evoluir e cooperar melhor entre si. Entre os especialistas pesquisados e entrevistados, uma clara maioria considerou que, embora inúmeras instituições trabalhem nestas questões, outros fóruns ou instituições poderão ser benéficos. Um número menor de especialistas duvida expressamente da necessidade de outras instituições.

Outro aspecto da falta de coordenação diz respeito à disponibilidade de regimes e normas adequados. Dos especialistas consultados, 44,5% "discordaram" e outros 10% "discordaram fortemente" da afirmação de que dispomos dos regimes e normas para enfrentar os desafios jurídicos transfronteiriços na Internet. Apenas 11% dos especialistas consultados "concordaram", e nenhum "concordou fortemente". Dos especialistas consultados, 34,5% indicaram que não "concordam nem discordam".

INFOGRÁFICO 7

DISPOMOS DOS REGIMES E NORMAS ADEQUADOS PARA ENFRENTAR OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Em seus comentários, os especialistas pesquisados apontaram diferenças regionais, sendo que alguns observaram que os padrões globais não existem e são inatingíveis. Outros assinalaram que os desafios jurídicos transfronteiriços na Internet estão sendo tratados por leis nacionais ordinárias, e alguns acrescentaram que muitos dos desafios transfronteiriços não podem ser resolvidos de forma eficaz no âmbito nacional.

A PESQUISA DESTACA QUE:

1. os Estados estão tentando resolver os desafios jurídicos transfronteiriços na Internet, aplicando as suas leis vigentes;
2. entretanto, as respostas nacionais são inadequadas; e, portanto,
3. há uma necessidade clara de coordenação e cooperação transnacionais.

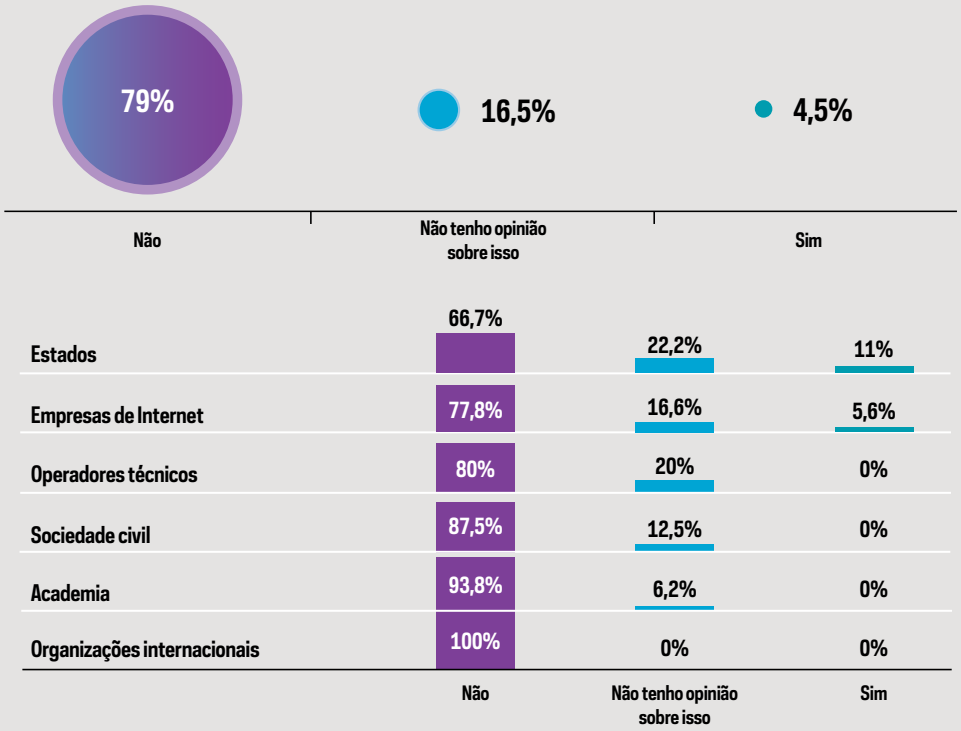
1.7. A coordenação é insuficiente

Os atores enviaram uma forte mensagem de que os atuais esforços de coordenação são insuficientes.

Quando questionados sobre a existência de coordenação e coerência internacionais suficientes para fazer face aos desafios jurídicos transfronteiriços na Internet, nada menos do que 79% dos especialistas consultados responderam "não", enquanto apenas 4,5% responderam "sim". 16,5% responderam que não tinham opinião sobre esta pergunta.

INFOGRÁFICO 8

EXISTEM COORDENAÇÃO E COERÊNCIA INTERNACIONAIS SUFICIENTES PARA FAZER FACE AOS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Embora os resultados da pesquisa revelem um consenso claro e esmagador entre setores e regiões, deve-se notar que alguns afirmaram que a coordenação e a cooperação internacionais sólidas podem ser vistas entre certos grupos e em determinados setores. Um exemplo citado foi a coordenação entre os organismos responsáveis pela execução da lei, por exemplo, através dos trabalhos da Interpol, da Europol e do Conselho da Europa.

1.8. Atributos fundamentais da Internet estão em jogo

A Internet deve ser preservada? Embora a imprecisão desta pergunta seja óbvia, a resposta instintiva é provavelmente ainda um retumbante "sim". Afinal de contas, a Internet já revolucionou a forma como as pessoas, as empresas e os governos interagem; desempenha um papel central na vida de bilhões de pessoas; e trouxe inúmeros e significativos benefícios econômicos e sociais.

Embora haja um apoio aparentemente claro para a preservação da Internet como a conhecemos, também é amplamente reconhecido que a Internet está em constante evolução. Isso talvez seja particularmente verdadeiro no sul global, onde a absorção, a estrutura e o uso da Internet estão evoluindo rapidamente. Da mesma forma que a maneira como usamos a Internet mudou ao longo dos anos, o conteúdo disponível on-line e a infraestrutura técnica da Internet também mudaram. A mudança on-line é constante e natural e tipicamente se traduz em progresso desejável.

No entanto, talvez existam certas características da Internet que devam ser protegidas contra a mudança. Em caso afirmativo, quais seriam essas características?

O que existe na Internet que instintivamente merece ser preservado? Estes tipos de perguntas podem ser respondidos em diferentes níveis de abstração. Em um nível relativamente elevado, pode-se apontar para a abertura da Internet e para o seu papel de facilitador e protetor dos direitos humanos e dos valores democráticos, qualidades que particularmente valem a pena preservar. Outras qualidades incluem o potencial da Internet de contribuir para um mundo mais justo e equitativo, e de aproximar as pessoas através de um meio de comunicação global, apoiando, em última análise, uma coexistência pacífica.

> **As características da Internet a serem preservadas devem ser ativamente protegidas.**

Infelizmente, todas essas características estão atualmente sob ameaça e, em diferentes graus, não podem ser consideradas garantidas. Pelo contrário, é preciso reconhecer que a Internet é um ambiente frágil e que as características da Internet a se-

rem preservadas devem ser ativamente protegidas. Duas dessas características da Internet são sua natureza transfronteiriça e a ausência de autorização prévia – ambas ameaçadas.

1.8.1. Não se pode tomar a Internet transfronteiriça como garantida

Conforme observado em uma breve nota conceitual, de setembro de 2018, da Internet Society, sobre a Internet e os efeitos extraterritoriais das leis: "A globalização é uma característica da Internet, não uma falha, e os sistemas jurídicos de todos os lugares devem reconhecer isso, em vez de tentar 'corrigi-la'.[15] Esta observação é ao mesmo tempo precisa e importante. No entanto, como discutido em detalhes a seguir, o cenário regulatório on-line (e off-line) sempre foi fragmentado. Esta é uma consequência direta da soberania da qual os Estados gozam, na medida em que eles têm a capacidade de elaborar suas próprias leis. De fato, observou-se que a dificuldade de aplicar e fazer cumprir qualquer sistema regulatório on-line pode ser atribuída ao fato de que a operação da Internet envolve um universo altamente fragmentado de atores, normas, procedimentos, processos e instituições, incluindo diversas entidades não estatais.[16]

Embora este tipo de fragmentação não seja nada de novo no ecossistema on-line, os Estados estão fazendo reivindicações jurisdicionais cada vez mais agressivas e apoiando essas reivindicações com multas pesadas ou até mesmo a ameaça de prisão (Capítulo 4.1.2), aumentando o que está em jogo com relação às questões regulatórias. Por conseguinte, tanto indivíduos como empresas podem optar por evitar a presença on-line em determinados mercados. Por exemplo, aqueles que desejam evitar o contato com determinados Estados podem utilizar medidas técnicas, tais como tecnologias de geolocalização (Capítulo 4.2.1), ou medidas não técnicas, como isenções de responsabilidade ou termos de serviço, excluindo o acesso baseado na localização.

Seja técnica ou não técnica, este tipo de fragmentação — se generalizada — constitui uma ameaça para a Internet transfronteiriça e acarreta consequências sociais e econômicas. A fragmentação on-line contribui para a fragmentação off-line, resultando na perda de algumas interações úteis e compromissos transfronteiriços que podem despertar confiança mútua e

compreensão. Quanto à vertente financeira, observou-se que: "A balcanização da Internet vai mudar a forma como as empresas fazem negócios. Isso provavelmente reduzirá a eficiência e, de uma forma macro, terá algum efeito na economia global."[17]

Ao mesmo tempo, pode-se argumentar que um certo grau de fragmentação é a única forma de defender as regras nacionais — que podem ser necessárias para evitar uma Internet sem lei — e evitar reivindicações de jurisdição global (Capítulos 3.1.2.1, 3.1.6.2 e 4.1.7). A tarefa, então, é determinar o tipo e o grau de fragmentação aceitáveis, sem colocar em risco as características da Internet que devem ser protegidas de mudança.

De certo modo, estamos assistindo a uma lacuna decrescente entre a Internet inicialmente sem fronteiras e os sistemas jurídicos territorialmente fundamentados; a Internet está se tornando menos "sem fronteiras" e os sistemas jurídicos estão cada vez menos ancorados na territorialidade. Se devidamente coordenada e gerida, esta evolução irá proporcionar grandes benefícios tanto para a luta contra os abusos como para a proteção dos direitos humanos, bem como para a economia digital. No entanto, se mal gerenciada, ela pode significar um desastre para o ambiente on-line.

A fragmentação também ocorre em um sentido mais técnico. Foi feita uma distinção útil entre fragmentação na Internet, como discutido acima, e fragmentação da Internet — fragmentação das infraestruturas físicas e lógicas subjacentes à Internet.[18]

A espinha dorsal física dos cabos de fibra óptica que atravessam oceanos e fronteiras internacionais permite uma experiência on-line relativamente perfeita, independentemente da localização. Tradicionalmente, estes cabos são controlados por operadores de telecomunicações, mas uma mudança de propriedade deu origem a pelo menos dois "novos" tipos de proprietários. O primeiro são as principais empresas de Internet. Algumas dessas empresas investiram em seus próprios cabos transoceânicos, resultando em redes privadas que conectam seus centros de dados e operam fora das regras que governaram a Internet e seus operadores de rede até o momento, como aqueles referentes ao transporte comum e à neutralidade.[19]

A segunda categoria de novos proprietários de cabos inclui os Estados que procuram buscar estratégias cibernéticas geopolíticas. A China, mais notavelmente, está fazendo investimentos

significativos para construir uma infraestrutura geograficamente estratégica que permita que os dados fluam ao redor do mundo inteiramente na infraestrutura de fibra óptica de propriedade chinesa.[20] Essa infraestrutura controlada nacionalmente pode ser utilizada para reduzir o acesso à informação, limitar a participação em fóruns on-line, restringir a privacidade dos dados e a liberdade de expressão, e talvez incorporar capacidades de vigilância e censura.[21] Estes desenvolvimentos podem ser vistos como uma extensão lógica do Grande Firewall da China (Capítulo 4.2.2), e podem, de fato, tornar o atual Grande Firewall da China redundante. De qualquer forma, eles representam um ataque sério à neutralidade da infraestrutura central da Internet. Além disso, representam um afastamento da Internet enquanto "rede de redes" — uma característica fundamental que incentiva uma abordagem multissetorial da governança da Internet — e uma ameaça à Internet transfronteiriça.

Outro desenvolvimento tecnológico que pode levar à fragmentação é exemplificado nas ambições do governo russo de desenvolver um sistema de backup independente do sistema de Servidores de Nomes de Domínio (DNS) que, de acordo com relatórios de 2017, não estaria sujeito ao controle por organizações internacionais.[22] O Secretário de Imprensa da Presidência Russa declarou que a Rússia não pretende se desconectar da Internet global, argumentando, em vez disso, que a recente imprevisibilidade dos EUA e da UE exigiu que a Rússia estivesse preparada para qualquer mudança de eventos.[23] Em 11 de fevereiro de 2019, a Rússia tomou várias medidas importantes nessa direção.[24]

Em maio de 2019, a lei russa sobre a soberania da Internet foi alegadamente assinada por Vladimir Putin, criando uma rede doméstica isolada de Internet.[25] Além disso, as principais ligações à Internet por satélite, embora estejam ainda incipientes, podem ter o potencial de facilitar e acelerar a fragmentação da Internet.

Em certo sentido, a fragmentação da infraestrutura técnica provavelmente representa uma ameaça maior para a Internet global do que a fragmentação resultante do panorama regulamentar on-line. Além disso, embora exista certa vontade política para tentar superar os efeitos negativos da fragmentação provocada pelos desafios regulamentares, não existem atualmente sinais de desenvolvimentos que possam impedir ou mesmo retardar a fragmentação das infraestruturas técnicas.

Ao abordar estas questões, é essencial ter em mente que a Internet transfronteiriça não pode ser considerada garantida; trata-se de um recurso que tem de ser ativamente protegido. Com efeito, a Internet transfronteiriça — tanto do ponto de vista técnico como regulatório — é um ambiente sensível e frágil, que compreende múltiplos atores e intervenientes; as alterações para um grupo de atores podem ter consequências potencialmente irreversíveis para outros.

1.8.2. A natureza da Internet que dispensa permissão precisa de proteção ativa

Uma característica distintiva do ambiente on-line é a sua natureza que não exige permissão. Na criação de um site, por exemplo, pode-se ser responsabilizado por esse site, mas não é necessária permissão para criá-lo. Ao eliminar barreiras à entrada, a natureza do ambiente on-line, que não exige permissão, tem sido um grande facilitador da inovação e sua importância é amplamente reconhecida. Um dos princípios da NETmundial destaca esta importância:

> *A capacidade de inovação e criação tem estado no centro do notável crescimento da Internet e trouxe grande valor para a sociedade global. Para preservar o seu dinamismo, a governança da Internet deve continuar a permitir a inovação sem necessidade de permissões através de um ambiente de Internet favorável, coerente com outros princípios do presente documento. Empreendimento e investimento em infraestrutura são componentes essenciais para um ambiente favorável.*[26]

A Diretiva de Comércio Eletrônico da UE de 2000 inclui outra articulação da natureza que dispensa permissão do ambiente online. O artigo 4(1), enfatiza que:

> *Os Estados-membros asseguram que o acesso à atividade de um prestador de serviços da sociedade da informação e o seu exercício não podem ficar sujeitos a autorização prévia ou a qualquer outro requisito de efeito equivalente.*[27]

O fato de a Internet, por tradição, ter sido uma rede de redes sem uma autoridade central tem ajudado — ou mesmo deman-

dado — a natureza que dispensa permissão discutida aqui. No entanto, com a mudança para a fragmentação no nível da infraestrutura, a natureza que dispensa permissão não pode ser considerada como garantida no futuro. Ao contrário, deve ser ativamente protegida e preservada.

Além disso, todas as razões pelas quais os "reguladores da primeira geração" tão fortemente ao consagrarem a natureza do ambiente on-line que dispensa permissão devem ser lembradas na nossa atual era de "hiper-regulação" (Capítulo 2.2.2). Quando a complexidade regulatória cria uma barreira substancial à entrada de novos atores inovadores no mercado, a natureza sem autorização prévia do ambiente on-line fica indiscutivelmente prejudicada.

> **Com a mudança para a fragmentação no nível da infraestrutura, a natureza que dispensa permissão não pode ser considerada como garantida no futuro.**

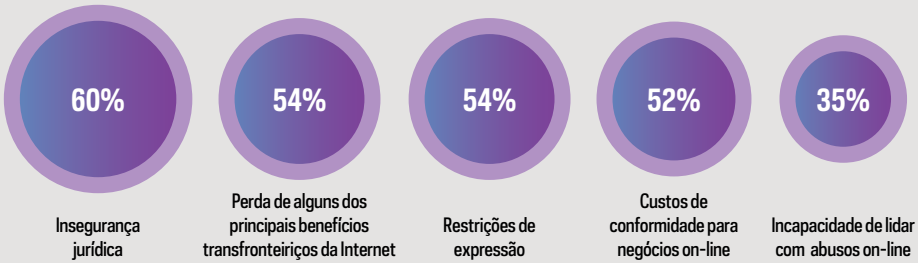
1.9. Pagamos um custo alto ao não lidar com desafios jurisdicionais

A falta de resposta adequada aos desafios jurídicos transfronteiriços na Internet implicará custos elevados para todos os atores e poderá causar danos irreparáveis. Tais consequências negativas foram destacadas em pesquisas e entrevistas.

Quando questionadas sobre as eventuais consequências negativas que poderão advir se os desafios jurídicos transfronteiriços na Internet não forem devidamente enfrentados, as partes interessadas da Rede de Políticas Internet e Jurisdição sublinharam, em especial, o seguinte:

INFOGRÁFICO 9

QUAIS CONSEQUÊNCIAS NEGATIVAS, SE HOUVER, VOCÊ PREVÊ, SE OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET NÃO FOREM DEVIDAMENTE ABORDADOS?



As 5 principais respostas dos entrevistados

FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Nas suas observações, os especialistas consultados também identificaram a falta de regras para governar a conduta na Internet como um risco. Como observou um especialista consultado, como acontece em todos os jogos sem regras, o mais forte é que irá prevalecer.

1.10. Uma abordagem multissetorial ainda é necessária

A gestão conjunta dos recursos da Internet por governos, empresas e sociedade civil nas suas respectivas funções — isto é, multissetorial[28] *— continua sendo a abordagem preferida para enfrentar os desafios transfronteiriços na Internet*[29]*. Este foi um tema claro entre os especialistas consultados e entrevistados.*

Muitos especialistas entrevistados apontaram para modelos multissetoriais que operam atualmente em determinados espaços, como governos que trabalham com empresas de mídia social em uma abordagem colaborativa ou cooperativa para combater questões como material de abuso infantil ou atividade extremista on-line. Alguns dos exemplos específicos citados incluem as atividades da Corporação da Internet para Atribuição de Nomes e Números (ICANN)[30] e as organizações associadas à Organizações Regionais *At-Large* Associadas,[31]

o World Wide Web Consortium (W3C)[32] e o Fórum de Governança da Internet (IGF), incluindo suas iniciativas regionais.[33] Entretanto, os especialistas entrevistados consideraram que deve haver uma interação mais robusta em mais áreas. Por exemplo, um especialista entrevistado disse que a sociedade civil e os cidadãos devem ter uma voz mais forte nessas discussões. Outro especialista entrevistado destacou a importância de um modelo multissetorial que inclua um acordo com o setor, em oposição à supervisão absoluta por parte do governo — um sistema ágil e flexível que permita que as questões sejam abordadas à medida que surgem.

Outro especialista comentou que estamos vendo ameaças ou tentativas de minar a abordagem multissetorial, especialmente devido a iniciativas unilaterais de governos e atores do setor privado impulsionados por seus próprios interesses nacionais ou comerciais.

Assim, a mensagem clara é de que, embora uma abordagem multissetorial seja desejada, o modelo multissetorial ainda não foi aperfeiçoado e está enfrentando a concorrência das iniciativas unilaterais mencionadas.

Além disso, alguns especialistas entrevistados apontaram para uma lacuna importante na confiança generalizada no multissetorialismo. As decisões judiciais têm um impacto significativo em todas as questões jurídicas transfronteiriças na Internet. No entanto, por sua natureza, as decisões judiciais não são alcançadas através de qualquer processo que possa ser descrito como multissetorial. Normalmente, apenas as partes no litígio podem apresentar argumentos ao tribunal. Existe, portanto, um risco óbvio de interesses importantes não serem representados nos julgamentos e ignorados pelos tribunais.

“A mensagem clara é de que, embora uma abordagem multissetorial seja desejada, o modelo multissetorial ainda não foi aperfeiçoado e está enfrentando a concorrência das iniciativas unilaterais.

Para fazer face a esta fragilidade do sistema judicial, alguns tribunais permitem a apresentação dos chamados *amicus curiae* — “amigo da corte”. Os tribunais têm permitido um grande número de manifestações (opinião independente, de alguém que poderá ser afetado com o resultado) em alguns casos recentes

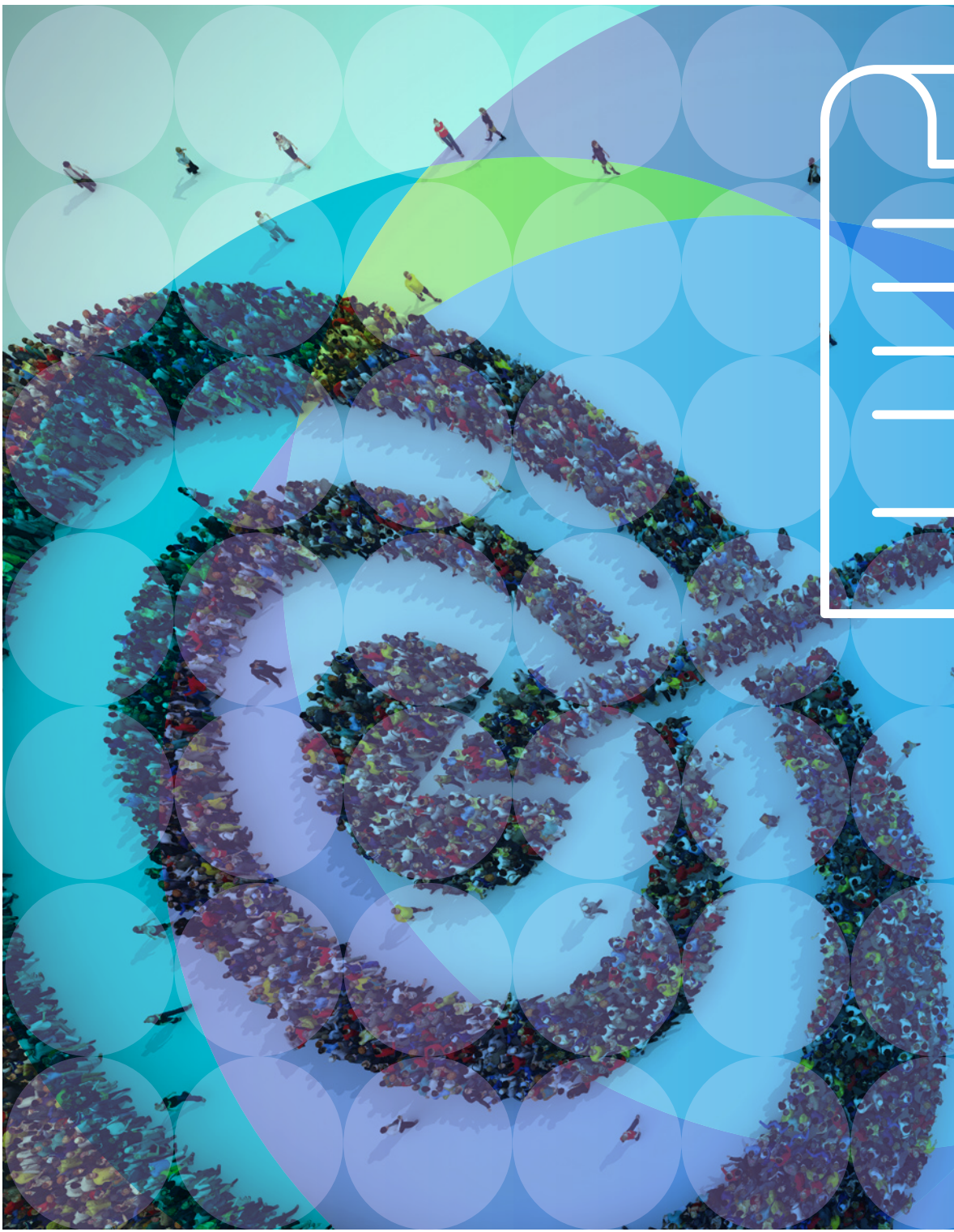
de jurisdição na Internet de alta visibilidade, como o *caso Microsoft Warrant*[34], julgado na Suprema Corte dos EUA em fevereiro de 2018. De uma perspectiva internacional, porém, essa solução de *amicus* é uma exceção e a maioria dos tribunais evita contribuições externas, ao: (1) não permitir manifestações de *amicus* em caso algum, (2) adotar regras judiciais que excluem manifestações de *amicus* em todas as circunstâncias, exceto as mais excepcionais, ou (3) interpretar as regras do tribunal restritivamente para excluir contribuições daqueles que não sejam parte. As abordagens restritivas em relação aos pareceres de *amicus* podem justificar-se pelo risco de atrasos e custos adicionais. Estes são legítimos quando se trata de manifestações de *amicus*, particularmente aqueles apresentados por estrangeiros. Ao mesmo tempo, porém, os interesses em jogo muitas vezes também são elevados para terceiros, incluindo terceiros estrangeiros.[35] Nos casos em que os tribunais se sentem competentes para tomar decisões com impacto internacional, pode-se argumentar que eles devem aceitar a responsabilidade de assegurar que estejam suficientemente expostos aos interesses internacionais que possam ser afetados por suas decisões. Neste contexto, a reforma do sistema *amicus curiae* é indiscutivelmente o reforço mais urgentemente necessário para o multissetorialismo eficaz.

1.11. Um desafio premente, insuficientemente abordado

Os desafios jurídicos transfronteiriços que a Internet enfrenta atualmente estão recebendo mais atenção na mídia e nas discussões políticas do que nunca antes.

Em muitos aspectos, os desafios no contexto da jurisdição da Internet são semelhantes àqueles que o mundo enfrenta com as alterações climáticas. Ambos só podem ser enfrentados através da cooperação e coordenação transfronteiriças e ambos têm um impacto global que afeta de forma mais aguda os países em desenvolvimento. A natureza dos dois desafios também pode fazer indivíduos (e mesmo Estados individuais) se sentirem incapazes de fazer algo de impacto por conta própria para afetar a mudança. No entanto, outra semelhança é encontrada nas enormes implicações econômicas e sociais que estão em jogo.

Existem também diferenças importantes entre as respectivas crises que se desenrolam no ambiente natural e no ambiente on-line. Por exemplo, embora os argumentos econômicos de curto prazo sejam frequentemente citados contra propostas de medidas decisivas para combater as alterações climáticas, há poucos, se houver, argumentos econômicos contra o enfrentamento dos desafios jurídicos transfronteiriços na Internet. Pelo contrário, uma ação decisiva contra os desafios jurídicos transfronteiriços na Internet será também recompensada economicamente a curto prazo, e não apenas a longo prazo. Além disso, embora ainda existam aqueles que negam as mudanças climáticas, poucos duvidam ou mesmo questionam o impacto negativo caso os desafios jurídicos transfronteiriços na Internet não sejam enfrentados. Em termos mais gerais, embora tenha sido sugerido que alguns Estados preferem operar com um quadro jurídico pouco claro e caótico no que diz respeito a questões como a espionagem cibernética e a agressão cibernética, poucos são os que se beneficiam do caos jurisdicional e da "hiper-regulação" on-line (Capítulo 2.2.2). Estes últimos pontos sugerem que deve haver uma vontade política clara e justificativas econômicas e sociais inquestionáveis para enfrentar de forma decisiva os desafios confrontados no contexto da jurisdição da Internet.



02.
Tendências dominantes

- Expressão
- Segurança
- Economia

A combinação de estudos detalhados e contribuições dos atores — através da pesquisa e das entrevistas — chamou a atenção para várias tendências globais que são centrais para qualquer discussão sobre os desafios jurídicos transfronteiriços na Internet. Estas "meta-tendências" dominantes estão moldando as tendências atuais (Capítulo 3) e, em certa medida, estabelecem os parâmetros dentro dos quais as abordagens jurídicas e técnicas podem ser exploradas (Capítulo 4).

Em primeiro lugar, algumas das tendências dominantes dizem respeito à evolução do cenário tecnológico, o que cria a necessidade de "preparar para o futuro" quaisquer abordagens jurídicas ou técnicas que adotemos hoje. Neste contexto, há uma clara tendência de erosão das fronteiras entre o mundo dos dados on-line e o mundo físico e há uma tendência igualmente clara de migração contínua para a nuvem.

Em segundo lugar, algumas das meta-tendências dominantes dizem respeito ao ambiente regulatório na Internet. Embora talvez seja uma observação rudimentar, existe uma clara tendência de reconhecimento de que a regulação legal é necessária — a questão de regular ou não é um "assunto encerrado". A proliferação de iniciativas indica que os desafios jurídicos transfronteiriços na Internet estão sendo levados a sério, talvez mais do que nunca. No entanto, as medidas tomadas sofrem de falta de coordenação e de cooperação. Isso só agrava os desafios decorrentes das tendências de sobrecarga de informações e de acesso à informação.

Uma terceira tendência diz respeito a tentativas sérias de repensar o papel da territorialidade na regulação da Internet, e a uma vontade política emergente para que isso seja feito. Na verdade, existe um reconhecimento crescente, em alguns contextos, de que a territorialidade é largamente irrelevante. Os legisladores também estão demonstrando maior apetite para estender as leis on-line, muitas vezes em uma maneira 'extraterritorial' que afeta indivíduos, empresas e organizações no exterior, ou mesmo outros Estados; podemos agora estar em uma era de hiper-regulação jurisdicional (Capítulo 2.2.2). O crescente alcance geográfico das legislações nacionais pode ser visto como uma resposta natural, nas quais as leis nacionais são

os únicos instrumentos para abordar questões transnacionais. No entanto, esta tendência está associada a alguns problemas, inclusive a dificuldades de execução, e existe algo de irônico na medida em que a aplicação de mais leis transnacionais incentivará maior cooperação, pois muitas vezes ela é necessária para a observância da legislação.

Em quarto lugar, há um conjunto de tendências abrangentes que se relacionam com pluralidade normativa, convergência e fertilização cruzada. Tornar indistinta a diferença entre conteúdo ilegal, conteúdo que viola termos de serviço e conteúdo censurável só aumentou a diversidade de fontes normativas. Uma tendência observada neste contexto é a harmonização através das normas da empresa; outra é a fertilização cruzada judicial impulsionada pela replicação e imitação que nem sempre leva devidamente em conta as questões de escalabilidade. Nesse contexto, os atores da Rede de Políticas Internet & Jurisdição apontam para uma tendência em que atores novos e menores ficam vinculados a decisões de atores já estabelecidos e maiores. Isto, por sua vez, pode motivar o desenvolvimento do que pode ser chamado de "avaliações de impacto no sul global".

Uma quinta tendência refere-se ao aumento da complexidade em torno do papel dos intermediários da Internet. Em alguns casos, esses intermediários são guardiões autoproclamados; em outros, eles são guardiões involuntários. Às vezes, eles são simplesmente bodes expiatórios e alvos "fáceis" para litígios e ordens de restrição de conteúdo.

2.1. Uma paisagem tecnológica em constante fluxo

Existe uma interação necessária e constante entre a lei e a tecnologia, uma vez que os desenvolvimentos em uma esfera normalmente impactam a outra.

A interação constante entre lei e tecnologia ocorre tanto on-line quanto off-line. No passado, essa evolução foi tipicamente lenta, gradual e relativamente esporádica. No ambiente on-line, no entanto, as principais evoluções tecnológicas são rápidas, dramáticas e numerosas. Isto coloca uma pressão significativa no aparelho legislativo e exige certo grau de preparo para o

futuro que vai muito além do que historicamente foi exigido. A prontidão para esta tarefa parece muitas vezes limitada nos países industrializados e é quase ausente em muitos países em desenvolvimento.

2.1.1. A unificação dos mundos on-line e físico

Uma tendência clara e abrangente é o fato de que as fronteiras entre o mundo orientado por dados on-line e o mundo físico estão se corroendo e se tornando menos claras, ou mesmo sem sentido. Este é um processo contínuo e não é algo novo. As pessoas já não "entram on-line" — estamos constantemente on-line. Isso ocorre há vários anos e, em grande parte, deve-se à adoção dos smartphones.

No entanto, na era da Internet das Coisas, a velocidade com que estas fronteiras se dissipam está aumentando drasticamente, com efeitos para todos os aspectos da sociedade.

Como um especialista entrevistado observou, as grandes empresas orientadas por dados que conhecemos do ambiente on-line estão cada vez mais usando sua expertise em dados para se expandir para indústrias tradicionais no mundo físico (carros autônomos são um exemplo, mas essa tendência vai muito além disso). Da mesma forma, as empresas tradicionalmente off-line estão se reposicionando cada vez mais como empresas orientadas por dados, mas ainda podem não ter a capacidade de se envolver plenamente com a abrangência das questões jurisdicionais transfronteiriças, uma vez que elas "chegaram atrasadas para a festa". Isso levanta várias questões jurídicas relacionadas com a concorrência, por exemplo, e o abuso de posições dominantes no mercado. Talvez ainda não tenhamos uma visão completa de como isso irá impactar os desafios jurídicos transfronteiriços on-line.

Como vários especialistas entrevistados apontaram, a tecnologia neste contexto atua não apenas como objeto de regulação, mas como força reguladora propriamente dita. De fato, há muito se reconhece que a tecnologia concorre com a lei como força reguladora, o que, por sua vez, transforma aqueles que controlam a tecnologia em reguladores.[36]

2.1.2. Uma migração contínua para a nuvem

De forma simplificada, a computação em nuvem envolve o fornecimento sob demanda de recursos computacionais através da Internet.[37] Nesta área, rotineiramente se estabelece uma distinção entre infraestrutura como serviço (IaaS), plataforma como serviço (PaaS) e software como serviço (SaaS), mas cada vez mais, inclui governo como serviço (GaaS), monitoramento como serviço (MaaS) e segurança como serviço (SECaaS).[38] Todas essas formas de computação em nuvem têm implicações profundas para os desafios jurídicos transfronteiriços na Internet.

Intencionalmente ou não, a computação em nuvem normalmente cria pontos de conexão com jurisdições estrangeiras em situações que anteriormente poderiam ter sido inteiramente domésticas.

Além disso, a computação em nuvem resulta na manutenção de dados por outras partes que não aquelas que na realidade "possuem" os dados, o que tem consequências em relação à lei relativa à privacidade de dados, por exemplo, e à capacidade de cumprimento da lei para acessar os conteúdos necessários como prova.

A computação em nuvem, com seus fluxos de dados frequentemente altamente fluidos, pode dificultar ou mesmo impossibilitar[39] a determinação, em tempo real, do local onde dados específicos estão localizados. Isso, por sua vez, prejudica severamente a utilidade da localização dos dados como fator de conexão jurisdicional ou ponto focal. Tal como argumentado recentemente por um tribunal dos EUA, quando é impossível determinar a localização dos dados, torna-se também mais difícil argumentar que a soberania de um determinado Estado estava implicada quando esses dados foram acessados por uma autoridade de execução da lei: "Mesmo que a interferência com a soberania de um Estado estrangeiro esteja envolvida, a natureza fluida da tecnologia de nuvem do Google não deixa claro qual soberania de qual país estrangeiro estaria sofrendo interferência quando o Google acessa o conteúdo das comunicações para produzi-lo em resposta ao processo legal."[40]

É importante, evidentemente, não confundir a questão de saber com *qual* soberania de Estado se está interferindo com a questão de saber se a soberania de *qualquer* Estado está sendo afetada. O raciocínio do tribunal aqui pode ser acusado de não reconhecer esta distinção. No entanto, há certamente algum

mérito na questão para a qual o tribunal procura chamar a nossa atenção. Enquanto o estudo da computação em nuvem como um campo regulatório ou jurídico distinto parece ter declinado, o desenvolvimento tecnológico está em curso. Além disso, os Estados,[41] empresas[42] e regiões[43] ainda estão desenvolvendo formas de usar a computação em nuvem, e nem todas as tentativas de estabelecer arranjos de computação em nuvem foram bem-sucedidas. Um especialista entrevistado enfatizou que não são apenas os dados que vão para a nuvem. À medida que grandes quantidades de software se movem para o ambiente de nuvem, garantir o controle e a segurança é um desafio, e a segurança nem sempre é incorporada desde o início. Consequentemente, há poucas dúvidas de que a computação em nuvem continuará a impactar os desafios jurídicos transfronteiriços na Internet como uma meta-tendência global.

2.2. Regulação: não se, mas como e por quem

É útil distinguir entre a regulação da Internet, por um lado, e a regulação na Internet, por outro. É principalmente esta última que está em foco aqui.

2.2.1. Regular ou não regular não é a questão

Durante a década de 1990, houve um debate se seria desejável regular o ciberespaço, e se seria possível fazê-lo. Este debate ocorreu em vários níveis; nos círculos políticos e no meio acadêmico, nacional e internacionalmente, entre o número comparativamente limitado de Estados que à época estavam ativos on-line. Na arena acadêmica, as principais contribuições para o debate em língua inglesa foram feitas por vários proeminentes estudiosos norte-americanos.[44]

“ É geralmente reconhecido que há uma necessidade de regulação legal para muitas atividades on-line.

O exemplo mais famoso, no contexto político, data de 1996, quando Barlow apresentou sua conhecida Declaração de Independência do Ciberespaço, que capturou o espírito da época:

Governos do Mundo Industrial, seus cansados gigantes de carne e aço, eu venho do Ciberespaço, a nova casa da Mente. Em nome do futuro, eu exijo a vocês do passado que nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não possuem autoridade soberana no lugar em que nos reunimos. [...]
Vocês não têm o direito moral de nos impor regras nem possuem nenhum método de execução que tenhamos razão para temer. [...] O ciberespaço não está dentro das suas fronteiras. [...] O nosso é um mundo que está em todos os lugares e em nenhum lugar, mas não onde os corpos vivem. [...] Seus conceitos legais de propriedade, expressão, identidade, movimento e contexto não se aplicam a nós. [...] Nossas identidades podem ser distribuídas por muitas de suas jurisdições. A única lei que todas as nossas culturas constituintes geralmente reconhecem é a Regra de Ouro. Esperamos que possamos construir as nossas soluções específicas com base nisso. Mas não podemos aceitar as soluções que vocês estão tentando impor."[45]

Hoje, alguns desses pensamentos podem parecer pertencer a uma era passada. No entanto, outros aspectos continuam claramente relevantes — talvez mais como uma explicação das questões regulatórias que o ecossistema ainda enfrenta hoje, e não como manifesto. Soberania e execução continuam a ser questões complexas e controversas. O ciberespaço pode ser hoje menos "sem fronteiras" do que era então, mas o conflito entre as leis baseadas na territorialidade e uma Internet *prima facie* sem fronteiras e virtualmente global permanece. Além disso, alguns conceitos jurídicos continuam a ser difíceis de transpor para o ambiente on-line.

No entanto, as questões de saber se é possível e desejável regular o ciberespaço atualmente são "questões encerradas". É geralmente reconhecido que há uma necessidade de regulação legal para muitas atividades on-line. Por exemplo, poucos aceitariam a ideia de um ambiente on-line onde não se apliquem leis contra os materiais de abuso infantil. Os consumidores são menos propensos a participar do comércio eletrônico se não lhes for concedida proteção, e a proteção da privacidade de dados é pelo menos tão importante

on-line quanto off-line. O fato de a regulação jurídica desempenhar um papel importante on-line é uma importante meta-tendência global que afeta todos os aspectos das tendências atuais (Capítulo 3) e das abordagens jurídicas e técnicas (Capítulo 4).

Em todo caso, as áreas em relação às quais o ecossistema se baseia na regulação normativa não são necessariamente estáticas. Conforme discutido em mais detalhes abaixo, enquanto a lei é amplamente invocada para criar confiança em transações comerciais on-line hoje, contratos inteligentes baseados em blockchain podem atuar cada vez mais como um concorrente em algumas áreas - mesmo que a lei continue sendo um facilitador subjacente da confiança criada por contratos inteligentes (Capítulo 3.3 .5 .3).

Enquanto isso, a aplicabilidade da lei on-line está agora firmemente estabelecida. Estudiosos como Ost, van de Kerchove[46] e Weitzenboeck[47] enfatizaram que o modelo piramidal de regulação — caracterizado pela centralidade do Estado como regulador — tem sido severamente prejudicado pela evolução das tecnologias da informação, globalização, interdependência econômica, foco nos direitos humanos e ascensão de organizações transnacionais. Tal como foi resumido por Weitzenboeck, a "regulação da rede" ou "regulação da malha", que alegadamente tem substituído o modelo piramidal de regulação, mostra que: "o Estado deixa de ser a única fonte de soberania (tendo que compartilhar isso não apenas com autoridades superestatais, mas também com entidades privadas poderosas); a vontade do legislador deixa de ser recebida como dogma (é aceita apenas sujeita a condições, após um processo de avaliação complexo tanto antes quanto após a promulgação de uma lei); as fronteiras entre fato e direito tornam-se, por vezes, indistintas; as diferentes potências do Estado interagem (juízes tornam-se coautores da lei e a subdelegação do poder normativo que, em princípio era proibida, se multiplica); os sistemas jurídicos (e, mais amplamente, os sistemas normativos) ficam enredados; o conhecimento da lei que tradicionalmente proclamou a sua pureza metodológica (monodisciplinar) agora se inclina para um modo interdisciplinar e é mais o resultado de um processo de aprendizagem do que axiomas a priori. Além disso, a justiça, que no modelo piramidal se reduziu às hierarquias de valores fixados na lei, é hoje compreendida em termos do equilíbrio de interesses e do equilíbrio de valores que são simultaneamente diferentes e variáveis."[48]

AUTORREGULAÇÃO

A autorregulação desempenhou um papel importante no desenvolvimento da Internet e pode ocorrer em vários níveis, desde a governança das infraestruturas até à moderação dos conteúdos orientados pelos pares num fórum on-line específico. O sistema de nomes de domínio é frequentemente citado como um importante exemplo de autorregulação bem-sucedida. Como outro exemplo, um especialista entrevistado citou a autorregulação das medidas de luta contra o terrorismo na Internet, em oposição às regras impostas externamente. Mais amplamente, outro especialista entrevistado salientou a necessidade de um acordo internacional sobre normas de jurisdição na Internet, porque, embora as empresas devam ser incentivadas a fazer a autorregulação, os governos também precisam assumir a responsabilidade.

No entanto, é possível que o vento esteja mudando no que tange à autorregulação das empresas (mesmo nos EUA). Na verdade, a ICANN hoje poderia ser vista como uma organização mais híbrida, já que os governos desempenham um papel crescente na sua regulação.

Se esta mudança de paradigma foi concluída, se está meramente em curso, ou até se é mesmo exagerada, pode ser um assunto aberto para discussão. No entanto, é inegavelmente verdadeiro o fato de que estamos assistindo a sinais destas tendências, que são simultaneamente impulsionadas pelo ambiente on-line e têm um impacto fundamental nas questões da Internet transfronteiriça que suscitam preocupação neste relatório.

Além disso, embora nos afastemos da Declaração de Barlow, a era da chamada autorregulação de modo algum acabou. E, de fato, existem vários tipos de regulamentação a se destacar no cenário on-line, incluindo:

1. regulação do direito privado;
2. regulação do direito público;
3. acordos públicos-privados;
4. autorregulação; e
5. código técnico ou *lex informatica*.[49]

Os quatro primeiros, mas normalmente não o quinto, destes tipos de regulação podem ser específicos do país e variar consideravelmente de país para país. Isso complica ainda mais o cenário regulatório.

Aqui podemos fazer uma pausa para considerar como as iniciativas regulatórias, enquadradas nesses diferentes tipos

regulatórios, de diferentes partes do mundo interagem.

Pelo menos cinco opções podem ser identificadas.

Diferentes iniciativas regulatórias podem:

1. resultar em confrontos fundamentais;
2. resultar em confrontos menores;
3. coexistir sem interação;
4. estar inter-relacionados; ou
5. ser interdependentes.

Em última análise, independentemente do tipo regulatório, regular a Internet requer uma mão firme e uma mente serena. A história já provou que tanto a falta de ação como a ação exagerada podem ser prejudiciais para este ambiente sensível e, de fato, frágil.

2.2.2. Proliferação de iniciativas

Uma infinidade de novas iniciativas de atores públicos e privados de todo o mundo foram anunciadas ou adotadas para abordar as questões em jogo. Estas incluem novas leis nacionais, diretrizes, opiniões, códigos de conduta, modelos de leis, convenções de acordos multilaterais, declarações e políticas da empresa. Muitas dessas iniciativas são discutidas no Capítulo 3, que delineia as principais tendências atuais, e no Capítulo 4, que analisa uma série de abordagens jurídicas e técnicas.

Neste contexto, é útil fazer uma pausa para considerar o endurecimento da chamada *soft law* (medidas não vinculantes) que é cada vez mais evidente.[50] A *soft law* que assume uma posição sobre a interpretação adequada de leis complexas, como os pareceres e orientações emitidos por muitas autoridades designadas ou outros organismos, assume frequentemente um papel praticamente indistinguível da *hard law*, como a legislação e a jurisprudência. Isto não ocorre apenas no ambiente on-line, mas talvez se possa dizer que é particularmente prevalente na regulação da Internet.

Em qualquer caso, os desenvolvimentos intensivos sobre desafios jurídicos transfronteiriços on-line sinalizam que estas questões estão sendo levadas a sério, o que é certamente importante. No entanto, ações descoordenadas, tomadas de forma reativa sob a pressão da urgência, criam uma corrida armamentista legal com impactos potencialmente prejudiciais - uma corrida armamentista envolvendo a implementação ativa de medidas ao invés de simplesmente armazenar medidas potenciais. Garantir que a

multiplicação de diferentes regimes não crie tensões adicionais, ou mesmo conflitos, é um grande desafio.

O grau em que os Estados procuram aplicar suas leis às atividades na Internet não tem sido estático ao longo dos anos. De fato, é possível identificar um padrão de oscilações do pêndulo entre o que pode ser descrito como "subrregulação jurisdicional" de um lado, e "superregulação jurisdicional" do outro.[51]

Hoje, o ambiente regulamentar está claramente pendendo para a superregulação jurisdicional. Na verdade, o apetite com que os Estados estão tentando expandir sua jurisdição e aplicar suas leis às atividades na Internet é sem precedentes. Assim, pode-se falar disso como uma era de 'hiper-regulação' jurisdicional caracterizada pelas seguintes condições:

1. a complexidade do sistema jurídico contextual de uma parte (isto é, a combinação de todas as leis que pretendem aplicar-se a essa parte numa determinada questão — ver mais no Capítulo 2.2.6) constitui um obstáculo insuperável à adequação legal; e
2. o risco de cumprimento das leis (ou ao menos partes delas) que compõem o sistema jurídico contextual é mais do que uma possibilidade teórica.

Um especialista entrevistado enfatizou que os governos estão buscando controlar o ambiente on-line, o que resulta na criação de mais leis, já que sua resposta típica é introduzir novas leis em vez de aplicar leis existentes para enfrentar os desafios.

Uma tendência relacionada é o ritmo acelerado de mudanças nas agendas políticas e regulamentos. Por exemplo, várias questões on-line que ganharam atenção limitada há apenas alguns anos, como o bullying on-line, a disseminação do discurso de ódio e a distribuição não consensual de conteúdo sexualmente explícito, são agora amplamente reconhecidos como problemas. A constante mudança de prioridades e atenção de um tópico para outro, muitas vezes estimulada pelos meios de comunicação, cria uma sensação de urgência que deixa os governos com tempo insuficiente para decidir ou coordenar abordagens.

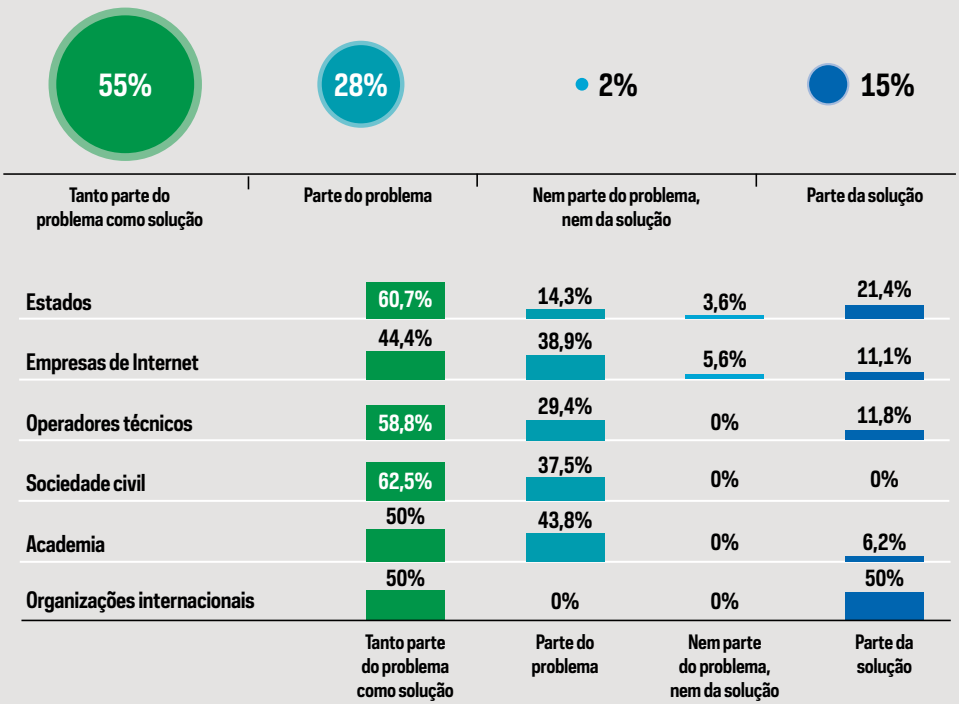
2.2.3. Um apetite crescente para regular o ciberespaço

Alguns especialistas entrevistados observaram que, embora no passado os governos em grande parte tinham a visão de que a regulação da Internet era difícil ou impossível, a vontade polí-

tica para regular a Internet está agora mais forte do que nunca. De fato, líderes da indústria de tecnologia também estão, cada vez mais, pedindo mais regulação.[52]

INFOGRÁFICO 10

MAIOR REGULAÇÃO DO CIBERESPAÇO: PROBLEMA OU SOLUÇÃO?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Pouco mais de metade dos especialistas pesquisados indicaram que veem isso como parte do problema e parte da solução. Mais detalhadamente, 55% indicaram que o aumento da execução da legislação nacional em casos envolvendo servidores, usuários ou empresas localizados em outros países faz parte do problema e parte da solução. 28% consideraram isso apenas como parte do problema, enquanto que 15% viram-no apenas como parte da solução. 2% viram o aumento da execução das leis nacionais em casos envolvendo servidores, usuários ou

empresas localizadas em outros países como não sendo parte do problema nem parte da solução.

Em suas observações, os especialistas consultados manifestaram preocupações relativamente ao reforço da aplicação das legislações nacionais nos casos que envolvam servidores, usuários ou empresas localizadas em outros países. Em particular, os especialistas pesquisados apontaram preocupações sobre arbitrariedade, incerteza, consequências não intencionais, impactos inadequados e uma tensão entre as prioridades do Estado e uma visão global. Outros observaram que, embora a adesão aos tratados seja ideal, na sua ausência, as leis nacionais extraterritoriais — se devidamente implementadas — são uma solução provisória sensata. Algumas argumentaram também que as tentativas unilaterais destacam fraquezas nos regimes existentes e, como tal, funcionam como um catalisador inevitável para a mudança a longo prazo.

Houve claras diferenças setoriais sobre esta questão da pesquisa, sendo os atores do setor governamental e das organizações internacionais consideravelmente mais positivos em relação a estes avanços.

2.2.4. Excesso de informações e acesso a informações

Para avançar com os desafios jurídicos transfronteiriços na Internet da forma mais bem-sucedida possível, todos os atores devem ter acesso a informações relevantes. Na verdade, esta é uma das razões para este Relatório. No entanto, tanto o feedback fornecido pelos especialistas entrevistados quanto pelos pesquisados, bem como o próprio processo de redação do relatório revelaram os atuais obstáculos que impedem o nível de acesso necessário para o desenvolvimento de políticas informadas.

Um especialista consultado salientou que a tradução da ordem judicial é uma questão importante e sugeriu que talvez um idioma deva ser escolhido como idioma oficial, tal como nas relações diplomáticas. Alguns especialistas entrevistados apontaram para o forte domínio da língua inglesa como um problema atual no contexto do acesso à informação, observando que o custo das traduções é um fator limitante. No entanto, também foi observado que esta barreira atual provavelmente irá diminuir, uma vez que as gerações mais jovens em muitos países têm altos níveis de proficiência em inglês.

Um especialista entrevistado fez a observação importante de que os materiais que estão disponíveis apenas em uma língua estrangeira obrigam o leitor a confiar em fontes secundárias, que muitas vezes não têm nuance e são escritos para um público generalista. Esta realidade assola todos os grupos de atores e é também uma preocupação legítima em relação a alguns dos materiais invocados neste Relatório.

Um especialista consultado afirmou que o acesso à informação se dá principalmente em escala regional. Outro observou que, embora existam informações substanciais disponíveis sobre decisões nos EUA e na Europa, não há muita informação sobre decisões e avanços noutros Estados — incluindo sua fundamentação, leis e a interpretação dessas leis. Isto pode ser visto como um apelo para que os Estados em todo o mundo se empenhem mais para fornecer e promover o acesso gratuito on-line às suas leis e decisões judiciais, de preferência com os principais avanços acessíveis em vários idiomas.

Esta observação é igualmente interessante em relação à falta generalizada de problematizações e exemplos de outras regiões (fora da UE e dos EUA) nas discussões sobre desafios jurídicos transfronteiriços na Internet — um problema fortemente enfatizado por numerosos especialistas entrevistados e pesquisados. Especialistas entrevistados e pesquisados observaram que muito está sendo feito para garantir a diversidade regional nas discussões, incluindo uma maior representação dos países em desenvolvimento. No entanto, pode-se razoavelmente supor que parte do problema decorre dos desenvolvimentos vindos da UE e dos EUA terem se tornado o denominador comum nas discussões, em parte devido à sua acessibilidade. Consequentemente, estes desenvolvimentos ganham maior atenção à custa de exemplos de outras regiões, mesmo quando essas regiões estão representadas nas discussões.

> **Para avançar com os desafios jurídicos transfronteiriços na Internet da forma mais bem-sucedida possível, todos os atores devem ter acesso a informações relevantes.**

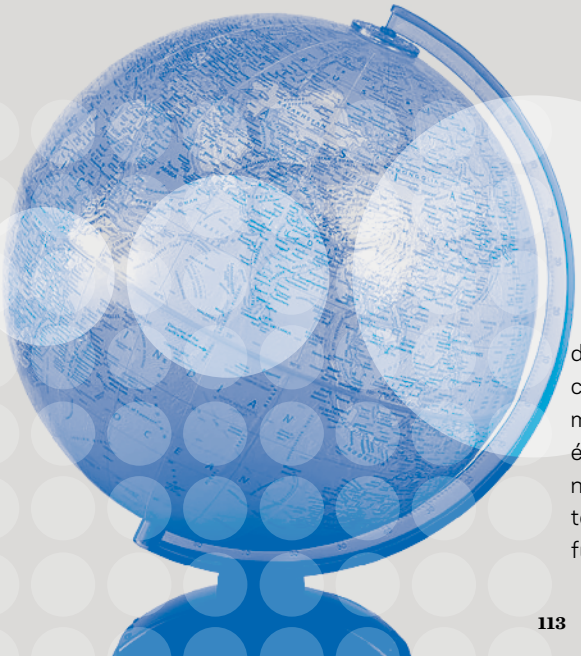
VARIAÇÃO NO ACESSO A MATERIAIS DE DIFERENTES REGIÕES

Numerosos especialistas consultados e entrevistados apontaram a I&J Retrospect Database da Rede de Políticas Internet & Jurisdição como a principal fonte de informações sobre atores e iniciativas relevantes, detalhes das leis relevantes e sua aplicação, bem como de decisões judiciais relevantes sobre os desafios jurídicos transfronteiriços da Internet.

No entanto, a ampla variação no acesso aos materiais de diferentes regiões também se reflete na Retrospect Database da Rede de Políticas Internet & Jurisdição.[53]

Por exemplo, um exame dos casos relatados durante o ano de 2018 — 240 no total — revelam as seguintes estatísticas:

- 95 deles lidam exclusivamente com a Europa e outros 12 envolvem a Europa e pelo menos uma outra jurisdição;
- 28 casos tratam exclusivamente da América do Norte e outros 12 envolvem a América do Norte mais pelo menos uma outra jurisdição;
- 19 casos são geograficamente neutros;
- 17 casos tratam exclusivamente da Ásia (além da China, Índia e Rússia) e outro 1 caso envolve Ásia (além da China, Índia e Rússia) e pelo menos uma outra jurisdição;
- 14 casos tratam exclusivamente da Rússia e 1 caso envolve a Rússia e pelo menos uma outra jurisdição;
- 10 casos tratam exclusivamente da Índia e 1 caso envolve a Índia e pelo menos uma outra jurisdição;
- 9 casos tratam exclusivamente da América do Sul e outros 2 envolvem a América do Sul mais pelo menos uma outra jurisdição;
- 8 casos tratam exclusivamente da Austrália/Nova Zelândia e outros 2 envolvem Austrália/Nova Zelândia mais ao menos uma outra jurisdição;
- 9 casos tratam exclusivamente da China;
- 9 casos tratam exclusivamente de África; e
- 7 casos tratam exclusivamente do Oriente Médio e 1 caso envolve o Oriente Médio mais pelo menos uma outra jurisdição.



Embora a Retrospect Database da Rede de Políticas Internet & Jurisdição destine-se claramente a coletar informações de todo o mundo, a prevalência de materiais europeus é, no entanto, esmagadora. Isso demonstra a necessidade de mais e melhor compartilhamento de informações e aponta para a utilidade de futuros relatórios regionais.

Neste contexto, vale a pena enfatizar que o compartilhamento de informações corresponde a impacto. Por exemplo, se uma pessoa da América do Sul conhece alguém da Ásia e nenhum deles sabe muito sobre as leis e abordagens do outro, mas ambos têm uma compreensão básica das abordagens europeias e norte-americanas, talvez eles possam basear sua discussão no conhecimento comum que compartilham. Isto resulta numa influência desproporcional das legislações europeia e norte-americana, que é uma questão-chave tanto para o reforço das capacidades como para a inclusão. Aqui a questão do idioma discutido acima pode ser usada de forma proveitosa. Uma proficiência crescente da língua inglesa pode erradicar as barreiras linguísticas atuais no lado do receptor; ou seja, o acesso a materiais da língua inglesa em Estados não ingleses pode não ser um grande problema. No entanto, as barreiras linguísticas continuarão a ser um obstáculo considerável do lado do provedor. O resultado provável é que as pessoas de Estados não ingleses estão se tornando hábeis em acessar/consumir informações em inglês, mas ainda não têm meios eficazes para tornar suas leis em idioma que não seja o inglês acessíveis a pessoas que não falam seu idioma. Assim, o aumento da proficiência em inglês pode funcionar contra a influência de países que não falam inglês.

A necessidade de capacitação foi um tema recorrente nos comentários de especialistas entrevistados e consultados, sendo relevante também nesse contexto. Por exemplo, um especialista entrevistado comentou a importância de desenvolver uma nova forma para educar tomadores de decisão, legisladores e outros, de modo a que a discussão permaneça robusta em termos de tradição jurídica, mas de uma forma que possa ser facilmente compreendida para evitar que esses atores "se desliguem". Especialistas entrevistados do setor tecnológico fizeram comentários semelhantes sobre o desenvolvimento de capacidades, com alguns enfatizando a necessidade de legisladores e de autoridades entenderem a tecnologia e a terminologia.

2.2.5. Cada problema tem uma solução, mas cada solução tem um problema

Pode-se argumentar que a criatividade judicial e legislativa diminuiu nos últimos anos. No entanto, foram e estão a ser avançadas soluções para resolver as complicações relacionadas ao estabelecimento da jurisdição pessoal de um tribunal sobre

um réu em outro território. Muitos se recordarão, por exemplo, do teste da "escala móvel" articulado pelos tribunais americanos em meados da década de 1990, que procurou organizar os websites por referência à sua "interatividade".[54] E do famoso processo na Suprema Corte da Austrália, de 2002, entre a editora americana Dow Jones e o empresário Gutnick, de Vitória — no qual, pela primeira vez, a mais alta corte de um Estado julgou a questão de jurisdição sobre difamação transfronteiriça na Internet — o Juiz Kirby determinou que a solução fosse encontrada na doutrina do *forum non conveniens*.[55]

Estas soluções, como muitas outras, não resistiram à prova do tempo. Mas a autocontenção judicial que o Juiz Kirby antecipou na forma de *forum non conveniens* ainda é frequentemente citada como uma solução potencial, mesmo que as atitudes dos tribunais em relação à jurisdição pareçam estar se afastando da autocontenção.[56]

Por conseguinte, poucas soluções propostas são verdadeiramente "novas" e ater-se ao fato de elas serem ou não, indiscutivelmente, não é a abordagem mais frutífera. Mais importante, então, é o quão bem uma determinada solução aborda as preocupações em questão.

A realidade é que as questões jurisdicionais on-line e off-line são complexas e, tendo em vista as tentativas de encontrar soluções, parece claro que soluções perfeitas são improváveis; de fato, a busca pela perfeição pode tornar-se um obstáculo ao progresso. E dado que o mundo é cada vez mais caracterizado pela complexidade, chegar a um tratado internacional abrangente para resolver os inúmeros desafios jurídicos transfronteiriços on-line é altamente improvável no futuro previsível e até mesmo distante.

Em vez de esperar que os problemas desapareçam, ou que sejam resolvidos por um improvável tratado internacional, os atores devem continuar a trabalhar em muitas frentes diferentes e assegurar que o seu trabalho seja o mais coordenado possível. Esse trabalho também deve ser fundamentado em sólidos quadros conceituais — um componente que é tipicamente fornecido pela pesquisa acadêmica.

No entanto, apesar do papel central que a Internet desempenha na sociedade moderna e de seu crescente destaque nas discussões políticas, os desafios jurídicos transfronteiriços na Internet continuam a ser tratados como questões marginais na literatura acadêmica jurídica — sobretudo nos domínios do

direito internacional público e privado. Isto é insustentável. As questões jurídicas transfronteiriças relacionadas à Internet são questões centrais da sociedade atual, e isso deve se refletir nos debates sobre direito internacional público e privado.

Lamentavelmente, parece que as questões jurídicas sobre jurisdição da Internet estão recebendo menos atenção na literatura acadêmica jurídica.

Os desafios jurídicos transfronteiriços surgem em praticamente todos os domínios do direito material e são frequentemente abordados e debatidos no contexto de cada área. Por exemplo, estes desafios podem ser discutidos no contexto de reforma do direito da propriedade intelectual, de leis de difamação, de crimes cibernéticos ou da tributação.

É igualmente importante reconhecer que se pode abordar os desafios jurídicos transfronteiriços na Internet como um tema *per se* e não apenas como um componente de diferentes áreas do direito material. Isso revela até que ponto surgem desafios jurisdicionais idênticos ou semelhantes em diferentes contextos, permitindo que soluções e abordagens de um contexto sejam transpostas para outro. Neste campo, é necessário mais trabalho "meta-nível".

> **Soluções perfeitas são improváveis [...] a busca pela perfeição pode se tornar um obstáculo ao progresso.**

AS QUESTÕES JURISDICIONAIS REPRESENTAM UMA PARCELA DECRESCENTE DO TRABALHO ACADÊMICO

Ano	1994 – 1998	1999 – 2003	2004 – 2008	2009 – 2013	2014 – 2018
Número total de artigos sobre questões de jurisdição na Internet[57]	841	1.997	1.451	1.501	1.281
Número total de artigos sobre a Internet[58]	13.762	31.646	34.680	39.292	37.981
Porcentagem de artigos abordando questões de jurisdição na Internet do total de artigos sobre a Internet	6,1%	6,3%	4,2%	3,8%	3,4%

2.2.6. Aumento da insegurança jurídica

As atividades de pessoas físicas (indivíduos) e pessoas jurídicas (empresas e outras organizações) são reguladas por lei. No ambiente off-line, normalmente é bastante fácil identificar a lei aplicável. Por exemplo, uma pessoa dirigindo um carro em estradas na Alemanha está sujeita às regras de trânsito alemãs. Identificar a(s) lei(s) aplicável(eis) on-line é muitas vezes mais complicado.

Ao enviar um e-mail da Argentina para o Japão, por exemplo, uma pessoa pode estar sujeita tanto às leis da Argentina quanto às do Japão. No entanto, quando a mesma pessoa na Argentina publica um comentário difamatório sobre uma pessoa na Finlândia em um site de mídia social, ela pode estar sujeita não apenas às leis da Argentina e da Finlândia, mas às leis de todos os países em que ela tem contatos em sua rede de mídia social — e talvez qualquer lei especificada em seu acordo com a plataforma de mídia social. Como mostra este exemplo, é importante ter em mente que as leis aplicáveis são determinadas pelas atividades que realizamos.

Para entender as complicações que surgem, é útil pensar nas leis que se aplicam a uma pessoa em determinada situação como um "sistema jurídico contextual" — isto é, um sistema de regras jurídicas de diferentes Estados que se aplicam todas à atividade exercida por essa pessoa. É claro, então, que, no exemplo envolvendo um e-mail enviado da Argentina para o Japão, o sistema jurídico contextual é menos complexo (porque consiste nas regras legais de dois Estados) do que o último exemplo envolvendo uma postagem difamatória de mídia social.

Um problema sério do ambiente on-line é que as pessoas são muitas vezes incapazes de prever todas as leis dos Estados que fazem parte de seu sistema jurídico contextual para qualquer atividade. Mesmo quando as pessoas podem verificar quais as leis estatais lhe são aplicáveis, nem sempre é fácil acessar todas essas leis. Com efeito, mesmo nos casos em que o acesso pode ser assegurado, as questões linguísticas podem impedir a plena compreensão dessas leis. Além disso, as regras de um sistema jurídico interno são tipicamente estruturadas para evitar situações em que uma regra jurídica exige algo que outra regra jurídica proíbe. No entanto, quando um sistema jurídico contextual consiste em regras jurídicas de diferentes Estados

— como é normalmente o caso em relação às atividades on-line —, tal coordenação não pode ser presumida. Como resultado, não é incomum, no ambiente on-line, que uma norma jurídica, dentro de um sistema jurídico contextual relevante, exija algo que outra norma jurídica dentro do mesmo sistema proíba. Esta falta de harmonização legal, embora natural considerando a forma como o mundo está organizado, é um obstáculo importante, pois cria um ambiente em que a garantia do cumprimento legal é difícil ou mesmo impossível.

Isto impõe desafios práticos óbvios. Em um nível mais profundo, também mina a legitimidade de pelo menos um princípio jurídico fundamental: o princípio segundo o qual o desconhecimento da lei é inescusável (*Ignorantia juris non excusat*), que constitui uma pedra angular de qualquer sistema jurídico em funcionamento. Se alguém reconhece que o ambiente regulatório on-line torna muitas vezes impossível ser informado sobre suas obrigações legais, é difícil sustentar que o desconhecimento da lei não desculpa ninguém. Por enquanto, a impossibilidade geral de conhecer todas as leis que se pretendem aplicáveis e o fato de que a ignorância da lei geralmente é inescusável parecem irreconciliáveis, afetando tanto as tendências atuais (Capítulo 3) quanto as abordagens jurídicas e técnicas (Capítulo 4).

Além disso, em qualquer situação que envolva conflito de normas, não devemos nos limitar a algo tão grosseiro como avaliar se as leis de um determinado país se aplicam à situação, porque nem todas as leis de um país são relevantes para qualquer situação específica.

Imagine que a pessoa jurídica Y do Estado A celebra um contrato de compra com a pessoa física Z do Estado B. Se o Estado B quiser aplicar suas leis de proteção ao consumidor à situação, essas leis do Estado B podem ter uma conexão substancial com a questão e o Estado B pode ter um interesse legítimo em aplicar essas leis de defesa do consumidor. No entanto, se o Estado B, baseado no mesmo conjunto de fatos, pretende aplicar suas leis de governança corporativa à Y, a conexão é mais fraca e o interesse em fazê-lo é menos legítimo. Para levar este exemplo ao extremo, imagine que, com base no cenário mencionado, o Estado B quer aplicar suas leis matrimoniais a todos os funcionários da pessoa jurídica Y; então tanto a conexão quanto o interesse são inexistentes.

Assim, qualquer avaliação quanto à aplicabilidade das leis do Estado B depende de quais normas esse Estado procura aplicar. É a aplicabilidade de normas individuais de um determinado Estado, em vez da totalidade de suas leis, que deve estar em foco. Esta maior granularidade deve refletir-se nas regras de direito internacional privado, especialmente quando afetam o ambiente on-line.

> **Um problema sério do ambiente on-line é que as pessoas são muitas vezes incapazes de prever todas as leis dos Estados que fazem parte de seu sistema jurídico contextual para qualquer atividade. Mesmo quando as pessoas podem verificar quais as leis estatais lhes são aplicáveis, nem sempre é fácil acessar todas essas leis.**

2.3. Repensar o papel da territorialidade

No que se refere à questão da jurisdição, a territorialidade visa a essencialmente desempenhar duas funções. A primeira consiste em estabelecer um critério para quando um Estado pode reivindicar jurisdição. No entanto, on-line, é particularmente fácil encontrar pontos de ancoragem territoriais para demandas jurisdicionais. A segunda função da territorialidade é atuar como um "sinal de parada" que fornece um aviso quando se entra no domínio exclusivo de outro Estado. Aqui novamente, porém, a territorialidade falha on-line.

É simplesmente irreal pensar que um Estado fará parte da comunidade global e ainda gozar da exclusividade tradicional, no sentido Westfaliano.

Na verdade, parece cada vez mais óbvio que a distinção entre reivindicações jurisdicionais territoriais e extraterritoriais é equivocada. Isso ocorre porque:

1. Não existe acordo (internacional) sobre quando uma reivindicação de jurisdição é extraterritorial (o que, assumindo que extraterritorial é o oposto de territorial, exclui logicamente qualquer acordo sobre quando uma reivindicação de jurisdição é territorial); e

2. Algumas reivindicações de jurisdição "extraterritoriais" são claramente apoiadas no direito internacional, como é o caso, por exemplo, no âmbito do princípio da nacionalidade. Com efeito, as exceções a uma adesão estrita à territorialidade são agora tão numerosas que a territorialidade já não pode ser vista como a base jurisprudencial da jurisdição.

Mesmo quando uma regra jurisdicional é redigida em termos de critérios territoriais, o seu verdadeiro objetivo subjacente é determinar se o Estado que faz o pedido jurisdicional tem uma ligação suficientemente forte com a questão para criar um interesse legítimo em reivindicar a jurisdição; um critério territorial é meramente uma procuração para este objetivo subjacente. Por exemplo, enquanto o Artigo 3 do GDPR pretende delinear o escopo de aplicação do GDPR em um sentido espacial, ele realmente faz isso de uma maneira que é tanto dependente da territorialidade quanto independente da territorialidade. No final, a natureza binária da distinção entre territorial vs. extraterritorial não explica a verdadeira natureza da realidade com a qual trabalhamos.

Falar de extraterritorialidade é semelhante a descrever carros como "carruagens sem cavalos" — ambas as descrições são fundadas numa noção equivocada do que é "normal". Embora o termo "extraterritorialidade" ainda seja amplamente utilizado por razões de conveniência, devemos estar conscientes de que a extraterritorialidade, como conceito, foi desacreditada.[59]

Está bem estabelecido e para além de uma disputa inteligente que o foco do direito internacional na territorialidade não se coaduna bem com a fluidez do ambiente on-line, o qual se caracteriza por uma constante e substancial interação transfronteiriça. No entanto, até recentemente, pouco tinha sido feito, e ainda menos alcançado, na busca de desembaraçar a jurisdição da Internet da territorialidade.

Em documentos de política e escritos acadêmicos, a fonte mais comumente citada para um foco de territorialidade é o clássico caso *Lotus*[60], que foi decidido pelo Tribunal Permanente de Justiça Internacional em 1927. Este caso diz respeito à colisão entre dois navios.

> **Em vez de admitir que a ausência de jurisprudência relevante significa que esta é uma área de direito instável, tem havido uma tendência de sobrevalorizar inapropriadamente a decisão do caso *Lotus*.**

Embora os princípios articulados em uma configuração possam ser legitimamente aplicados a casos em outros contextos, os casos relativos à colisão de navios diferem claramente dos que se encontram no contexto da jurisdição da Internet. E, embora os princípios jurídicos não devam ser abandonados apenas porque são velhos, também não devem deixar de ser reavaliados apenas porque são velhos. Dado que os métodos legais gerais exigem tratar diferentes casos distintamente, parece haver pouco sentido em fundamentar nosso pensamento sobre a jurisdição da Internet na decisão do caso *Lotus*. De fato, a opinião majoritária no caso *Lotus* enfatizou a necessidade de se concentrar em "precedentes que oferecem uma estreita analogia ao caso em questão; pois é apenas a partir de precedentes desta natureza que a existência de um princípio geral aplicável ao caso particular pode aparecer."[61]

Talvez a verdadeira razão pela qual a decisão do caso *Lotus* ainda recebe tanta atenção seja o fato de haver tão poucas outras decisões internacionais sobre este tema. Em vez de admitir que a ausência de jurisprudência relevante significa que esta é uma área de direito instável, tem havido uma tendência de sobrevalorizar inapropriadamente a decisão do caso *Lotus*.

Além disso, o acórdão *Lotus* não é uma base particularmente sólida para o princípio da territorialidade, porque contém contradições e carece de clareza em algumas áreas. É também uma decisão em que nada menos de metade dos membros do tribunal expressou uma opinião dissidente, e não há sequer qualquer acordo quanto ao tipo de jurisdição — prescritiva, adjudicatória ou de execução — que envolveu o caso *Lotus*.

À medida que o papel da estrita territorialidade diminui no contexto da jurisdição, outra coisa deve ocupar o seu lugar como o núcleo jurisprudencial das reivindicações jurisdicionais. No contexto de execução de decisões para acesso às provas digitais, há, pelo menos, sinais de um consenso emergente[62] para se concentrar em saber se o Estado que reivindica a jurisdição tem um interesse legítimo e uma ligação substancial com a questão em

apreço, combinada com uma avaliação da consideração de outros interesses.[63] As discussões relativas às questões jurídicas transfronteiriças associadas ao acesso de autoridades estatais a provas digitais estão relativamente avançadas e, como observou um especialistas entrevistado, este domínio é um dos principais motores das questões jurídicas transfronteiriças. Portanto, a confiança neste quadro de três fatores pode se espalhar, uma vez que também pode ser aplicada a outros contextos em que é necessário impor normas sobre as reivindicações de jurisdição.[64] Concentrar-se em saber se o Estado que reclama a jurisdição tem um interesse legítimo e uma relação substancial com a questão em apreço, combinada com uma apreciação da consideração de outros interesses, tem a vantagem de incorporar uma vasta gama de conceitos complexos de direito internacional, sendo também facilmente compreensível. Esta facilidade de utilização torna-o um instrumento eficaz para superar alguns dos "desafios regulatórios artificiais" associados a questões jurídicas transfronteiriças na Internet. Além disso, se beneficia por ser relevante tanto para assuntos que tradicionalmente são abrangidos pelo direito internacional público quanto para aqueles que tradicionalmente se encontram no direito internacional privado (ou conflito de leis).

2.3.1. Um alcance geográfico crescente de legislações nacionais

Quando as regras jurisdicionais são amplas, correm o risco de capturar comportamentos com os quais não há um grau de contato suficiente para justificar a reivindicação jurisdicional de um Estado. Isso pode levar ao exercício de jurisdição sobre partes sem uma notificação adequada. Ao mesmo tempo, quando as regras jurisdicionais são limitadas, correm o risco de deixar as vítimas sem reparação judicial. Acertar o equilíbrio não é tarefa fácil e focar nas distinções entre territorialidade e extraterritorialidade frequentemente leva a ambos esses problemas.

Muitos Estados fazem amplas reivindicações de jurisdição sobre atividades na Internet — reivindicações que, possivelmente, eles não podem sustentar com uma execução efetiva. Enquanto comum, tais "arrastões jurisdicionais" constituem muitas vezes uma abordagem regulatória destrutiva, especialmente quando conduz a uma aplicação arbitrária, o que, como salientaram os especialistas entrevistados, é pouco compatível com o Estado de Direito.

Além disso, à medida que os Estados competem para que as suas leis sejam respeitadas, muitos estão aumentando as potenciais multas para aqueles que não as cumprem. Isso é problemático nos casos em que o cumprimento da lei de um Estado exige a violação da lei de outro Estado.

O referido "arrastão jurisdicional" e as multas de elevado potencial são apenas dois exemplos de Estados que flexionam os músculos em relação à Internet. Comparando a questão da jurisdição on-line e off-line, sem dúvida a maior diferença é que, para a jurisdição on-line, há uma maior necessidade de vincular a questão de uma reivindicação de jurisdição ser apropriada com a questão sobre qual jurisdição é reivindicada. Em outros termos, é mais difícil, no contexto on-line, determinar quais os aspectos da atividade de uma pessoa física ou jurídica são capturados por uma reivindicação jurisdicional e quais não são. Este é um tema que até agora ganhou pouca atenção, e há uma clara necessidade de ferramentas mais sofisticadas para garantir que as reivindicações de jurisdição não sejam mais amplas do que o necessário para alcançar os objetivos dos legisladores.[65]

No entanto, talvez o maior desafio esteja relacionado com a tentativa de mudar as atitudes. Muitas vezes, o objetivo das regras de jurisdição é meramente promover os objetivos de política interna das leis materiais pertinentes. Por exemplo, se a lei de difamação visa a proteger a reputação dos indivíduos, o objetivo das regras jurisdicionais relevantes é percebido como sendo a lei material sobre difamação tão amplamente aplicável quanto possível, alargando globalmente a reivindicação de jurisdição. Mas isso é muito simplista. O papel subjacente das regras de jurisdição deve consistir sempre em procurar a aplicação efetiva do direito material, minimizando, ou mesmo evitando, o risco de tensões e conflitos internacionais, sem impor encargos excessivos àqueles submetidos à regulação.

2.3.2. Desafios da executoriedade

É fácil entender por que os Estados querem que suas leis sejam respeitadas on-line da mesma forma como são respeitadas off-line. De fato, da forma como o mundo está estruturado hoje, é possível compreender cada Estado como tendo o direito de ditar o que está disponível on-line nesse Estado. Ao mesmo tempo, apesar da legitimidade óbvia de sua ambição de paridade legal on-line e off-line, há várias outras considerações que devem fazer parte da equação.

Em primeiro lugar, alegar simplesmente que as leis de um Estado se aplicam em todo o mundo on-line não faz com que isso seja assim. O direito internacional impõe algumas restrições — embora vagas — sobre quando um Estado pode alegar que as suas leis se aplicam. Além disso, a capacidade de um Estado fazer cumprir suas leis é muitas vezes mais limitada do que as reivindicações que faz sobre o alcance de suas leis.

Em segundo lugar, à medida que os Estados fazem reivindicações jurisdicionais mais amplas, podem tornar-se cada vez mais dependentes da cooperação de outros Estados para a execução dessas alegações. Por conseguinte, embora reivindicações mais amplas de jurisdição possam conduzir a confrontos óbvios em alguns casos, podem também incentivar uma maior cooperação e coordenação entre os Estados.

Qualquer impacto positivo potencial de reivindicações jurisdicionais mais amplas pode ser perdido quando os Estados se contentam em limitar-se ao que pode ser denominado "execução interna de reivindicações extraterritoriais". Em vez de confiar na execução pela cooperação de Estados estrangeiros, os Estados, neste cenário, podem impor "medidas de destruição do mercado" ao agente estrangeiro, tais como restringir o seu acesso aos usuários no país em questão.[66] Tais exercícios de "soberania de mercado" parecem estar aumentando em frequência.

Em terceiro lugar, quando um Estado alega que as suas leis se aplicam a determinadas atividades on-line, tem de estar preparado para aceitar reivindicações igualmente amplas de outros Estados.

Em quarto lugar, a hiper-regulação jurisdicional (Capítulo 2.2.2) impõe um custo significativo de conformidade a todas as pessoas físicas e jurídicas que pretendam respeitar as leis aplicáveis. Em quinto lugar, existe o risco de que as pessoas físicas e jurídicas que busquem cumprir todas as leis aplicáveis adotem os padrões mais rigorosos, segundo a lógica de que o cumprimento das normas mais rigorosas garante o cumprimento de todas as leis relevantes. Tal abordagem é imprudente, uma vez que não existe um Estado que tenha as leis mais rigorosas sobre todos os temas. Assim, para saber qual lei é a mais rigorosa sobre qualquer tópico, é preciso conhecer todas as leis de todos os Estados do mundo. Além disso, pode desencadear um "nivelamento por baixo" com o risco de consequências irreversíveis para a diversidade on-line.

Em conjunto, essas considerações sugerem que o objetivo legítimo de ter leis estatais respeitadas on-line da mesma forma que off-line deve ser perseguido de forma cuidadosa e inteligente. Em nossa atual era de hiper-regulação jurisdicional (Capítulo 2.2.2), há uma clara meta-tendência de Estados que fazem uma dicção demasiado ampla, em que reivindicações de jurisdição mais limitadas, inteligentes e matizadas:

1. seriam mais fáceis de defender moralmente e ao abrigo do direito internacional;
2. seriam mais fáceis de executar;
3. imporiam custos de conformidade mais baixos; e
4. seriam menos propensas a incentivar reivindicações excessivamente amplas de jurisdição por parte de outros Estados.

> **À medida que os Estados fazem reivindicações jurisdicionais mais amplas, podem tornar-se cada vez mais dependentes da cooperação de outros Estados para a execução dessas alegações. Por conseguinte, embora reivindicações mais amplas de jurisdição possam conduzir a confrontos óbvios em alguns casos, podem também incentivar uma maior cooperação e coordenação entre os Estados.**

2.3.3. Quando a territorialidade é irrelevante

Tendo em conta o que precede, é natural que tenhamos assistido a um declínio lento, mas constante, no enfoque da territorialidade para fins jurisdicionais. Tal como discutido no Capítulo 3.2.2.3, alguns exemplos recentes incluem o US CLOUD Act de 2018; a *Proposta de Diretiva do Parlamento Europeu e do Conselho da UE que estabelece regras harmonizadas para a nomeação de representantes legais para efeitos de coleta de provas em processos penais*[67]; e a *Proposta da UE de Regulamento* do *Parlamento Europeu e do Conselho relativo relativo às ordens europeias de entrega ou de conservação de provas eletrônicas em matéria penal*.[68] O trabalho em curso sobre o segundo protocolo adicional do Conselho da Europa que altera a Convenção de Budapeste é outro exemplo. Além disso, o artigo 3 (1) do GDPR enfatiza especificamente que a localização do processamento de dados é irrelevante (Capítulo 3.1.6.1). Com estes instrumentos, a UE e os EUA estão a afastar-se da localização dos dados em questão e da territorialidade de forma mais ampla.

Observou-se também que a *soft law* é "um modelo regulamentar que desenvolve e estabelece regras independentemente do princípio da territorialidade".[69] Isto é significativo, uma vez que, como já foi referido, a *soft law* é particularmente prevalente na regulação da Internet.

A mudança da adesão cega à territorialidade como fundamento da jurisdição deve ser entendida à luz do fato de que o pensamento baseado na territorialidade incentiva a localização dos dados (capítulo 4.2.7) e a fragmentação de forma mais ampla. Além disso, como observado, a territorialidade, como conceito, sofre de várias fraquezas, especialmente quando aplicada em contextos on-line, onde determinar a localização de uma atividade específica requer entrar no atoleiro das ficções jurídicas.

> **A Jurisdição, como conceito jurisprudencial, não está enraizada na territorialidade.**

Ao mesmo tempo, deve-se notar que as dificuldades na aplicação do conceito de territorialidade não se limitam, de modo algum, ao ambiente on-line. Tais dificuldades são também comuns off-line, especialmente em campos como os direitos humanos, o direito da aviação e o direito anticoncorrencial. É tempo de reconhecer que aquilo que normalmente é discutido como "exceção" ao princípio da territorialidade é demasiado numeroso, e demasiado importante, para ser visto como mera exceção. Essas exceções devem, em vez disso, ser reconhecidas pelo que realmente são: indicadores de que a jurisdição, como conceito jurisprudencial, não está enraizada na territorialidade.

2.4. Pluralidade, convergência e fertilização cruzada de normas

É fato bem estabelecido que o direito não é o único fator que afeta a conduta on-line.[70] *Na verdade, o direito nem sempre tem o maior efeito sobre a conduta on-line. Isto tem profundas implicações.*

2.4.1. O desfocar das categorias

Especialistas entrevistados observaram que às vezes há uma linha tênue entre o discurso político legítimo, por um lado, e discurso de ódio ou conteúdo difamatório do outro.

Algumas medidas destinadas a remover o último correm o risco de suprimir o primeiro. Um especialista entrevistado também observou que não há um amplo acordo sobre as normas, comportamentos e tipos de conteúdo que são universalmente aceitáveis. As diferenças internacionais são grandes; o conteúdo pode ser classificado como discurso de ódio em uma jurisdição, por exemplo, ao passo que pode ser classificado como aceitável em outra.

Especialistas entrevistados enfatizaram este ponto fazendo uma comparação entre a forma como os EUA e a Alemanha tratam o discurso de ódio.

Num relatório de 2012, o Relator Especial da ONU sobre a Liberdade de Expressão apontou três tipos diferentes de expressão: (1) expressão que constitui uma ofensa ao abrigo do direito internacional e pode ser processada criminalmente; (2) expressão que não é criminalmente punível, mas pode justificar uma restrição e um processo civil; e (3) expressão que não dá origem a sanções penais ou civis, mas que ainda suscita preocupações em termos de tolerância, civilidade e respeito aos outros.

Essa continua sendo uma categorização útil e, como observou o Relator Especial, estas categorias de expressão impõem diferentes questões que exigem distintas respostas jurídicas e políticas.[71]

Se essas categorias não forem levadas em consideração, as distinções entre conteúdo ilegal, conteúdo que é contrário aos termos de serviço e conteúdo censurável podem ficar indistintas. Tal dissipação de contornos deve ser evitada, especialmente tendo em conta que, como afirmou a Comissão de Direitos Humanos da ONU, o artigo 19 do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP) protege a expressão de opiniões e ideias, mesmo que alguns indivíduos possam vê-los como profundamente ofensivos.[72]

Com base no trabalho acima mencionado, pode ser possível apontar para os seis tipos de expressão, a saber:

OS SEIS TIPOS DE EXPRESSÃO:

1. Expressão que constitui uma ofensa à luz do direito internacional e pode ser processada criminalmente
2. Expressão que constitui uma ofensa à luz do direito nacional e pode ser processada criminalmente
3. Expressão que não é criminalmente punível, mas pode ser reclamada nos termos do direito civil
4. Expressão que não é contra a lei aplicável, mas viola os termos de serviço relevantes ou outra *soft law*
5. Expressão que não é contra a lei aplicável, nem contra os termos de serviço relevantes ou outra *soft law*, mas é vista por alguns como censurável
6. Expressão que é totalmente incontroversa

Pode ser tentador ver esta estrutura como uma forma de classificação. Contudo, fazê-lo implica pelo menos uma simplificação inadequada: nem todas as leis são estabelecidas igualmente. Muitas vezes se argumenta que as leis devem superar os termos de serviço, porque as leis são o resultado de um processo democrático estabelecido, ao passo que os termos de serviço são unilateralmente impostos por empresas com fins lucrativos. Este raciocínio não carece de mérito, mas se a posição de superioridade das leis se baseia em seu pedigree democrático, o que acontece com as leis que não são baseadas em processos democráticos? Qual é, por exemplo, a relação adequada entre os termos de serviço e as leis ditatoriais destinadas a suprimir os movimentos democráticos? Este é um tema importante que merece um estudo mais aprofundado.

2.4.2. Harmonização através das normas da empresa

Outra tendência abrangente notável é o grau comparativamente elevado de harmonização transnacional através das normas de empresas, em contraposição ao fraturado estabelecimento de normas e tomadas de decisão com base no país. Existe um grau considerável de harmonização entre as normas (por exemplo, termos de uso, termos de serviço) implementadas pelas principais plataformas de Internet (baseadas nos EUA). Isso pode ser explicado, em parte, pelo fato de que essas plataformas estão sujeitas aos mesmos requisitos legais de vários Estados. Mas essa harmonização ultrapassa claramente os requisitos legais, o que sugere que deve ser entendida como

sendo do interesse das plataformas — embora até onde essa harmonização possa se expandir para além das plataformas de Internet dominantes é algo a ser acompanhado.

Em contrapartida, as leis dos diferentes Estados ainda não atingiram um grau de harmonização comparável. Tendo em conta a forma como as diferenças culturais, econômicas, sociais e religiosas impactam as leis fundamentais de cada Estado, tal harmonização parece improvável.

Especialistas entrevistados também chamaram a atenção para o espírito cooperativo entre as principais plataformas de Internet na busca de objetivos comuns, como a moderação de conteúdo. Como alguns especialistas entrevistados observaram, existe menos espírito de cooperação entre os Estados, além da cooperação setorial no contexto, por exemplo, da execução da lei. Na verdade, os especialistas entrevistados observaram uma clara tendência do individualismo entre os Estados, com cada Estado priorizando seu próprio interesse imediato sobre o interesse da comunidade global.

Vale ressaltar também que, em relação a alguns tipos de conteúdo, as plataformas assumiram a liderança na definição de padrões. O movimento contra a distribuição não consensual de material sexualmente explícito é um exemplo disso (Capítulo 3.1.4).

Num ambiente em que a criação de normas não é de domínio exclusivo dos Estados-nação, estas diferenças entre as normas harmonizadas de empresas e a definição de normas fragmentadas por país podem ter implicações a longo prazo de grande relevância para os desafios jurídicos transfronteiriços na Internet.

2.4.3. Fertilização judicial cruzada — escalabilidade, replicação e imitação

A estrutura física da Internet é, em grande medida, coordenada. Muitos aspectos da camada lógica, como a esfera do nome de domínio, também são coordenados. No entanto, tanto a literatura quanto as contribuições fornecidas pelos atores para este Relatório sugerem que existe uma falta de coordenação internacional e cooperação em matéria de regulação da Internet de forma mais ampla.

Uma clara maioria (68%) dos especialistas consultados "discordaram fortemente" ou "discordaram" que os instrumentos existentes de cooperação jurídica interestatal estão abordando

eficazmente os abusos on-line. Apenas 2% "concordaram" ou "concordaram fortemente", enquanto 30% responderam que "não concordam nem discordam".

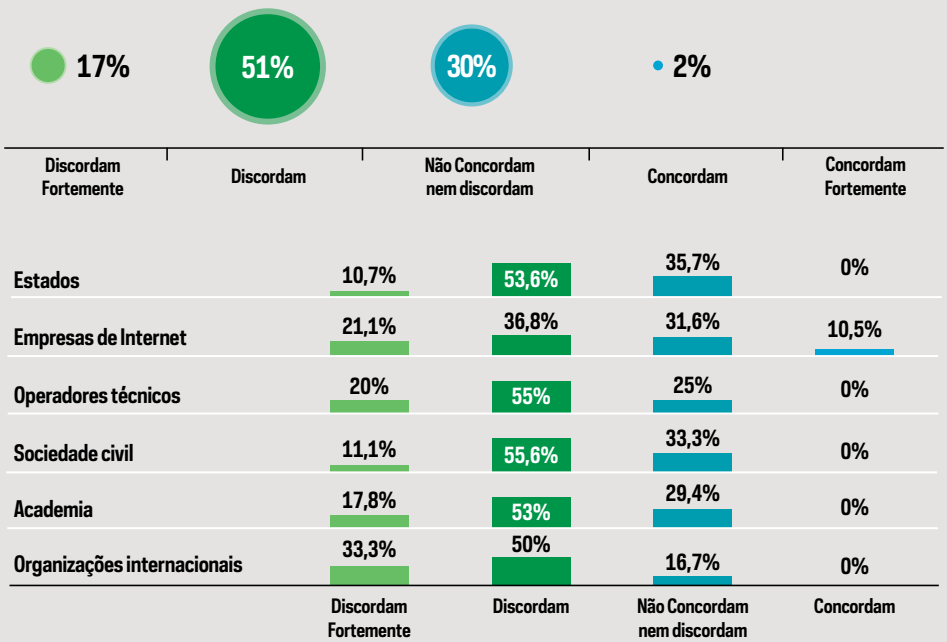
As respostas evidenciaram o consenso entre regiões e grupos de atores, e vários comentários importantes de especialistas pesquisados englobaram as preocupações de todo o ecossistema. Por exemplo, um especialista pesquisado observou que as ferramentas por si só não podem resolver os abusos on-line, e que uma mitigação eficaz requer (1) uma conscientização sobre as ferramentas disponíveis e (2) habilidades para usá-las. Além disso, vários especialistas consultados salientaram que, embora os instrumentos existentes de cooperação jurídica interestatal possam ser suficientes para questões não urgentes, os procedimentos burocráticos lentos se adaptam mal ao ritmo acelerado da Internet.

Em seus comentários sobre os instrumentos de cooperação jurídica interestatal existentes, os especialistas pesquisados também enfatizaram a necessidade de uma abordagem multissetorial (Capítulo 1.10). Por exemplo, um comentário observou que não são apenas os governos que precisam trabalhar em conjunto, mas também as empresas e a sociedade civil. Ao mesmo tempo, vários especialistas pesquisados comentaram que, embora ainda haja um longo caminho a percorrer, são notáveis as melhorias.

A falta de coordenação é uma consequência direta, e talvez natural, do fato de os Estados gozarem de soberania na medida em que têm a capacidade de fazer suas próprias leis. Dado que os Estados adotam abordagens fundamentalmente diferentes em questões como o equilíbrio dos direitos humanos, a proteção dos consumidores e o apoio às empresas, não é surpreendente ver problemas na coordenação da regulação da Internet. Os esforços mais complicados de coordenação são as diferenças fundamentais nas atitudes do Estado em relação aos papéis que a democracia e a religião devem desempenhar em questões jurídicas. A complexidade desta situação só aumentará à medida que mais Estados em desenvolvimento desempenharem papéis mais importantes on-line. Como observado anteriormente, o clima internacional também mudou de forma mais ampla nos últimos anos, à medida que os Estados se afastam dos esforços colaborativos internacionais e objetivos comuns, em direção a políticas mais domésticas que priorizam os interesses imediatos de cada Estado.

INFOGRÁFICO 11

AS FERRAMENTAS DE COOPERAÇÃO JURÍDICA INTERESTATAL EXISTENTES ABORDAM EFICAZMENTE OS ABUSOS ON-LINE?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

Para simplificar, a desconfiança internacional parece estar aumentando. Esta tendência política mais ampla constitui inevitavelmente um obstáculo adicional a uma coordenação eficaz da regulação da Internet.

Ao mesmo tempo, é fato que, devido à natureza transfronteiriça da Internet, os desafios enfrentados on-line só podem ser endereçados por meio de esforços de colaboração internacionais e da prossecução de objetivos comuns; os atores não podem simplesmente se dar ao luxo de não colaborar. Um Estado individual não pode, nem deve controlar a Internet ou o que está disponível on-line. Por enquanto, o diálogo internacional multissetorial continua a ser a única alternativa. No entanto, existem inúmeros

indicadores de que o mundo não está pronto para um acordo internacional geral para resolver todas as questões de regulação da Internet. Um salto tão gigantesco é, infelizmente, irrealista. Em vez disso, o progresso será alcançado através de muitos pequenos passos, pelo menos por enquanto. Os Estados poderiam intensificar os esforços para identificar elementos de união e resolver, ao menos, as mais graves inconsistências e confrontos entre os sistemas jurídicos nacionais, tanto no que se refere ao direito material quanto ao direito processual. Neste contexto, os especialistas entrevistados observaram que, embora a harmonização possa atualmente ser impossível em alguns temas, uma maior harmonização parece possível e valiosa noutros temas (por exemplo, sistemas de notificação de violação de dados).

Sugestões do progresso de "pequenos passos" discutidos acima podem ser vistas no surgimento da jurisprudência global por fertilização judicial cruzada. Simplificando, os tribunais e os reguladores estão cada vez mais atendendo a, copiando e imitando as abordagens feitas por tribunais estrangeiros. Exemplos disso são proeminentes no campo da privacidade de dados, onde o GDPR da UE (Capítulo 3.1.6.1) está sendo amplamente copiado e imitado.

Conforme discutido mais detalhadamente abaixo, a fertilização judicial cruzada não ocorre de maneira uniforme. Em muitos casos, a influência é unidirecional e não mútua – normalmente dos Estados industrializados para os Estados em desenvolvimento.

De forma mais ampla, esta fertilização judicial cruzada funciona como uma "espada de dois gumes". Nos casos em que a abordagem adotada por outro Estado trabalha no sentido de uma maior harmonização internacional, imitar essa abordagem pode obviamente ter um impacto positivo. No entanto, nos casos em que a abordagem adotada por outro Estado é de natureza agressiva, cada adoção dessa abordagem para um novo sistema jurídico nos distancia ainda mais das soluções para as questões transfronteiriças enfrentadas on-line. Além disso, nem todas as abordagens são escaláveis. Os tribunais e legisladores devem sempre ter isso em mente, tanto ao selecionar como eles abordam uma questão legal específica, quanto ao decidir quais, se houver, abordagens de tribunais ou legisladores estrangeiros devem adotar.

Na verdade, é indiscutivelmente razoável esperar que os legisladores nos países que comumente influenciam a evolução da política e da legislação a nível mundial realizem o que pode ser denominado "avaliação de impacto no sul global", considerando: (1) o impacto que as suas abordagens terão no Sul global; e (2) o que acontecerá se o Sul global adotar as suas abordagens.

Além disso, os tribunais e legisladores devem ter presente que o objetivo final do direito internacional é contribuir para a sobrevivência da espécie humana, com subobjetivos óbvios, tais como assegurar a coexistência pacífica, a proteção do ambiente e a defesa dos direitos humanos. A Internet pode desempenhar um papel importante para ajudar na criação de ligações e relações internacio nais através da comunicação e da interação transfronteiriças. Temos, portanto, de evitar utilizar o ambiente on-line como uma nova arena de conflitos internacionais. Estes objetivos devem ser integrados em qualquer avaliação da jurisdição da Internet.

Na verdade, é indiscutivelmente razoável esperar que os legisladores nos países que comumente influenciam a evolução da política e da legislação a nível mundial realizem o que pode ser denominado "avaliação de impacto no sul global", considerando: (1) o impacto que as suas abordagens terão no Sul global; e (2) o que acontecerá se o Sul global adotar as suas abordagens.

2.4.4. As regras são criadas para — e pelos — grandes atores estabelecidos

Uma análise dos resultados da pesquisa e da entrevista aponta para cinco fatores que, em conjunto, fazem com que uma série de atores — países em desenvolvimento, países menores e atores menores da Internet — se sintam descapacitados:

1. Existe uma percepção de que, em comparação com os países desenvolvidos, os países em desenvolvimento têm menos influência nas abordagens adotadas pelos principais atores da Internet;
2. Existe uma percepção de que, em comparação com os principais atores da Internet, os pequenos atores da Internet têm menos influência nas abordagens adotadas pelos reguladores;

3. Existe uma percepção de que tanto os pequenos atores da Internet quanto os países em desenvolvimento não têm voz no diálogo internacional;
4. A extraterritorialidade permite que os Estados dominantes imponham suas leis ao mundo, enquanto os Estados menores não têm a posição e os meios para fazer cumprir suas leis até mesmo nacionalmente; e
5. As abordagens jurídicas dos países desenvolvidos estão sendo replicadas a tal ponto que impacta a soberania e a autodeterminação dos países em desenvolvimento.

Uma preocupação levantada por vários especialistas entrevistados e consultados é que grande parte da discussão sobre como lidar com as questões transfronteiriças da Internet se concentra em torno das maiores empresas de Internet — particularmente empresas baseadas nos EUA, como Google, Microsoft, Facebook, Apple, Amazon, Twitter e eBay. Existem também exemplos não ocidentais desta dinâmica; as normas chinesas, por exemplo, são introduzidas como uma componente *de facto* de projetos subsidiados de infraestruturas de banda larga móvel e terrestre em partes da África. Isso leva a uma perspectiva distorcida das questões enfrentadas pela grande maioria dos atores da Internet, que consiste em pequenas empresas e organizações.

Na verdade, os grandes atores também podem estar em desvantagem em diálogos onde eles têm uma estrutura ou modelo de negócio divergente das estruturas mais padronizadas dos principais atores. Por exemplo, a Wikipédia opera além-fronteiras e está disponível em diferentes versões, como outras grandes plataformas de Internet. No entanto, as várias versões da Wikipédia são baseadas em idiomas e independentes umas das outras — o que é distintamente diferente da abordagem mais padronizada de publicação de diferentes versões de países de uma plataforma. As implicações desta diferença estrutural são profundas. No contexto de ordens de remoção de conteúdo, por exemplo, uma ordem judicial para remover determinado conteúdo afetará inevitavelmente todos os usuários da versão da Wikipédia em questão e a remoção em uma versão linguística não tem impacto sobre o que está disponível em outra versão linguística. Os tribunais e as entidades reguladoras têm de estar atentos às implicações jurídicas deste tipo de diferenças estruturais.

Existem razões óbvias e práticas para direcionar a maior atenção para as principais plataformas de Internet. Onde os governos desejam maximizar o impacto, eles naturalmente visam empresas com o maior número de usuários. E as principais empresas de Internet têm os recursos para participar de discussões sobre questões de regulação da Internet. No entanto, apesar de tais justificativas práticas, a sub-representação dos pequenos atores da Internet continua a ser uma meta-tendência dominante que deve ser abordada. Além disso, a construção de soluções baseadas na regulação das principais empresas tecnológicas pode não ser uma forma eficaz de abordar comportamentos indesejáveis por parte de pequenos atores que operam em condições marcadamente diferentes. Destacando outra meta-tendência, muitos especialistas entrevistados e pesquisados de países em desenvolvimento (e, em certa medida, de países menores) perceberam que só tomam conhecimento e participam em importantes discussões políticas e regulatórias depois que muitas decisões já tenham sido tomadas. Trata-se, em parte, de uma questão de acesso à informação, discutida mais detalhadamente noutras partes do presente Relatório (Capítulo 2.2.4).

Há uma necessidade contínua de trabalhar em soluções para solicitar e incorporar rapidamente as contribuições de todos os atores. A sub-representação dos pequenos atores na Internet e dos países em desenvolvimento na elaboração de soluções exige reconsideração e reestruturação. O aumento da capacitação é uma das respostas mais óbvias. Há também um desequilíbrio de poder no contexto da aplicação extraterritorial da legislação. Alguns Estados têm maior poder para que suas leis sejam cumpridas de forma extraterritorial, mesmo nos casos em que as leis em questão são idênticas ou quase idênticas. Este desequilíbrio de poder — muitas vezes entre países industrializados e países em desenvolvimento — pode tornar-se cada vez mais visível à medida que mais Estados adotam requisitos de "localização de rep", discutidos no capítulo 4.1.3.

A sub-representação dos pequenos atores na Internet e dos países em desenvolvimento na elaboração de soluções exige reconsideração e reestruturação.

2.5. Novas funções para os intermediários

Sem os intermediários da Internet, como motores de busca, plataformas de leilão, plataformas de vídeo e plataformas de mídia social, a Internet seria consideravelmente menos útil e consideravelmente menos fácil de usar. De fato, os intermediários da Internet desempenharam um papel central no funcionamento do ambiente on-line no passado, no presente e continuarão a desempenhá-lo no futuro.

2.5.1. Aumento da responsabilidade conferida aos operadores privados

Os papéis e as responsabilidades exatas dos intermediários da Internet são temas discutíveis e controversos e objeto de um trabalho extenso e detalhado. O Stanford World Intermediary Liability Map, por exemplo, é um recurso on-line que fornece às plataformas da Internet e outras pessoas informações sobre leis de responsabilidade on-line.[74] A crescente responsabilidade conferida aos operadores privados — através de leis que fazem das plataformas de Internet os guardiões do conteúdo, bem como a assunção voluntária de responsabilidade — tem ocorrido em vários campos. Esta tendência é particularmente perceptível em certas áreas e evoluiu especialmente no contexto do terrorismo, extremismo e discurso de ódio — domínios em que algumas leis exigem tempos de resposta rápidos no bloqueio de conteúdo.

Por exemplo, em 19 de dezembro de 2018, o Facebook anunciou que havia banido 425 páginas, 17 grupos, 135 contas no Facebook e 15 contas no Instagram por se envolverem em comportamentos coordenados e não autênticos, relacionados à situação em Myanmar.[75] As contas proibidas estavam compartilhando mensagens Anti-Rohingya — o mesmo tipo de mensagens que alimentaram um genocídio mais amplo em Myanmar.[76]

A possibilidade do Facebook de remover páginas que não cumprem seus termos de serviço foi confirmada pelo Tribunal Distrital dos EUA em um recente caso da Primeira Emenda apresentado por um demandante russo (Agência Federal de Notícias).[77] No tocante ao extremismo e ao discurso de ódio, um dos quadros jurídicos mais reconhecidos é o chamado *Christchurch Call* de maio de 2019.[78]

Outro instrumento digno de nota, especificamente destinado a aumentar a responsabilidade conferida aos operadores privados, é o Código de Conduta de 2016 sobre a luta contra o discurso de ódio ilegal on-line apresentado pela Comissão Europeia, juntamente com Facebook, Microsoft, Twitter e Youtube. Ao abrigo deste Código, as empresas de TI mencionadas comprometem-se a:

- Ter processos claros e eficazes para rever notificações relativas a discursos de ódio ilegais em seus serviços para que possam remover ou desativar o acesso a esse conteúdo.
- Ter Regras ou Diretrizes de Comunidade que esclarecem a proibição da promoção do incitamento à violência e conduta odiosa.
- Após o recebimento de uma notificação de remoção de conteúdo válida, revisar esses pedidos de acordo com as suas regras e diretrizes comunitárias e, se necessário, com as legislações nacionais que transpõem o Regime de Decisão 2008/913/JAI, com equipes dedicadas à análise dos pedidos.
- Revisar a maioria das notificações válidas para a remoção de discurso de ódio ilegal em menos de 24 horas e remover ou desativar o acesso a esse conteúdo, se necessário.

As implicações transfronteiriças são óbvias.

2.5.2. Guardiões (in)voluntários

O papel dos intermediários da Internet e a possível proteção dos intermediários da Internet são frequentemente abordados de pontos de vista extremistas. Alguns procuram impor um regime de liberdade de expressão intransigente, sob o qual os intermediários da Internet não impõem restrições sobre o que os usuários da Internet postam. Outros veem os intermediários da Internet como pouco mais do que ferramentas úteis para o controle governamental de conteúdo e atividades da Internet. Tais pontos de vista extremos são, em última análise, inúteis, e temos de nos esforçar por um equilíbrio adequado.

Historicamente, os países ocidentais consideraram os intermediários da Internet como cruciais para o desenvolvimento da Internet, motivo pelo qual lhes proporcionaram uma ampla proteção — por exemplo, sob a forma do conhecido §230 da Lei de Decência das Comunicações dos EUA de 1996 e através

dos Artigos 12-15 da Diretiva da UE para Comércio Eletrônico.[79] Ambos os instrumentos fornecem aos intermediários da Internet proteção contra responsabilidade em determinadas circunstâncias. Mas essa atitude parece estar mudando.

Ao centrar-se nos desafios jurídicos transfronteiriços na Internet em relação aos intermediários da Internet, ao menos cinco questões-chave devem ser tratadas com urgência:

1. A necessidade de minimizar ou, preferivelmente eliminar, situações em que os intermediários da Internet correm o risco de violar a lei de um Estado ao cumprir a lei de outro Estado;
2. A necessidade de esclarecer em que medida os intermediários da Internet - enquanto atores privados - podem desempenhar funções quase-judiciais (seja voluntária ou involuntariamente);
3. A necessidade de ter um arcabouço jurídico sobre a forma como os intermediários da Internet devem determinar o âmbito geográfico da jurisdição (Capítulo 4.1.7) quando bloqueiam ou eliminam conteúdos;
4. A necessidade de assegurar que a lei forneça as orientações mais claras quanto ao que se espera dos intermediários da Internet; e
5. A necessidade de distinguir claramente as situações em que os intermediários da Internet são vistos como editores e nas quais são vistos como plataformas neutras.

As situações em que uma parte corre o risco de violar a lei de um Estado ao cumprir a lei de outro Estado são referidas como conflitos de leis "verdadeiros". Existe um reconhecimento generalizado de que essas situações não beneficiam ninguém e devem ser evitadas. O problema é encontrar uma forma de evitá-las em um ambiente em que os Estados raramente estão dispostos a comprometer a aplicabilidade das suas leis.

Um modelo potencial pode ser encontrado na Lei de Privacidade da Austrália. A seção 6A limita o efeito extraterritorial da lei, estabelecendo que: "o ato ou prática não viola um Princípio de Privacidade Australiano se: a) o ato ou a prática forem realizados fora da Austrália e dos Territórios externos; e b) o ato ou prática for exigido(a) por uma lei aplicável de um país estrangeiro."[80]

A definição de conflitos de leis centrada em deveres descreve apenas uma parte do problema. Há também os chamados 'falsos' conflitos de leis. Estes ocorrem quando uma pessoa sujeita

a duas ou mais leis pode cumprir todas as leis aplicáveis, o que pode ser o caso se uma lei é mais flexível do que a outra, ou se uma lei dá um direito e a outra impõe uma obrigação contrária.

No contexto dos intermediários da Internet, a importância desses conflitos de leis "falsos" pode ter sido subvalorizada. A relação correlativa entre direitos e deveres, que nos é familiar a partir do direito interno, não existe no ambiente transfronteiriço; os direitos previstos no sistema jurídico de um Estado não podem necessariamente criar obrigações correspondentes ao abrigo de outro sistema jurídico. Para avaliar se duas (ou mais) leis são conflitantes, precisamos ter em conta os deveres e os direitos que essas leis preveem. Em outras palavras, mesmo quando os deveres não se chocam, mas os direitos de um país se conflitam com os deveres de outro Estado, temos de avaliar cuidadosamente qual é a prioridade jurídica. Em um contexto internacional, não há razões legais gerais para que um intermediário da Internet priorize automaticamente os deveres impostos por um Estado sobre os direitos concedidos por outros Estados. No entanto, a nível prático, os intermediários da Internet podem tentar evitar sanções, respeitando as obrigações impostas por um Estado, em vez de exercerem os direitos conferidos pela legislação de outros Estados, a menos que recebam garantias.

Isto leva a um risco de bloqueio excessivo e a um "nivelamento por baixo".[81]

Os intermediários da Internet cumprem funções quase-judiciais em diversos contextos. Às vezes, isso acontece voluntariamente e, às vezes, esse papel lhes é imposto. Exemplos dos primeiros incluem ações como a remoção de material de abuso infantil. Em 24 de outubro de 2018, por exemplo, o Facebook anunciou que havia removido 8,7 milhões de imagens de abuso infantil nos três meses anteriores, usando software previamente não divulgado que ajuda a sinalizar potenciais materiais de abuso infantil para os seus revisores.[82]

> **Os intermediários da Internet cumprem funções quase-judiciais em diversos contextos.**

Uma observação feita por um especialista entrevistado é particularmente pertinente neste contexto. Talvez devido à

estrutura da empresa comumente adotada pelas principais plataformas de Internet dos EUA, e talvez por conveniência, as decisões relacionadas a bloqueio e a remoção de conteúdo são muitas vezes implementadas em uma base regional, e não nacional, em algumas partes do mundo. Por exemplo, se um país no Oriente Médio solicitar que o conteúdo seja bloqueado ou retirado devido a leis de blasfêmia, esse conteúdo é frequentemente bloqueado para ou removido de toda a região, mesmo que o conteúdo em questão possa ser legal em alguns países da região.

Há muitos exemplos de intermediários da Internet sendo forçados a assumir uma função quase-judicial. Por exemplo, em 6 de dezembro de 2018, os provedores de serviços de Internet (ISPs) ugandenses começaram a implementar uma diretiva da Comissão de Comunicações do Uganda (UCC) para bloquear o acesso a sites com conteúdo adulto;[83] exemplos da China, Indonésia, Coreia, Rússia, Turquia, bem como Austrália e UE são mencionados posteriormente no Relatório.

Nessas situações, os intermediários da Internet tornam-se os censores e os guardiões do discurso — um papel para o qual eles normalmente não são adequados. É questionável se a sociedade deve atribuir um papel tão crucial às entidades privadas.

Alguns podem apontar para o fato de que os jornais, as emissoras de rádio e TV têm atuado há muito tempo como censores ao decidir que conteúdo disponibilizar. Mas o papel do intermediário da Internet é tão fundamentalmente diferente que não se pode e não se deve fazer tal comparação. Um argumento comum sustenta que os intermediários da Internet são mais parecidos com o serviço postal, distribuindo passivamente o conteúdo de outras pessoas sem interferência. No entanto, tais analogias só podem servir de distração, em vez de fornecer uma ferramenta útil para discussão. A realidade é que nenhum intermediário na história teve que gerenciar o volume de conteúdo gerado pelo usuário como os intermediários da Internet fazem atualmente.

O papel dos intermediários da Internet deve, portanto, ser abordado com novos olhos, livres de noções preconcebidas baseadas em comparações com os papéis dos intermediários off-line.

As expectativas dos intermediários da Internet servem apenas para complicar a situação. Embora a maioria das pessoas esperem que os intermediários da Internet cumpram a lei de

seus respectivos países, elas provavelmente não querem que eles cumpram *todas* as leis de todos os outros países do mundo.

No final, tal conformidade forçaria os intermediários da Internet a priorizar as leis mais restritivas de todos os países do mundo. Esse "nivelamento por baixo" é certamente uma direção insalubre para a Internet. E se isso não for desejado, há uma necessidade de considerar se um intermediário de Internet globalmente ativo pode ser desculpado por não cumprir todas as leis em todo o mundo que afirmam se aplicar à sua conduta. Se os atores respondem afirmativamente a essa pergunta, como um intermediário de Internet globalmente ativo deve decidir quais leis deve obedecer? Estas são, em certa medida, questões novas no direito internacional.

Sem uma orientação clara da lei, os intermediários da Internet podem ser encarregados de decidir a legalidade de determinado conteúdo.[84] Em tal situação, pode-se argumentar que os intermediários da Internet são criados para falhar devido à imprecisão das leis que devem aplicar. Note-se também, neste contexto, que os intermediários da Internet têm a tarefa de desempenhar essas funções quase-judiciais a um ritmo acelerado. Embora o poder judiciário possa levar meses ou mesmo anos para chegar a uma decisão sobre um determinado assunto, os intermediários da Internet podem ser obrigados a decidir o mesmo assunto em minutos, dado o volume de decisões que precisam tomar.

Uma vez que pode ser difícil identificar e levar à justiça a parte responsável por determinadas atividades on-line, litigantes e reguladores podem, em vez disso, ser tentados a visar o intermediário da Internet utilizado para tais atividades. O juiz Fenlon abordou esta questão muito claramente no caso canadense Equustek acima mencionado, afirmando: "O Google é um espectador inocente, mas, involuntariamente, facilita as violações contínuas dos réus às ordens deste Tribunal. Não há outra forma prática de interromper as vendas dos sites dos réus."[85] A mensagem do juiz Fenlon é clara: onde o sistema jurídico falha, os intermediários da Internet podem se tornar os bodes expiatórios da vez.

Há também uma questão de longa data que trata de distinguir entre intermediários da Internet como editores e intermediários da Internet como plataformas neutras. Obviamente, as proteções para plataformas neutras podem não se estender a situa-

ções em que os intermediários da Internet atuam como editores. Esta neutralidade crucial é minada quando as plataformas são necessárias para promover narrativas específicas, como foi o caso no Código de Conduta da União Europeia de 2016 sobre o combate ao discurso de ódio ilegal on-line (Capítulo 3.1.1). Neste contexto, verificou-se que: "Embora a promoção de contra-narrativas possa ser atraente diante do conteúdo 'extremista' ou 'terrorista', a pressão por tais abordagens corre o risco de transformar plataformas em portadores de propaganda muito além das áreas estabelecidas de preocupação legítima."[86] Um especialista entrevistado considerou que através de fusões, aquisições e do crescimento, muitos intermediários estão mudando de funções na medida em que dentro da mesma empresa, pode haver um anunciante, titular da marca, registrador e editor, e que isso cria uma tensão interessante. Outro especialista entrevistado comentou que os intermediários se deparam com muitas jurisdições diferentes e regras conexas que representam um desafio significativo — não apenas pela sua conformidade com essas regras, mas também pela comunicação como eles as aplicam.

Ainda, outro especialista entrevistado observou que esse aspecto leva à aquisição de poder significativo por essas empresas para implementar soluções. Ou seja, se essas empresas implementam soluções localizadas em determinadas questões, isso pode levar a uma Internet mais fragmentada com regras diferentes que se aplicam em diferentes lugares. Este especialista estava preocupado com a falta de capacidade dos atores menores, incluindo empresas e países pequenos, de influenciar os intermediários de maior dimensão na implementação das políticas. Na verdade, como salientou um especialista entrevistado, esta questão também se estende às potências de nível médio que adotam políticas, as quais grandes plataformas ignoram em grande parte, a menos que se encaixem com as abordagens atuais dos países maiores. Há também casos em que plataformas de mídia social são usadas pelos governos para forçar seus valores em pessoas em outros Estados. Por exemplo, o aplicativo de mídia social de propriedade chinesa TikTok agora proíbe o conteúdo ProLGBT mesmo em países onde a homossexualidade nunca foi ilegal.[87] Tais ações têm consequências de longo alcance. No mínimo, isso provavelmente prejudica a popularidade das mídias sociais afetadas.

Deve-se fazer uma observação final. Em tudo isso, devemos perceber que, à medida que os governos desviam as responsabilidades e a tomada de decisões para as plataformas on-line, tornando-as os guardiões da Internet, os governos também estão transferindo poder para essas plataformas. Isto pode comprometer a *accountability*, a transparência e, em última análise, a justiça.

2.5.3. Apelações e recursos passaram a ser questões-chave

Quando um tribunal ou uma autoridade decide uma questão, normalmente é possível recorrer da decisão e obter um posicionamento sobre o raciocínio que levou à decisão. Atualmente, falta um mecanismo de recurso transparente em situações em que um ator privado atua como tomador de decisão. Esta é uma consideração séria num contexto em que os operadores privados têm aumentada a responsabilidade de agir como filtros de discurso.

Dito isto, deve-se, naturalmente, reconhecer que qualquer decisão tomada por um intermediário da Internet pode ser contestada perante os tribunais. Isto pode proporcionar algum conforto. No entanto, esse processo geralmente não é uma resposta eficiente às injustiças percebidas e muitas vezes pode envolver questões jurisdicionais complexas.

Como observou um especialista entrevistado, a falta de mecanismos de resolução de reclamações e a necessidade de transparência entre as plataformas estão sendo discutidas como parte da Coalizão Dinâmica do Fórum de Governança da Internet da ONU sobre Responsabilidade de Plataformas.[88] Este especialista observou que o Relator Especial da ONU sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão (Special Rapporteur on FOE) também recomendou, em um Relatório Temático de 2018 ao Conselho de Direitos Humanos das Nações Unidas, que as empresas melhorem sua transparência e *accountability* na regulamentação de conteúdo.[89]

Note-se que muitas das maiores empresas de Internet emitem relatórios de transparência. Mas, como observado por um especialista entrevistado, enquanto esses relatórios incluem números agregados de desmantelamentos de conteúdo, eles atualmente não fornecem detalhes sobre como as decisões estão sendo tomadas.[90] Sobre o tema da transparência, um

especialista entrevistado disse que as empresas ainda não encontraram uma forma bem sucedida de comunicar os detalhes dos seus procedimentos internos e a forma como aplicam regras diferentes. Este fracasso provocou uma reação normativa por parte dos governos, particularmente no contexto do discurso de ódio e notícias falsas.

A questão da prestação de contas também está recebendo mais atenção. O Institute for Accountability in the Digital Age (I4ADA), por exemplo, foi fundado com a missão de garantir que as violações de normas e valores on-line não comprometam o potencial da Internet para aumentar o acesso ao conhecimento, difundir a tolerância e compreensão globais e promover a prosperidade sustentável.[91] Para tanto, o I4ADA está trabalhando em um conjunto de princípios — os *Princípios Globais de Haia para a Accountability na Era Digital*[92] — com implicações significativas para os desafios jurídicos transfronteiriços na Internet.

03.
Tendências atuais

- Expressão
- Segurança
- Economia

As preocupações relativas às tensões jurisdicionais no ciberespaço são generalizadas, uma vez que a natureza transfronteiriça da Internet entra em conflito com a colcha de retalhos das leis nacionais vinculadas territorialmente. O elevado grau de insegurança jurídica aumenta o custo de fazer negócios e cria desafios para os governos que procuram proteger seus cidadãos e garantir o respeito pelas suas leis. Pode igualmente impedir que os usuários da Internet acessem um vasto leque de conteúdo, como de outra forma poderiam, e suscita preocupações da sociedade civil quanto ao fato de os abusos não serem devidamente tratados ou de que as tentativas de soluções possam prejudicar os usuários. É urgente tratar destas questões.

Para compreender os detalhes e toda a complexidade dos desafios jurídicos transfronteiriços na Internet, é útil mapear as principais tendências dentro dos tópicos mais relevantes para os grupos de atores interessados da Rede de Políticas Internet & Jurisdição.

Para tal efeito, o presente Capítulo visa a destacar uma seleção de "tendências" particularmente significativas dentro de temas que vão desde a privacidade dos dados à tributação, e da Internet das Coisas a crimes cibernéticos. Estes temas diversos foram agrupados em três categorias mais amplas:

1. Expressão
2. Segurança
3. Economia

Embora esta abordagem possa dar mais clareza à apresentação, alguns tópicos podem ser incluídos em mais de uma categoria. Existem também pontos de ligação óbvios e, de fato, sobrepõem-se a estas categorias. Por exemplo, a interdependência econômica entre os Estados continua sendo uma verificação do comportamento agressivo,[93] que enfatiza a ligação entre segurança e economia.

Em cada um dos tópicos discutidos, é dada uma atenção mais detalhada a tendências particularmente importantes, identificadas através dos resultados da pesquisa, entrevistas e extensa pesquisa documental, incluindo uma análise da abrangente coleção de tendências e desenvolvimentos relevantes da Rede de Políticas Internet & Jurisdição disponível na I&J Retrospect Database.[94]

Estas fontes permitiram também delinear brevemente outras tendências significativas dentro de cada área temática.

O objetivo é ser abrangente sem ser necessariamente exaustivo.

Embora seja, portanto, óbvio que outras tendências poderiam ter sido incluídas,[95] o objetivo do trabalho foi garantir uma alta probabilidade de as partes interessadas da Rede de Políticas Internet & Jurisdição concordarem que todas as tendências incluídas são importantes.

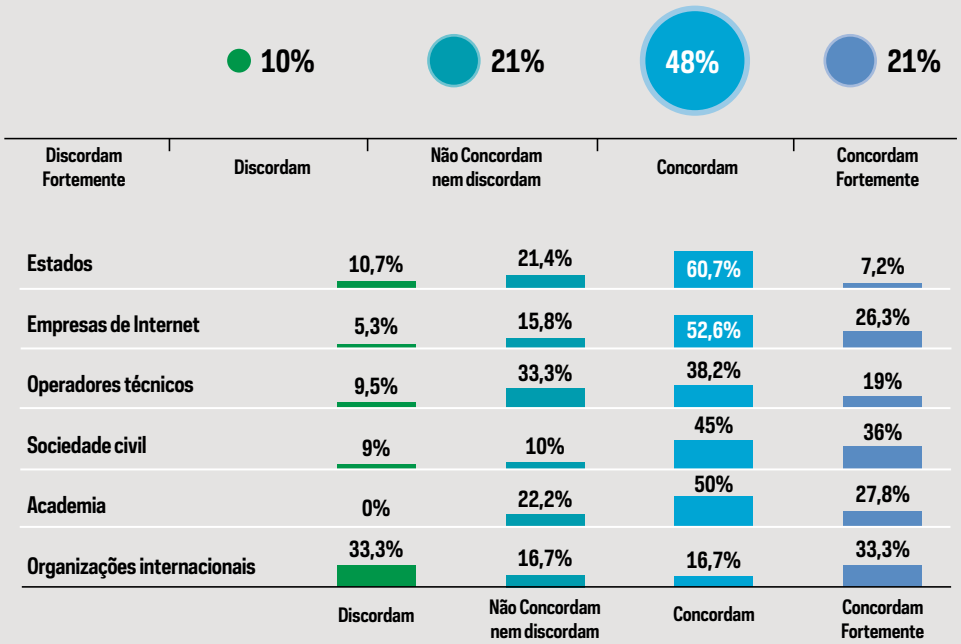
3.1. Expressão

A primeira categoria de grandes tendências atuais diz respeito à expressão. Discussões recentes em torno da interseção entre Internet, jurisdição e expressão têm focado em preocupações sobre discurso de ódio, extremismo e notícias falsas, bem como a reforma generalizada dos regimes de privacidade de dados em todo o mundo. Cada vez mais, reivindicações amplas permeiam essas discussões e há um apetite crescente entre os reguladores para reexaminar os papéis e as responsabilidades dos intermediários da Internet.

Incentivar e facilitar a expressão transfronteiriça tem sido uma força motriz por trás de grande parte do desenvolvimento da Internet, tanto nas dimensões física (por exemplo, hardware) como não física (por exemplo, plataformas de conteúdo). Como muitos avanços críticos iniciais se originaram nos EUA, a perspectiva americana sobre a liberdade de expressão — mais proeminentemente articulada na Primeira Emenda à Constituição dos EUA — tem colorido grande parte do discurso inicial e os princípios orientadores.[96] Embora atualmente mais fraca devido à forte proliferação da utilização da Internet fora dos EUA — onde, por exemplo, mais de 80% dos usuários do Facebook atualmente residem — o incentivo e a facilitação da liberdade de expressão, incluindo a expressão transfronteiriça, continua a ser uma pedra angular da Internet valorizada em grande parte do mundo. Em reconhecimento disso, a ONU salientou que o direito à liberdade de expressão na Internet é uma questão de crescente importância.[97]

INFOGRÁFICO 12

OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET CONSTITUEM UM OBSTÁCULO SIGNIFICATIVO PARA AS PEQUENAS E MÉDIAS EMPRESAS (PME)?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

A IMPORTÂNCIA DE EXPRESSÃO TRANSFRONTEIRIÇA

Quando questionados quais as eventuais consequências negativas que preveem se os desafios jurídicos transfronteiriços na Internet não forem devidamente enfrentados, 59% dos especialistas consultados levantaram a questão das eventuais restrições à expressão. Esta foi uma das preocupações mais fortes entre os atores.

A liberdade de expressão é um direito humano fundamental — tanto off-line quanto on-line[98] — e está protegido por vários instrumentos internacionais de direitos humanos, bem como pelo direito interno de muitos Estados. No entanto, a liberdade

de expressão é um dos vários direitos humanos fundamentais e deve ser encarada como parte de um sistema de direitos que, por vezes, têm de ser reconciliados ou equilibrados. Isto é destacado em obras como o Guia dos Direitos Humanos do Conselho da Europa para os Usuários da Internet, adotado em abril de 2014.[99] O Guia descreve o quadro básico de princípios para proteger os direitos humanos fundamentais garantidos pela Convenção Europeia dos Direitos do Homem para todos os usuários da Internet.

Entre os muitos Estados que valorizam a liberdade de expressão, há uma grande diversidade quanto à quando eles veem que é apropriado ter outros direitos concorrentes, contrabalançando os direitos da liberdade de expressão.[100] O caso Yahoo! França, que remonta ao ano 2000,[101] é a disputa de jurisdição mais ilustrativa — e fundamental — na Internet até os dias de hoje.

Enquanto o caso Yahoo! envolveu uma disputa transatlântica, a diferença de atitudes em relação à liberdade de expressão varia ainda mais no nível global. Deve-se enfatizar que os desafios da defesa à liberdade de expressão on-line variam tanto em grau quanto em natureza, entre países e regiões. Como apontaram alguns especialistas pesquisados e entrevistados, isso varia, em parte, de acordo com diferentes distinções entre poder religioso e político. A Autoridade de Telecomunicações do Paquistão (PTA), por exemplo, anunciou em outubro de 2017 que iria formar um comitê de alto nível para monitorar e bloquear conteúdo blasfemo on-line.[102] O conteúdo que preocupa a PTA é perfeitamente legal na maior parte do mundo, e pode, de fato, ser discurso protegido em muitos Estados. A questão, então, é em que medida leis como as leis religiosas do Paquistão podem e devem influenciar a disponibilidade de tais conteúdos on-line.

Surgem questões semelhantes de restrição de discurso de um Estado que influenciam a disponibilidade de conteúdo noutros Estados, por exemplo, em torno do "direito ao desreferenciamento" da UE (Capítulo 3.1.6.2), da lei dos direitos de autor dos EUA (Capítulo 3.3.1.2) ou das restrições chinesas às imagens do Ursinho Pooh.[103]

> **Perceber quão diferente é a situação da liberdade de expressão em todo o mundo é um primeiro passo necessário para proteger a expressão transfronteiriça da Internet.**

A abordagem destas questões é uma necessidade e deve ser uma prioridade política mundial. Um relatório de 2018 da Freedom House observa que os direitos políticos e as liberdades civis em todo o mundo se deterioraram ao seu ponto mais baixo em mais de uma década em 2017, e que apenas 39% da população mundial vivem em países que o estudo classifica como 'livre'.[104] Como o falecido jornalista Jamal Khashoggi observou em sua última coluna:

> *Aos governos árabes têm sido dadas rédeas livres para continuar silenciando a mídia em um ritmo crescente. Houve um tempo em que os jornalistas acreditavam que a Internet libertaria as informações da censura e do controle associado à mídia impressa. Mas esses governos, cuja própria existência depende do controle da informação, bloquearam agressivamente a Internet. Esses governos também prendem repórteres e pressionam anunciantes a prejudicar a receita de determinadas publicações.*[105]

O mesmo pode ser dito em relação a outras regiões e, tal como salientado por um especialista consultado, não há dúvida de que leis, políticas e várias medidas de cooperação podem dar poder ou prejudicar o jornalismo transfronteiriço.

Perceber quão diferente é a situação da liberdade de expressão em todo o mundo é um primeiro passo necessário para proteger a expressão transfronteiriça da Internet. Deve-se notar que, mesmo dentro de blocos legais comparativamente homogêneos, tal como a UE, existem diferenças consideráveis no que se refere à liberdade de expressão.[106] Pode haver também divergências de opinião dentro de um Estado, como evidenciado pelos recentes desafios federais à lei de neutralidade da rede da Califórnia.[107]

Esta diversidade entre os Estados tem implicações abrangentes. Em seu nível mais básico, isso significa que qualquer matéria relacionada ao discurso em que o tribunal de um Estado reivindica jurisdição para julgar no lugar de outro representa a priorização da abordagem desse Estado sobre os valores do outro Estado. Mesmo quando isso se justifica por referência à eficiência processual, continua a prejudicar a equidade e o devido processo, podendo, de fato, ter implicações negativas nas relações internacionais.

As respostas da entrevista e da pesquisa destacaram preocupações sobre o risco de um "nivelamento por baixo". Existe uma possibilidade real de os países com as opiniões mais restritivas imporem essas opiniões ao resto do mundo, conduzindo a um conjunto global de restrições incompatíveis com a liberdade de expressão de outros países.

Ao mesmo tempo, em parte devido ao aumento da inteligência artificial, a Internet corre o risco de ser inundada por conteúdos on-line indesejáveis, como discurso de ódio, bullying e *deep fakes*, na medida em que o seu valor como meio de comunicação é prejudicado. Tal "junkificação da Internet" seria altamente destrutiva e deve ser evitada.

Ao discutir a liberdade de expressão, deve-se notar também que as restrições que são geralmente apropriadas podem ser inadequadas para determinados atores. As bibliotecas, por exemplo, podem ser encarregadas de arquivar e preservar materiais — para fins de pesquisa e educação, bem como para garantir registros históricos precisos — que geralmente não podem ser comunicados. Neste contexto, um especialista observou que um tema comum é o fato de que, embora a Internet tenha permitido muitas das atividades que as próprias bibliotecas têm procurado promover há muito tempo, a regulação da Internet e práticas corporativas podem restringi-las. A dimensão jurisdicional é óbvia. Por meio da retenção de materiais que são acessados através das fronteiras e facilitando aos usuários o acesso a materiais mantidos em outros lugares, as bibliotecas estão expostas a complexas questões jurídicas transfronteiriças com as quais não é fácil lidar. Um desafio fundamental consiste em garantir que, em qualquer tomada de decisão sobre se e como controlar os fluxos de informação, os impactos sobre os usuários em todo o mundo sejam levados em conta.

3.1.1. Extremismo, terrorismo e discurso de ódio

A regulação do extremismo e do discurso de ódio é particularmente complexa em situações transfronteiriças. Em primeiro lugar, não há acordo mundial sobre o que é discurso de ódio ou extremismo. Além disso, como diz o ditado, aquele que luta pela liberdade para um é o terrorista para outro. Por conseguinte, não pode haver acordo geral sobre o que é promoção do terrorismo. Complicações práticas de jurisdição e execução também

surgem quando o conteúdo é criado e adicionado em um Estado, hospedado em um segundo Estado e acessado em um terceiro, como muitas vezes é o caso desses tipos de conteúdo.

O caso Yahoo! França[108] acima mencionado é ilustrativo neste contexto. Envolveu uma empresa americana, *Yahoo!*, operando um site que, entre outros, continha um serviço de leilão onde material nazista estava em oferta. A disponibilização desse material para venda era legal nos EUA, mas contrariava o código penal francês. Na sequência de uma reclamação de duas organizações francesas, um tribunal francês decidiu contra o *Yahoo!* e emitiu uma medida cautelar de direito civil com base no Código de Processo Civil francês. No entanto, um tribunal dos EUA posteriormente concedeu ao *Yahoo!* um julgamento sumário, determinando que os tribunais dos EUA não executassem a decisão francesa.[109] Embora se trate de uma questão de longa data, a divergência fundamental de atitudes aparente no caso envolvendo o *Yahoo!* francês retardou o progresso na regulação do extremismo transfronteiriço e discurso de ódio.

Há sugestões de que a promoção do extremismo, do terrorismo e do discurso de ódio está em ascensão on-line e a Internet provou ser um terreno fértil para a distribuição desse conteúdo. Alguns especialistas entrevistados e pesquisados indicaram que "atividades de ódio" estão aumentando em geral e o que acontece off-line normalmente é espelhado on-line.

Outros especialistas pesquisados e entrevistados sugeriram que questões como discurso de ódio e notícias falsas podem não estar necessariamente aumentando, e que há apenas mais discussão sobre elas. Isto, juntamente com o aumento da transparência, pode resultar na superestimação do aumento, ou mesmo no aumento da "ansiedade e histeria" em torno dessas questões.

Um especialista entrevistado também observou que há uma divisão entre o que os políticos dizem sobre o discurso de ódio, por um lado, e iniciativas legislativas reais, por outro. Este é um ponto importante, uma vez que os apelos políticos a leis mais rigorosas em resposta a acontecimentos trágicos, como os atos terroristas, geralmente negligenciam o fato de que são os mesmos políticos que são encarregados de promulgar tais leis, aqueles que não o fizeram.

No entanto, alguns Estados adotaram iniciativas para combater a distribuição de extremismo e discurso de ódio, com várias leis específicas sobre o assunto. A Lei de Execução sobre Redes

Sociais da Alemanha de 2017 (ou *Netzwerkdurchsetzungsgesetz*, NetZDG) ganhou uma atenção considerável e exige que as redes sociais eliminem o discurso de ódio ou o conteúdo criminoso e informem o número de reclamações de conteúdo ilegal recebidas. Posteriormente, o Facebook foi multado pela Alemanha por subnotificar suas reclamações de conteúdo ilegal.[110] Uma lei semelhante foi aprovada pela França em julho de 2019, exigindo que as plataformas removessem conteúdo "obviamente de ódio" dentro de 24 horas.[111]

E em 13 de julho de 2018, o ministro da Comunicação da Zâmbia anunciou que o governo iria introduzir leis para regular o uso das mídias sociais, a fim de lutar contra o discurso de ódio, roubo de identidade e conteúdo pornográfico.[112] O ministro declarou que as leis entrariam em vigor em 2019.[113] Estes são apenas três exemplos de uma tendência mais ampla que se desenrola tanto nos países em desenvolvimento quanto nos países desenvolvidos. Em 2019, a Austrália alterou o Código Penal especificamente visando o compartilhamento de material violento hediondo.[114] Um desafio particular na elaboração de tais leis é garantir a inclusão de exceções adequadas, por exemplo, para fins de pesquisa.[115]

Há também iniciativas dirigidas especificamente a conteúdos relacionados com terrorismo. Por exemplo, em 6 de fevereiro de 2017, o ministro israelense da Justiça afirmou que os esforços do governo para combater a propagação do conteúdo terrorista finalmente deram frutos; plataformas de Internet tinham cumprido parcial ou integralmente 1.400 pedidos de remoção de conteúdo desde 2016.[116] O ministro também propôs a introdução de legislação que aplique multas pesadas às plataformas que deixem de remover conteúdo que incite à violência.[117] Em fevereiro de 2019, o Reino Unido aprovou a Lei de Combate ao Terrorismo e Segurança das Fronteiras de 2019[118] que (entre outros regulamentos) criminaliza a visualização ou o acesso a conteúdos on-line suscetíveis de serem úteis na preparação de um ato terrorista. No entanto, existem exceções para atividades jornalísticas e acadêmicas, e para pessoas que não têm conhecimento, ou razões para acreditar, que os materiais contenham tal conteúdo. Além disso, um especialista consultado chamou a atenção para a forma como, em junho de 2019, o Representante da OSCE para a Liberdade dos Meios de

Comunicação Social emitiu uma revisão do projeto de Lei da Albânia sobre os Meios de Comunicação Audiovisual e a Lei das Comunicações Eletrônicas, abordando (entre outros) as medidas propostas relativas a conteúdos on-line que possam inspirar atos terroristas e os potenciais impactos na liberdade de expressão e preocupações conexas. O Gabinete do Representante fazia parte de uma consulta mais ampla entre o Gabinete do Representante e o Governo albanês. O Representante realiza outros trabalhos nesta área, por exemplo, organizando o Diálogo Judiciário da Ásia Central de 2019 sobre a proteção da liberdade de expressão no combate ao extremismo violento, incluindo conteúdos extremistas on-line.

Além disso, em setembro de 2018, a UE propôs novas regras para combater os conteúdos terroristas on-line. Esta proposta é digna de nota, na medida em que impõe prazos rigorosos para a eliminação de conteúdos terroristas.[119] A proposta inclui também um quadro para reforçar a cooperação entre os prestadores de serviços de hospedagem, os Estados-membros e a Europol. Nesse contexto, os prestadores de serviços devem designar pontos de contato disponíveis a qualquer momento para dar seguimento às ordens de remoção e encaminhamentos.[120] Em 6 de dezembro de 2018, o Conselho da UE adotou a sua posição sobre a proposta da Comissão Europeia de regulamento contra conteúdos terroristas on-line.[121] A posição apoia a exigência para que os provedores de serviços em nuvem e provedores de plataformas de Internet eliminem conteúdos terroristas no prazo de uma hora, mediante o recebimento de ordens das autoridades responsáveis pela execução da lei. Além disso, afirma que as plataformas devem aplicar determinadas obrigações cautelares para impedir a disseminação de conteúdos terroristas nos seus serviços e tomar medidas proativas para fazer face ao reaparecimento de conteúdo anteriormente removido.[122]

Em 11 de dezembro de 2018, três Relatores Especiais das Nações Unidas publicaram um Relatório Conjunto[123] sobre a proposta, levantando uma série de preocupações sobre os direitos humanos sobre a definição de "conteúdo terrorista", bem como o artigo 4 (sobre ordens de afastamento), o artigo 5 (sobre encaminhamentos para contribuições voluntárias) e o artigo 6 (sobre medidas proativas).[124]

O Parlamento Europeu aprovou a proposta em abril de 2019.[125]

Vários instrumentos internacionais de direitos humanos regulamentam o conteúdo extremista, o discurso de ódio e a promoção do terrorismo. O Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), por exemplo, deixa claro que: "Qualquer defesa de ódio nacional, racial ou religioso que constitua incitação à discriminação, hostilidade ou violência será proibida por lei."[126]

A Convenção Internacional sobre a Eliminação de todas as Formas de Discriminação Racial também aborda especificamente o discurso de ódio.[127]

Além do que foi discutido acima e do fluxo constante de trabalhos acadêmicos,[128] também há numerosas iniciativas não legislativas que devem ser notadas, incluindo:

Em **23 de setembro de 2019**, um grupo de especialistas independentes da **ONU** publicou uma carta aberta convidando os Estados e empresas de mídia social a tomarem medidas para conter a propagação do discurso de ódio.[129]

Em **18 de setembro de 2019**, o Comitê de Comércio, Ciência e Transportes do Senado dos **EUA** realizou uma audiência intitulada "Violência em Massa, Extremismo e Responsabilidade Digital".[130] Na audiência, representantes do Facebook, Google e Twitter foram questionados sobre como abordam esse conteúdo.

Em **agosto de 2019**, noticiou-se que a **OCDE** apoiaria os esforços da Austrália e da Nova Zelândia no sentido de combater a fala extremista on-line com medidas propostas para incluir a exigência de que plataformas apresentem relatórios sobre a eliminação do conteúdo extremista.[131]

Como reação ao ataque terrorista ocorrido em Christchurch, em março de 2019, a primeira-ministra **neozelandesa**, Jacinda Ardern, e o presidente **francês**, Emmanuel Macron convocaram Chefes de Estado e de Governo e líderes do setor tecnológico para adotar o Apelo de Christchurch em **15 de maio de 2019**.[132] Outras iniciativas decorrentes da publicação de vídeos dos tiroteios em Christchurch incluem empresas de telecomunicações **australianas** que bloquearam proativamente o acesso a sites que hospedaram vídeos do ato de terrorismo nos dias seguintes ao ataque[133] e plataforma de jogos de propriedade da Amazon.com, Twitch, que processou usuários por postar o conteúdo on-line.[134]

A reunião do **G20** em Osaka, em **2019**, produziu uma declaração dos líderes sobre a prevenção da exploração da Internet para o terrorismo e o extremismo violento em prol do terrorismo.[135]

O **Dangerous Speech Project** publicou um guia prático detalhado que define o Discurso Perigoso, explicando como determinar quais mensagens são perigosas e ilustrando por que o conceito é útil para prevenir a violência.[136]

Em **outubro de 2018**, o Departamento de Justiça dos **EUA** lançou um novo site de crimes de ódio.[137]

Em **setembro de 2018**, o **Twitter** lançou uma consulta buscando informações sobre sua proposta de alteração às Regras do Twitter (as Regras) para abordar a desumanização.[138]

O trabalho do **Fórum Global de Contraterrorismo** inclui o ambiente on-line e produziu ferramentas como o Kit de Ferramentas de Políticas sobre as Recomendações de Zurique-Londres para a Prevenção e Combate ao Extremismo Violento e ao Terrorismo on-line de **Setembro de 2018**.[139]

Em **junho de 2018,** o **Tribunal Europeu dos Direitos Humanos** emitiu uma nota informativa não vinculativa sobre discurso de ódio.[140]

Em **3 de janeiro de 2018**, foi noticiado que o Ministério da Tecnologia da Informação e Comunicações da **Indonésia** estava lançando um sistema automatizado de moderação da Internet para detectar e restringir o acesso a conteúdos extremistas e adultos, conforme anunciado em novembro 2017.[141] O lançamento do sistema coincide com a criação da Agência Nacional para Cibernética e Criptografia da Indonésia (BSSN), encarregada de combater o conteúdo extremista e a desinformação on-line.[142]

Existem outras declarações bilaterais e multilaterais de compromissos para enfrentar a utilização criminosa e extremista da Internet, incluindo o Plano de Ação **Britânico-Francês** para a Segurança na Internet (**2017**),[143] Declaração Ministerial de **Cinco Países** sobre Combate ao Uso Ilícito de Espaços on-line (**2018**)[144] e a Declaração de Compromisso do Ministro da Segurança do G7 (**2018**), que se refere à prevenção do extremismo violento e uso terrorista da Internet.[145] Em abril de **2019**, o **G7** divulgou um Documento de Resultados sobre Combate ao Uso da Internet para fins Violentos e Extremismos e apelou para que as empresas da Internet tomem medidas mais proativas contra a postagem de conteúdo terrorista e violento.[146]

Em **2017**, o Facebook, Microsoft, Twitter e YouTube criaram o **Fórum Global da Internet para o Combate ao Terrorismo** para formalizar e estruturar a maneira como essas empresas trabalharão juntas para reduzir a propagação do terrorismo e do extremismo violento. Um dos principais recursos é o banco de dados hash compartilhado do setor através do qual as empresas podem criar "impressões digitais" para conteúdo terrorista e compartilhá-lo com as empresas participantes. A rede de compartilhamento se expandiu, com várias outras empresas se juntando à iniciativa.[147]

A Declaração de **junho de 2017** dos chefes dos Estados-membros da **Organização de Cooperação de Xangai** sobre a luta conjunta contra o terrorismo internacional enfatizou "a necessidade de medidas coletivas para contrariar a disseminação da ideologia do terrorismo e do extremismo, incluindo a prevenção e a redução da propaganda terrorista e extremista, a incitação ao terrorismo e extremismo, bem como recrutamento, incluindo o recrutamento através da Internet."[148] Esta declaração deve ser lida no contexto da Convenção de Xangai sobre Combate ao Terrorismo, Separatismo e Extremismo.[149]

Em **2016**, o Facebook, a Microsoft, o Twitter e o YouTube concordaram com um Código de Conduta para combater o discurso ilegal de ódio on-line apresentado pela **Comissão Europeia**. Outras partes aderiram ao acordo em 2019.[150]

A **UNESCO** publicou um relatório intitulado Contra o Discurso de Ódio On-line em **2015**.[151]

Em **2015**, o grupo de apoio à liberdade de expressão **ARTICLE19** publicou um 'kit de ferramentas' que fornece orientações para ajudar a explicar e combater eficazmente o discurso de ódio, ao mesmo tempo em que protege os direitos à liberdade de expressão e à igualdade.[152] O ARTICLE19 também publicou um relatório particularmente relevante em **2018**.[153]

Em **2015**, a **Jordânia** lançou as reuniões de Aqaba, que constituem uma série de reuniões internacionais para reforçar a segurança e a cooperação militar, a coordenação e o intercâmbio de conhecimentos entre parceiros regionais e internacionais para combater o terrorismo dentro de uma abordagem holística.[154]

Em **2013**, a Comissão **Australiana** de Direitos Humanos publicou seu documento de referência: Direitos humanos no ciberespaço.[155] E em **30 de junho de 2019**, a Força-Tarefa australiana para o combate ao terrorismo e material violento extremo publicou um Relatório on-line.[156]

Na sequência de uma série de workshops de especialistas organizados pelo Gabinete do Alto Comissariado para os Direitos Humanos (**OHCHR**), o Plano de Ação de Rabat sobre a proibição da defesa do ódio nacionalista, racial ou religioso que constitua incitação à discriminação, hostilidade ou violência foi adotado em **2012**.[157]

O **Conselho da Europa** emitiu uma Recomendação de Política Geral sobre a luta contra a difusão de material racista, xenófobo e antissemita através da Internet em 2000,[158] e, em 2003, um protocolo adicional à Convenção sobre Crimes Cibernéticos que aborda a manifestação on-line do racismo e da xenofobia.[159]

Uma iniciativa da Diretoria Executiva do Comitê Contra o Terrorismo da **ONU**, "Tecnologia Contra o Terrorismo", visa a apoiar o setor tecnológico, incluindo empresas de tecnologia de menor dimensão, no combate à exploração terrorista da Internet. A iniciativa lançou uma 'Plataforma de Compartilhamento de Conhecimento' para ajudar empresas de menor porte de tecnologia a promover o compartilhamento de boas práticas que fortalecem as respostas nesta área.[160] Note-se também o Plano de Ação da ONU, de **2016** para Prevenir o Extremismo Violento.[161]

A organização sem fins lucrativos Southern Poverty Law Center monitora e emite relatórios sobre grupos e sites que incitam ao ódio nos **EUA**.[162]

Existem também várias resoluções do Conselho de Segurança da **ONU** que procuram abordar a utilização da Internet para fins terroristas.[163]

3.1.2. Difamação

Os litígios transfronteiriços de difamação da Internet têm uma história relativamente longa de destaque nas discussões jurídicas, datando do conhecido caso *Dow Jones contra Gutnick* em 2002 — uma disputa entre um empresário australiano e uma editora sediada nos EUA.[164] O custo do litígio mantém baixo o número de disputas transfronteiriças por difamação na Internet[165] e o tema agora recebe menos atenção na literatura acadêmica e nas discussões políticas.

De fato, as questões da difamação foram levantadas com pouca frequência nas entrevistas e nos resultados das pesquisas. No entanto, como observado por um especialista entrevistado, evidências ocasionais sugerem que as pessoas estão mais inclinadas a criticar outras pessoas, empresas e pontos de vista on-line e podem recorrer a mentiras e exageros em seus ataques à reputação. E, como em muitos outros campos jurídicos, os litigantes frequentemente buscam intermediários na Internet em casos de difamação, aumentando a complexidade jurisdicional. Por exemplo, em 6 de dezembro de 2017, a Primeira Câmara do Supremo Tribunal de Justiça do México confirmou que os tribunais mexicanos têm jurisdição sobre o Google, uma vez que as ações da plataforma de Internet têm implicações para os direitos dos cidadãos mexicanos.[166] A plataforma argumentou que os tribunais mexicanos não tinham jurisdição sobre o Google baseado nos EUA ao apresentar um recurso de *amparo*,[167] que permite que as pessoas físicas ou morais busquem remédio para a proteção de direitos não especificamente protegidos, mas geralmente consagrados, na Constituição do México.

A Primeira Seção do Supremo Tribunal rejeitou este argumento, citando o princípio *pro persona*, segundo o qual o dever de proteger os direitos fundamentais dos mexicanos tem prioridade sobre outros princípios jurisdicionais. No entanto, não se pronunciou sobre os méritos do próprio recurso.[168]

O Google apresentou um recurso em um caso julgado pelo Oitavo Tribunal Civil da Cidade do México, onde o réu, Morales, processou o Google por se recusar a remover um blog difamatório hospedado na plataforma Blogger.com do Google.[169] Após a rejeição do seu mandado de amparo pelo Supremo Tribunal da Primeira Câmara, o Google México informou

que retirara o seu recurso, evitando assim uma decisão do Supremo Tribunal sobre o escopo jurisdicional no âmbito dos tribunais mexicanos contra o Google.[170]

Além das questões jurisdicionais que surgiram no caso mexicano, a difamação on-line tem uma dimensão internacional decorrente do fato de que o direito à reputação está protegido por vários instrumentos internacionais de direitos humanos e é muitas vezes visto como conflitante com o direito à liberdade de expressão. Com efeito, vários instrumentos internacionais de direitos humanos sublinham especificamente que a liberdade de expressão está sujeita a restrições destinadas a proteger a reputação dos outros.[171]

Embora a atenção geral direcionada à difamação on-line tenha diminuído, novas "reviravoltas" sobre questões clássicas de difamação ainda surgem, como a questão de saber se os termos de pesquisa autocompletados podem resultar em difamação — uma questão que esteve perante os tribunais no Japão,[172] Austrália,[173] Hong Kong RAE,[174] e Alemanha.[175] Questões de escala também surgem, por exemplo, quando uma publicação original é retuitada. Uma publicação que originalmente só chegou a um pequeno grupo de pessoas pode, através da republicação on-line, ter de repente um alcance global e se conectar a um grande número de países. Em tais situações, o editor original pode acabar exposto a um risco legal muito maior do que o que poderia razoavelmente ter sido previsto. As observações sobre o potencial alcance das publicações on-line foram igualmente formuladas pelo Tribunal Europeu dos Direitos do Homem numa candidatura malsucedida apresentada pela Delfi, um canal de notícias on-line da Estônia, em que o Tribunal considerou a Delfi responsável pelos comentários difamatórios publicados por usuários num artigo on-line.[176]

Alguns progressos e iniciativas notáveis incluem:

Em **agosto de 2019**, o **Instituto de Direito Internacional** publicou sua Resolução sobre Danos aos Direitos de Personalidade Através do Uso da Internet: Jurisdição, Lei Aplicável e Reconhecimento de Acórdãos Estrangeiros.[177] A Resolução aborda uma seleção limitada de questões que surgem em ações civis decorrentes de danos causados pela utilização da Internet aos direitos de personalidade de uma pessoa, definidos para incluir, em particular, "a reputação de uma pessoa, dignidade, honra, nome, imagem e privacidade, bem como direitos similares que, independentemente de como são chamados, são protegidos pela lei aplicável".[178]

Em **2019**, o Grupo de Trabalho da Difamação, criado pelo Conselho de Advogados Gerais da Austrália, promoveu uma revisão da lei de difamação na **Austrália** para identificar áreas para a reforma nacional.[179]

Em **2018**, o Gabinete do Comissário para a Privacidade do **Canadá** lançou seu Projeto de Regulamento sobre Reputação on-line como parte do seu trabalho sobre "Reputação e Privacidade" — uma das suas prioridades estratégicas em matéria de privacidade para 2015-2020.[180]

Em **10 de novembro de 2018**, foi relatado[181] que o Facebook havia rejeitado o pedido do governo de **Singapura** para remover um post de um artigo on-line com críticas ao governo. O Ministério da Justiça do país informou que o Facebook se recusou a retirar uma publicação que é claramente falsa, difamatória e usa falsidades para atacar Singapura e indicou que o caso mostrou a necessidade de regulamentação sobre desinformação on-line.[182]

Em **outubro de 2018**, o **Conselho da Europa** publicou seu projeto de estudo sobre formas de responsabilidade e questões jurisdicionais na aplicação das leis de difamação civil e administrativa nos Estados-membros do Conselho da Europa.[183]

A Comissão de Direito de **Ontário** está realizando um grande projeto focado na lei da difamação na era da Internet: "O projeto está examinando o propósito e a função subjacentes das leis de difamação de Ontário e como a lei de difamação deve ser atualizada para contabilizar o 'discurso na Internet', incluindo mídias sociais, blogs, plataformas de Internet e mídia digital."[184] O Documento de Consulta do projeto, lançado em **novembro de 2017**, incluiu uma seção relativa à jurisdição e à escolha da lei.[185]

A **Declaração do Conselho da Europa** pelo Comitê de Ministros sobre a conveniência de normas internacionais relativas à seleção do tribunal ("Forum Shopping", em inglês) em matéria de difamação foi adotada em **4 de julho de 2012**.[186]

3.1.2.1. Âmbito geográfico do direito à reputação

Os litígios transfronteiriços de difamação dão frequentemente origem a questões de "escopo de jurisdição".[187] Por exemplo, quando são concedidas indenizações por conteúdos difamatórios publicados on-line, a questão envolve saber se devem ser concedidas indenizações globais ou mais limitadas, por exemplo, apenas para publicações num determinado Estado. Estas questões podem surgir tanto para a difamação transfronteiriça on-line[188] como off-line.[189]

No processo *Dow Jones contra Gutnick*, o demandante limitou seu pedido aos danos sofridos por publicações na Austrália. No entanto, quando os demandantes buscam indenização por publicações que ocorram fora do Estado em que o tribunal se encontra, ou mesmo por danos a nível mundial, o tribunal deve limitar o âmbito geográfico dos danos concedidos ou participar do complexo exercício de avaliar o que é essencialmente "danos estrangeiros". Esta última opção pode ser controversa devido à sua potencial interferência na liberdade de expressão no(s) Estado(s) afetado(s); ou seja, um tribunal pode acabar por reconhecer danos por publicações ocorridas em Estados nos quais o conteúdo não seria visto como difamatório.

O problema é amplificado ainda mais quando os demandantes buscam exclusão ou retificação do conteúdo difamatório, em vez de danos. Esta foi uma questão central numa decisão de 2017 do Tribunal de Justiça da União Europeia (TJUE).[190] No processo *Bolagsupplysningen OÜ*, o TJUE considerou que uma pessoa pode interpor recurso para: (a) retificação de informações incorretas relativas a essa pessoa, (b) eliminação das observações ilícitas relativas a essa pessoa e (c) reparação por todos os danos sofridos perante os tribunais do Estado-Membro em que se situa o seu "centro de interesses".[191]

A sentença não esclareceu explicitamente se a retificação e a remoção teriam um efeito global. Em 3 de outubro de 2019, foi dada ao TJUE a oportunidade de esclarecer esta questão controversa num processo que lhe foi submetido pelo Supremo Tribunal Austríaco.[192] As conclusões do advogado-geral foram publicadas em 4 de junho de 2019.[193] O advogado-geral Szpunar concluiu que a diretiva da UE relativa ao comércio eletrônico não regula o âmbito da questão de jurisdição e que, por conseguinte, não exclui que um prestador de hospedagem seja

ordenado a remover informações a nível mundial divulgadas através de uma plataforma de rede social.[194] O TJUE tratou apenas brevemente do âmbito da jurisdição. Após ter aceitado a conclusão do Advogado-geral Szpunar, apenas acrescentou que: "Cabe aos Estados-membros assegurar que as medidas que adotarem e que produzem efeitos a nível mundial têm em devida conta essas [as regras aplicáveis internacionalmente]."[195]

No entanto, também é importante o que o advogado-geral Szpunar salientou:

> *Para concluir, depreende-se das considerações que precedem que o tribunal de um Estado-Membro pode, em teoria, pronunciar-se sobre a eliminação mundial das informações divulgadas através da Internet. Todavia, devido às diferenças entre, por um lado, as legislações nacionais e, por outro, a proteção da vida privada e dos direitos de personalidade previstos nessas leis, e para respeitar os direitos fundamentais amplamente reconhecidos, esse tribunal deve, antes, adotar uma abordagem de autolimitação. Portanto, no interesse da cortesia internacional [...], esse tribunal deveria, na medida do possível, limitar os efeitos extraterritoriais de suas junções em relação aos danos à vida privada e aos direitos de personalidade. A implementação de uma obrigação de remoção não deve exceder o necessário para assegurar a proteção da pessoa lesada. Assim, em vez de remover o conteúdo, esse tribunal pode, em um caso apropriado, ordenar que o acesso a essas informações seja desativado com a ajuda de bloqueio geográfico.*[196]

Em 23 de outubro de 2019, o Supremo Tribunal de Délhi concedeu uma sentença exigindo que o Facebook, Twitter e Google removessem determinados conteúdos globalmente, argumentando que tal conteúdo era difamatório ao abrigo da lei local na Índia. Ao tomar a sua decisão, o Tribunal indiano baseou-se numa série de decisões recentes de todo o mundo, incluindo a sentença do TJUE no processo C-18/18.

Isto é significativo uma vez que, na sequência da decisão do TJUE no processo C18/18, vários importantes comentadores argumentaram que a decisão não passava de uma decisão sobre

a linha divisória entre o direito comunitário e o direito nacional, e não constituía uma luz verde às ordens de retirada globais.[197]

No entanto, este acórdão indiano salienta, com toda a clareza, a forma como o processo C-18/18 está sendo utilizado por tribunais estrangeiros. Isto mostra o quão cuidadosos os tribunais devem ser quanto à mensagem de seus acórdãos.

A questão do escopo da jurisdição, incluindo jurisprudência adicional, é discutida mais detalhadamente no Capítulo 4.1.7.

3.1.2.2. Ordens de supressão e desobediência à decisão judicial

Os aspectos jurisdicionais da desobediência a ordens judiciais foram proeminentes no caso de alta repercussão contra o Cardeal Pell por agressão sexual contra dois coroinhas. No momento em que a sentença foi prolatada, relatos do julgamento foram proibidos por uma ordem de supressão. No entanto, as notícias do veredito espalharam-se internacionalmente, levando o Diretor do Ministério Público de Victoria a perseguir vários jornalistas e meios de comunicação.[198]

Essencialmente, a questão é que as ordens de supressão que só são aplicadas localmente têm pouco efeito numa época em que o acesso transfronteiriço à informação é normalizado. Ao mesmo tempo, a ideia de que os tribunais de um Estado deveriam estar autorizados a determinar o que os jornalistas de outros países podem denunciar é incompatível com a maioria dos conceitos de liberdade de imprensa e prejudicaria gravemente a liberdade de expressão e de informação.

Há algum tempo que os especialistas pedem uma reforma do sistema jurídico de contumácia.[199] No entanto, não existem soluções fáceis e as atuais discussões[200] sobre um regime de reconhecimento e execução de ordens de supressão em jurisdições estrangeiras podem ser vistas como ingênuas, dado que a eficácia exige que todos os Estados sejam parte de tal regime.

3.1.3. Bullying on-line

O bullying on-line é predominantemente uma questão doméstica, envolvendo pessoas que têm um relacionamento prévio, como o bullying entre alunos de escolas. Assim, as discussões sobre o bullying on-line tiveram lugar em grande parte a nível nacional.[201] No entanto, a dimensão transfronteiriça é óbvia e inevitável. Afinal, as plataformas de Internet em que o

bullying ocorre são comumente baseadas fora da jurisdição em que as partes estão localizadas, e tanto o acesso a evidências do bullying quanto as medidas tomadas para ter conteúdo de bullying removido têm dimensões transfronteiriças claras. Além disso, o bullying on-line pode ocorrer além das fronteiras, com a vítima e o autor em diferentes Estados, e pode até ser automatizado, por exemplo, através do uso de bots.

O bullying on-line viola as diretrizes da comunidade e os termos de serviço de praticamente todas as principais plataformas de Internet, que também incluem instalações para denunciar conteúdo de bullying.

Tal como a questão da distribuição não consensual de material sexualmente explícito discutida abaixo, o bullying on-line é uma ilustração útil de uma área em que tem havido uma colaboração extensa e frutuosa entre plataformas de Internet, sociedade civil e governos.

A lei que trata de difamação é comumente aplicável em situações que envolvem bullying on-line, mas procedimentos de difamação raramente são seguidos, em grande parte porque eles são notoriamente caros. Em alguns Estados, há também uma dimensão de direito penal para formas graves de bullying on-line.

Em última análise, no entanto, o envolvimento ativo das plataformas parece ser uma ferramenta mais frutífera para lidar com o bullying on-line em geral.

Finalmente, muito parecido com a distribuição não-consensual de conteúdos sexualmente explícitos, o bullying on-line — especialmente entre os jovens — é uma preocupação predominantemente dos países industrializados, uma vez que a porcentagem de alunos com acesso à tecnologia da informação ainda é baixa nos países em desenvolvimento.

Isto irá obviamente mudar com a crescente disponibilidade de tecnologias da informação nos países em desenvolvimento.

3.1.4. Distribuição não consensual de material sexualmente explícito

A distribuição não consensual de vídeos e imagens sexualmente explícitas de um indivíduo — às vezes referida como "pornografia de vingança" — tem sido especificamente criminalizada em alguns Estados,[202] mas também pode ser atacada sob lei de difamação, lei de privacidade de dados, violação de confidencialidade ou até mesmo lei de direitos autorais.

Nos casos em que o autor utiliza uma das principais plataformas on-line, as situações de distribuição não consensual de material sexualmente explícito são — semelhantes ao bullying on-line — geralmente tratadas de forma mais eficaz através de meios de comunicação na plataforma em questão. Isso ocorre porque a distribuição não consensual de mídia sexualmente explícita viola as diretrizes de comunidade e os termos de serviço de praticamente todas as principais plataformas de Internet.

Uma tendência importante é que as plataformas do setor privado, e não os legisladores, tomaram em grande parte a iniciativa de abordar a distribuição não consensual de vídeos e imagens sexualmente explícitas, e de estabelecer rapidamente normas comuns que só depois encontraram uma tradução para alguns quadros legais. Trata-se de uma ilustração da meta-tendência do estabelecimento de normas pelas empresas, discutida nos Capítulos 2.4.2 e 2.5.

Algumas plataformas usam tecnologias de correspondência de fotos (*photomatching*, em inglês) para evitar a publicação ou a republicação não consensual de mídia sexualmente explícita.[203]

Um aspecto controverso desse sistema é que essas tecnologias de correspondência de fotos requerem acesso ao conteúdo da mídia sexualmente explícita que inicialmente foi distribuída sem consentimento. Portanto, uma pessoa com medo de se tornar vítima de distribuição não consensual de mídia sexualmente explícita precisará compartilhar o conteúdo com a plataforma para que as tecnologias de correspondência funcionem. Para evitar a repostagem, no entanto, as tecnologias de correspondência de fotos podem, naturalmente, contar com o conteúdo sexualmente explícito inicialmente detectado.

Mas a distribuição não consensual de mídias sexualmente explícitas também pode ser realizada através de outros canais, como plataformas menores ou por MMS. Nesses casos, as salvaguardas acima referidas não estão necessariamente disponíveis.

A distribuição não consensual de material sexualmente explícito não deve ser confundida com as formas de *sexting*, que envolvem o compartilhamento voluntário de vídeos e imagens sexualmente explícitas. No entanto, esse compartilhamento voluntário pode ainda dar origem a questões jurídicas complexas, como casos em que um menor de idade compartilha voluntariamente vídeos e imagens sexualmente explícitas. Inicialmente, a

mídia sexualmente explícita é frequentemente compartilhada voluntariamente, mas depois distribuída sem consentimento. Isto destaca uma ligação entre o *sexting* voluntário e a distribuição não consensual de mídias sexualmente explícitas.

Há algumas iniciativas que merecem destaque, incluindo:

- A Lei de Segurança On-line de **2018** da **Austrália** (compartilhamento não consensual de imagens íntimas) prevê sanções àqueles que publicam ou ameaçam postar imagens íntimas de outras pessoas on-line sem o seu consentimento. Os autores, websites, provedores de mídias sociais e de hospedagem de conteúdos que não removerem conteúdos ofensivos a pedido do Comissário de Segurança Eletrônica[204] cometem uma infração. O Comissário de Segurança Eletrônica tem uma série de iniciativas, incluindo um portal de abuso baseado em imagens e uma iniciativa de segurança desde a concepção (*by-design*).[205]
- Na área dos conteúdos de abuso sexual infantil, o relatório do **Grupo de Trabalho Técnico** da **Child Dignity Alliance,** de **2018,** fornece recomendações técnicas ao governo e à indústria, incluindo o estabelecimento de um inventário técnico de ferramentas e tecnologias para auxiliar no cumprimento da lei.[206]
- A **Internet Watch Foundation** trabalha para identificar e remover conteúdo de abuso sexual infantil on-line e oferece um portal de denúncias.[207]
- A **5Rights Foundation** defende os direitos às crianças no mundo digital.[208]

3.1.5. Notícias falsas e desinformação

Nem a desinformação nem a desinformação transfronteiriça são fenômenos novos. Nos últimos anos, todavia, tem-se manifestado um interesse sem precedentes nas atividades de desinformação on-line e, em particular, naquilo que foi denominado "notícias falsas" [equivalente à expressão em inglês *fake news*, que ganhou popularidade]. No seu relatório, Freedom on the Net 2017, a Freedom House observou:

> *Os governos de todo o mundo aumentaram drasticamente seus esforços para manipular informações nas mídias sociais ao longo do ano passado. Os regimes chinês e russo foram pioneiros no uso de métodos sub-reptícios para distorcer discussões on-line e suprimir a dissidência há mais de uma década, mas a prática desde então se tornou global. Tais intervenções declaradas representam uma grande ameaça à noção da Internet como uma tecnologia libertadora.*[209]

O quadro pintado no relatório Freedom on the Net de 2018 sugere que essas preocupações permanecem fortes.[210] Além disso, um estudo de 2018 do Reuters Institute for the Study of Journalism, baseado em dados que cobrem quase 40 países e cinco continentes, destacou que a confiança do consumidor nas notícias é baixa e que há altos níveis de preocupação com notícias falsas. Esta preocupação, observa o relatório, é "parcialmente alimentada pelos políticos, que em alguns países já estão usando isso como uma oportunidade para reprimir a liberdade das mídias sociais".[211] O mesmo estudo chamou a atenção para o fato de que, após anos de crescimento contínuo, o uso das mídias sociais para acessar notícias diminuiu em países como os EUA, o Reino Unido e a França, enquanto há um aumento no uso de aplicativos de mensagens para notícias. Esta é uma tendência importante, uma vez que torna o policiamento das redes sociais menos eficiente.

Existem várias iniciativas notáveis — tanto de países industrializados quanto de países em desenvolvimento — que procuram abordar notícias falsas e desinformações. Com foco naqueles que estão fora da esfera de defesa nacional, algumas iniciativas chave são:

As plataformas de mídias sociais anunciaram em **agosto de 2019** que identificaram e removeram contas vinculadas a uma "operação coordenada apoiada pelo Estado" da China espalhando desinformação para atingir a agitação social em **Hong Kong**.[212]

O Projeto de Lei Contra Conteúdo Falso proposto pelas **Filipinas** foi introduzido no Senado em **1 de julho de 2019**. A proposta de lei permite que o Gabinete de Cibercrime do Departamento de Justiça ordene intermediários da Internet, plataformas e indivíduos, onde quer que estejam

localizados, a corrigir, derrubar ou bloquear o acesso a conteúdo determinado pelo Gabinete como falso ou enganoso.[213]

Em **maio de 2019**, **Singapura** aprovou a Lei de Proteção contra Notícias falsas e Manipulação on-line, que permite ao governo exigir que "correções" sejam feitas em conteúdos "falsos".[214]

O Comitê de Seleção Digital, Cultura, Mídia e Esportes do **Reino Unido** divulgou um relatório sobre Desinformação e Notícias falsas em **fevereiro de 2019**[215] e um Livro Branco sobre Danos On-line em **abril de 2019**[216] com ambos os relatórios solicitando mais regulação das plataformas.

Em **2018**, membros do **Grande Comitê Internacional**, incluindo membros dos parlamentos nacionais da Argentina, Bélgica, Brasil, Canadá, França, Letônia, Singapura e Reino Unido assinaram a declaração sobre os Princípios da Lei que regem a Internet, abordando notícias falsas e desinformação on-line.[217]

Em **7 de dezembro de 2018,** foi noticiado[218] que funcionários do Ministério da Eletrônica e Tecnologia da Informação da **Índia** haviam se reunido com representantes do Facebook para rastrear as origens de desinformações que se espalharam pela plataforma de mensagens do Facebook, o WhatsApp, e levaram a surtos de violência.[219]

Em **26 de outubro de 2018**, o Facebook anunciou que havia removido 82 páginas, grupos e contas que estavam vinculados ao **Irã** e espalharam desinformação no Facebook e Instagram. Essas contas foram seguidas por mais de 1 milhão de usuários:[220] "Os administradores das páginas e os proprietários de contas normalmente se apresentavam como cidadãos dos EUA ou, em alguns casos, cidadãos do Reino Unido — e publicaram sobre temas de conteúdo político como relações raciais, oposição ao Presidente e imigração."[221]

Em **2018**, a **Malásia** apresentou Lei contra Notícias falsas. Uma tentativa de revogar a controversa lei foi rejeitada em **setembro de 2018**.[222]

Em **julho de 2018**, foi noticiado[223] que os membros do partido governante da **Rússia**, a Rússia Unida, apresentaram um projeto de lei que propõe responsabilizar as redes sociais pelos comentários "imprecisos" postados pelos usuários. Em especial, a lei exigiria que sites com mais de 100.000 visitantes diários retirassem postagens factualmente imprecisas ou enfrentassem multas de até 50 milhões de rublos (cerca de 800.000 dólares americanos).[224] Em **março de 2019**, houve relatos de que o presidente da Rússia assinou uma nova lei criminalizando usuários que disseminem o que o governo considera ser desinformação, incluindo conteúdo que mostra "desrespeito flagrante" ao governo.[225]

Em **9 de maio de 2018**, a Suprema Corte da **Gâmbia** decidiu que a proibição de "publicações falsas e sua difusão" era constitucional, sustentando a ilegalidade da divulgação de notícias falsas on-line, introduzida como parte da Lei de Informação e Comunicações de 2013.[226] Em 10 de maio de 2018, o secretário-geral da União de Imprensa da Gâmbia, Saikou Jameh, declarou que a decisão era um desvio gritante a uma recente decisão do tribunal da Comunidade Econômica dos Estados da África Ocidental (CEDEAO), que havia decidido que as regras violavam os direitos dos jornalistas e apelou ao governo de Gâmbia que as revogasse imediatamente.[227] Em **2018**, a **Federação Internacional de Associações e Instituições de Bibliotecas** (IFLA) emitiu uma declaração sobre notícias falsas, destacando que respostas políticas desproporcionais podem ter um grande impacto na liberdade intelectual. O depoimento enfatizou a importância de abordar o fenômeno por meio de alfabetização e esforços de pesquisa.[228]

Em **2018**, a **Freedom House** publicou seu relatório Liberdade na Internet: Monitoramento de Eleições.[229]

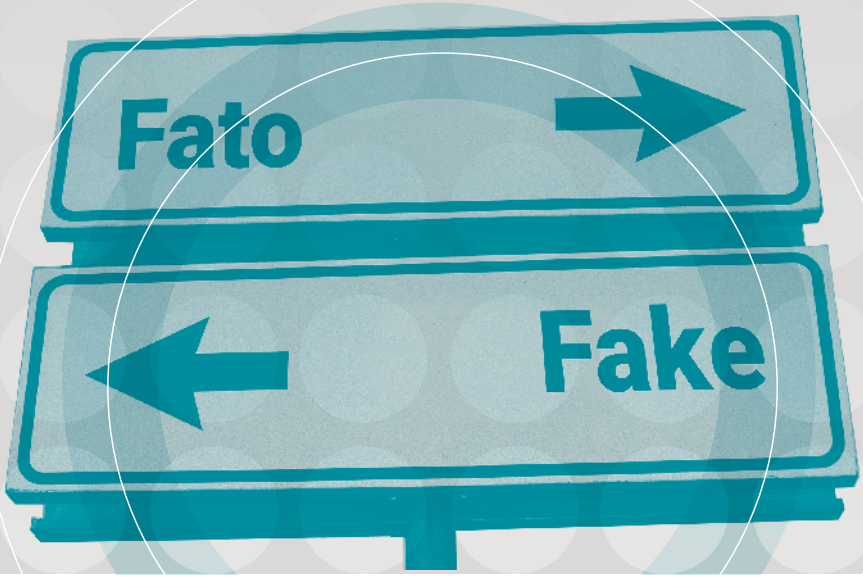
O Belfer Center for Science and International Affairs, da Harvard Kennedy School publicou uma análise de como a **Suécia** protegeu suas eleições de **2018**.[230]

Em **2018**, a **União Europeia** desenvolveu, e várias grandes empresas de Internet assinaram, um Código de Prática sobre Desinformação.[231] Os signatários comprometem-se "a implementar políticas e processos para interromper a publicidade e os incentivos de monetização de comportamentos relevantes, tais como deturpar informações materiais sobre si próprio ou sobre a finalidade de suas propriedades".[232] Em 2019, a Comissão Europeia publicou um relatório de implementação sobre o Código de Prática[233] e, posteriormente, emitiu uma declaração[234] apelando às plataformas de redes sociais para que se esforcem mais para reduzir a disseminação da desinformação. Considere-se também o relatório final do grupo de especialistas de alto nível da Comissão Europeia sobre Notícias falsas e Desinformação On-line.[235]

O **Egito** aprovou uma nova lei em **2018** que, entre outras coisas, aborda notícias falsas. O Artigo 7 da Lei Anticrimes Cibernéticos e Crimes de Tecnologia da Informação dá à autoridade competente encarregada de investigar o crime cibernético "o direito de fechar sites que espalhem notícias falsas contra o Estado egípcio ou ameacem a 'segurança nacional'".[236] A lei tem um efeito extraterritorial, na medida em que autoriza a autoridade competente "a desativar (não bloquear) sites estrangeiros, embora não esteja claro como isso poderia acontecer na prática".[237]

A Digital Citizen Initiative do **Canadá** é uma estratégia de múltiplos componentes destinada a construir resiliência cidadã contra a desinformação on-line e construir parcerias para apoiar um ecossistema de informação saudável.[238]

Através de seu Projeto de Pesquisa de Propaganda Computacional, o **Oxford Internet Institute** vem investigando o uso de algoritmos, automação e propaganda computacional na vida pública desde **2012**.[239] O Instituto já publicou inúmeros relatórios.



Alguns especialistas entrevistados expressaram maiores preocupações com as chamadas *deep fakes* do que com as notícias falsas (*fake news*) *per se*, particularmente no contexto dos temas atuais e da política internacional. As *deep fakes* envolvem a manipulação tecnológica de conteúdos de vídeo e áudio, resultando em representações visuais e/ou gravações áudio altamente realistas e difíceis de detectar de pessoas reais que fazem ou dizem coisas que nunca disseram ou fizeram.[240]

3.1.5.1. Ataques à democracia

As tentativas de usar notícias falsas para afetar os resultados eleitorais ganharam uma atenção considerável no contexto das eleições presidenciais dos EUA em 2016, da votação do Brexit no Reino Unido e de várias outras eleições recentes na França, Alemanha, Suécia e Brasil.[241] Um tema comum aqui é que as notícias falsas e as campanhas de desinformação são orquestradas, e em grandes partes operadas, fora do país afetado, dando origem a complexos desafios jurisdicionais. A preocupação é tal que foram feitos repetidos apelos contra o uso de sistemas de votação eletrônica.[242]

Até o momento, essas atividades raramente resultaram em processos judiciais, embora tenham sido feitas acusações em alguns casos.[243] As dificuldades associadas à apresentação de criminosos estrangeiros à justiça são bem conhecidas. Além disso, nos casos em que são realizadas campanhas de desinformação, apoiadas ou sancionadas por um governo estrangeiro, a assistência executória transfronteiriça contra os infratores é particularmente improvável.

Existem vários relatórios que investigam a interferência russa na eleição presidencial dos EUA de 2016. Um relatório recente, produzido a pedido do Select Committee on Intelligence do Senado dos EUA (SSCI, na sigla em inglês), centrou-se nas atividades da Agência de Pesquisa da Internet (IRA) da Rússia. O relatório revisou um amplo conjunto de dados de postagens e metadados fornecidos ao SSCI pelo Facebook, Twitter e Alphabet, bem como um conjunto de dados relacionados de plataformas adicionais.[244]

Esse relatório concluiu que as operações de interferência ativas e contínuas permanecem em várias plataformas.[245] Também observou que, à medida que a mídia cobriu suas operações no Facebook e Twitter, o IRA transferiu grande parte de sua atividade para o Instagram, e que "o Instagram provavelmente continuará sendo um importante campo de batalha".[246]

O relatório mostrou que "o IRA tinha um viés muito claro para o então candidato Trump que se estendia desde o início da campanha e por todo o conjunto de dados",[247] e concluiu que "devemos promover um modelo multissetorial no qual pesquisadores, plataformas tecnológicas e governo trabalhem juntos para detectar operações de influência estrangeira que tentam minar o discurso público e a democracia".[248] Um relatório contemporâneo do Computational Propaganda Research Project do Oxford Internet Institute chegou a conclusões semelhantes.[249] Há também, é claro, o Relatório sobre a Investigação da Interferência Russa na Eleição Presidencial de 2016 pelo Conselheiro Especial Robert S. Mueller.[250] Durante a eleição presidencial brasileira de 2018 houve vários relatos de desinformação espalhados pelo WhatsApp, bem como por outras plataformas de mídia social.

No dia 19 de outubro de 2018, o WhatsApp do Facebook anunciou[251] que estava tomando medidas legais para impedir que as empresas divulgassem informações erradas em sua plataforma no contexto das eleições presidenciais brasileiras. O segundo turno desta eleição ocorreu em 28 de outubro de 2018.[252]

As campanhas de desinformação que visam afetar vários resultados eleitorais[253] têm sido um ponto focal nas discussões sobre notícias falsas e desinformação. Esta é uma questão particularmente importante, uma vez que hoje muitas pessoas utilizam fontes on-line para se informar sobre questões políticas. Um estudo de junho 2018 por Agência de Pesquisa da Internet (IRA), por exemplo, constatou que 71% dos participantes do estudo acessaram informações políticas na Internet em 2018, em comparação com apenas 47% em 2014.[254] Embora esses números variem de país para país, há uma crescente fiabilidade no conteúdo político da Internet em muitos países.

3.1.5.2. Expressão e moderação da plataforma: responsabilidade, responsabilização e a questão da neutralidade

O papel das plataformas de Internet é um tema central em relação a muitos dos temas abordados no presente Relatório, bem como a várias meta tendências dominantes discutidas no Capítulo 2. O papel dessas plataformas ganhou uma atenção particularmente forte em discussões recentes sobre notícias falsas e desinformação. No rescaldo do escândalo de Cambridge Analytica, por exemplo, a pressão sobre as plataformas da Internet aumentou consideravelmente e várias iniciativas legislativas foram debatidas.

Alguns países já consideram delitos penais que podem ser relevantes. A lei canadense, por exemplo, contém a seguinte infração penal: "Todo aquele que voluntariamente publica uma declaração, conto ou notícia que ele sabe que é falso e que causa ou é susceptível de causar danos ou prejuízos a um interesse público é culpado de um crime sujeito a sanções penais e passível de prisão por um período não superior a dois anos".[255] No entanto, a dificuldade de aplicar a lei focalizada no conteúdo é bem conhecida e claramente ilustrada na jurisprudência, como no caso de *R. v. Zundel*,[256] em que a Suprema Corte do Canadá foi encarregada de examinar a constitucionalidade da referida Seção.

Atacar o equilíbrio certo no contexto das plataformas de Internet é difícil.

Por um lado, eles desempenham um papel importante na censura e combate a notícias falsas e desinformação. Por outro lado, há uma relutância óbvia em fazer com que as plataformas atuem como árbitros da "verdade".

Relacionada à questão da responsabilidade da plataforma, está a questão da responsabilização versus moderação de conteúdo. Estas questões são temas recorrentes ao longo deste Relatório.

Combater notícias falsas através de fontes coletivas (no termo em inglês "crowdsourcing") é outra alternativa. A POLITICO lançou uma dessas iniciativas.[257] Através de uma combinação de informações coletivas e suas próprias investigações, a POLITICO tenta identificar potenciais desinformações. Uma vez identificada, a informação é examinada pelo seu pessoal e, se encaixar em seus parâmetros de notícias falsas, será relatada nas suas conclusões. Os usuários poderão, então, recorrer ao seu banco de dados para verificar se as informações que leram on-line são reais ou falsas.

3.1.6. Privacidade de dados

Embora a privacidade de dados tenha aspectos econômicos e de segurança claros, ela é predominantemente abordada aqui no contexto da expressão.

O interesse pela privacidade de dados (ou proteção de dados) aumentou acentuadamente nos últimos 10 anos, com poucos outros tópicos ganhando tanta atenção em 2018. Isto foi fortemente impulsionado pelo tão aguardado GDPR[258], que entrou em vigor em 25 de maio de 2018. No entanto, ainda há muito

trabalho a fazer, como sugere a conclusão do Ranking do Índice de *Accountability* Corporativa de Direitos Digitais de 2019, segundo a qual a maioria das empresas ainda não consegue divulgar aspectos importantes do modo como tratam e protegem os dados pessoais.[259]

Com a crescente preocupação mundial com a evolução da privacidade dos dados na Europa, avanços importantes noutras partes do mundo — tanto nos países industrializados quanto nos países em desenvolvimento — foram amplamente ignorados. Um estudo destacou que, a partir de 31 de janeiro de 2017, nada menos que 120 países possuem leis de privacidade de dados que atendem aos padrões internacionais.[260] O mesmo estudo apontou para projetos de lei para novas leis de privacidade de dados (introduzidos ou não em legislações) de 30 países adicionais.

Alguns avanços na área de privacidade de dados dignos de destaque incluem:

Em **3 de julho de 2019**, foi relatado que **Ruanda** está trabalhando em uma legislação de proteção de dados pessoais.[261]

Após o recebimento de reclamações de privacidade, o Escritório do Comissário de Informação do **Reino Unido** emitiu um relatório em **junho de 2019** que considera as implicações do GDPR para o uso de lances em tempo real usados na tecnologia publicitária.[262]

Em **fevereiro de 2019**, a Comissão de Proteção de Dados Pessoais de **Singapura** publicou um documento de discussão sobre portabilidade de dados.[263]

Em **fevereiro de 2019**, a Agência Nacional de Desenvolvimento de Tecnologias da Informação da **Nigéria** divulgou seu projeto de Regulamento de Proteção de Dados, inspirado no GDPR.[264]

Em **2019**, o governo **canadense** lançou o Estatuto Digital: Confiança em um mundo digital que busca gerar confiança na proteção de dados.[265]

Em **2019** e após alguns atrasos, a Lei de Proteção de Dados da **Finlândia** entrou em vigor, implementando o GDPR.[266]

Através do Protocolo (CETS nº 223) que altera a Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automático de Dados Pessoais (ETS nº 108) adotado em **2018**, o **Conselho da Europa** modernizou sua Convenção 108.

Em **setembro de 2018**, a autoridade argentina de proteção de dados anunciou a introdução de um projeto de lei de proteção de dados para reformar o regime vigente.[267] A Lei de Proteção de Dados Pessoais da **Argentina** data de 2000. No entanto, o novo projeto de lei de proteção de dados visa a alinhar a lei argentina de proteção de dados com o GDPR.

Uma emenda de **setembro de 2018** fez com que o Projeto de Lei de Proteção de Dados Pessoais da **Tailândia** incorporasse várias disposições que refletem em grande parte as abordagens encontradas no GDPR. Por exemplo, isso se aplica à forma como a questão da extraterritorialidade é abordada.

No **Brasil**, o projeto de Lei Geral de Privacidade de Dados foi aprovado pelo Senado e enviado ao Presidente. No dia **15 de agosto de 2018**, o presidente brasileiro Michel Temer assinou a Lei Geral de Proteção de Dados (LGPD), que estabelece, pela primeira vez na história do país, um marco geral para a proteção de dados. A lei foi descrita como inspirada no GDPR.[268]

O governo do **Quênia** está em processo de desenvolvimento de uma Política e Marco Regulatório para Privacidade e Proteção de Dados, incluindo a Lei de Proteção de Dados 2018. Em **3 de julho de 2018**, um projeto de lei para estabelecer um regime de proteção de dados foi introduzido no Parlamento Queniano. O projeto de lei exige que pessoas físicas e jurídicas que coletam, processam e armazenam dados pessoais obtenham consentimento dos titulares dos dados, imponham obrigações e restrições de segurança de dados a transferências de dados de terceiros e introduzam penalidades por violações.[269]

Em 2018, um projeto de lei que altera substancialmente a Lei de Proteção de Dados nº 19.628 foi revisado e processado no Senado do **Chile**. Em **16 de junho de 2018**, o Congresso Nacional do Chile aprovou uma lei que torna a "proteção dos dados pessoais" um direito constitucional.[270] O Chile se junta ao México, Colômbia e Equador em um grupo de países latino-americanos onde a proteção dos dados é um direito constitucional.[271]

Em **2018**, a Lei de Privacidade 341 (2018) que reformou a lei de privacidade de dados da **Nova Zelândia** estava avançando no processo legislativo.

A Lei de Privacidade do Consumidor da **Califórnia** foi assinada em **2018** e entrará em vigor no início de **2020**. A lei regulamenta a conduta das empresas e expande certos direitos dos consumidores. A Lei se concentra em saber se a empresa em questão "faz negócios no Estado da Califórnia".[272]

Nos **Estados Unidos**, a Internet Association, uma associação comercial que representa exclusivamente as principais empresas globais de Internet em assuntos de política pública, lançou uma campanha para uma lei federal de privaci-

dade de dados.[273] Um especialista pesquisado apontou como os críticos da campanha sugerem que ela poderia ser vista como um esforço para evitar esforços estaduais semelhantes à Lei de Privacidade do Consumidor da Califórnia.[274]

Em **2018**, a Lei **Australiana** de Privacidade de 1988 (Cth) foi alterada para incorporar um sistema obrigatório de notificação de violação de dados. Em **2019**, a Austrália aprovou uma Lei de Direitos do Consumidor que fornece aos usuários direitos para obter acesso e portar seus dados de consumidores detidos pelas empresas.[275]

Após a ratificação da Convenção 108 do **Conselho da Europa**, o governo da **Tunísia** introduziu um projeto de lei sobre proteção de dados pessoais em **2018** (Projeto de Lei 25/2018).

Na **Índia**, a Suprema Corte defendeu o direito à privacidade como um valor constitucionalmente protegido em uma decisão histórica de **2017**,[276] e, em **2018**, um projeto de lei de proteção de dados chamado Lei de Proteção de Dados Pessoais foi apresentado.[277]

Em **2017**, a Lei de Proteção de Informações Pessoais (APPI) passou a vigorar no **Japão**. A Lei compartilha algumas semelhanças com o GDPR, incluindo disposições com aplicação extraterritorial e uma nova estrutura de transferência de dados transfronteiras.

O **Catar** promulgou a Lei nº 13 relativa à Proteção de Dados Pessoais (DPL) em **2016**.

O Marco da **Associação das Nações do Sudeste Asiático** (ASEAN, na sigla em inglês) sobre Proteção de Dados Pessoais foi criado em **2016** para orientar os Estados-membros na regulação da proteção de dados.

Em **2016**, a **Conferência das Nações Unidas sobre Comércio e Desenvolvimento** publicou seu relatório intitulado Regulamentos de proteção de dados e fluxos de dados internacionais: Implicações para o comércio e o desenvolvimento.[278]

A **Comissão Europeia** apresentou uma proposta de regulamento relativo à privacidade e às comunicações eletrônicas que substituirá a Diretiva relativa à privacidade eletrônica.[279]

Em **2015**, o **Conselho dos Direitos Humanos das Nações Unidas** nomeou o seu primeiro Relator Especial sobre o direito à privacidade. O trabalho do Relator Especial está em curso.[280] Observar, também, o Relatório de **2014** do Alto Comissariado das Nações Unidas para os Direitos Humanos intitulado O Direito à Privacidade na Era Digital.[281]

Os Princípios da **Global Network Initiative** sobre Liberdade de Expressão e Privacidade[282] (lançados pela primeira vez em 2008) foram atualizados em **2015** e as Diretrizes atualizadas foram aprovadas em **2017**.[283]

Em **2015**, a **Federação Internacional de Associações e Instituições de Bibliotecas** (IFLA) emitiu uma declaração sobre privacidade no ambiente de bibliotecas.[284]

Em **2013**, a **Organização de Cooperação e Desenvolvimento Econômico** (OCDE) publicou uma versão revista das suas Orientações sobre a Proteção da Privacidade e dos Fluxos Transfronteiriços de Dados Pessoais de 1980. A revisão sublinha a necessidade de abordar a dimensão global da privacidade através de uma melhor interoperabilidade.

Em **2013**, a **International Law Association** criou um Comitê para a Proteção da Privacidade no Direito Internacional e Processual Privado. Os trabalhos do Comitê estão em andamento.

O Centro para a Democracia e a Tecnologia apresentou um projeto de discussão sobre a legislação sobre privacidade para os **EUA**.[285]

Os especialistas entrevistados e consultados enfatizaram a importância dos esforços de coordenação em nível internacional e regional para discutir questões de proteção de dados, por exemplo:

- International Conference on Data Protection and Privacy Commissioners;[286]
- Asia Pacific Privacy Authorities (APPA) Forum;[287]
- IberoAmerican Data Protection Network (*Red Iberoamericana*) (RIPD ou RedIPD);[288]
- Latin American Network of Surveillance, Technology and Society Studies (Lavits);[289]
- European Data Protection Board (EDPB);[290]
- African Network of Data Protection Authorities (RAPDP);[291] e
- Central and Eastern Europe Data Protection Authorities (CEEC).[292]

3.1.6.1. Regulamento Geral de Proteção de Dados da UE (GDPR)

Com o seu potencial para multas extraordinariamente elevadas, o GDPR impacta de diversas maneiras os desafios jurídicos transfronteiriços na Internet. Mais obviamente, o GDPR afirma um amplo escopo de aplicação que vai muito além da UE e impõe restrições para a transferência de dados para fora da UE. Ele também força muitas entidades não pertencentes à UE a designar um representante na UE e se empenha em "configuração padrão", na medida em que algumas multinacionais optaram por adotar o GDPR como seu padrão de operação globalmente. No geral, porém, é a característica de "configuração-padrão" do GDPR que gerará o maior impacto; e o GDPR está sendo usado como o "modelo" para a ampla reforma da lei de privacidade de dados em todo o mundo, da Argentina à Nova Zelândia, e do Quênia à Tailândia.

O GDPR e seu impacto foi um dos temas mais comumente levantados tanto nos resultados quanto nas entrevistas, e foi de longe a iniciativa legislativa mais mencionada. Isso não é surpreendente, dada a quantidade de atenção global que o GDPR recebeu. Na verdade, pode-se sugerir que nenhuma outra iniciativa legislativa na história moderna tenha atraído maior atenção global.

"O GDPR está sendo usado como o "modelo" para a ampla reforma da lei de privacidade de dados em todo o mundo, da Argentina à Nova Zelândia, e do Quênia à Tailândia.

Há pelo menos seis razões pelas quais o mundo tem prestado tanta atenção ao GDPR. Em primeiro lugar, como aludido, o GDPR afirma um amplo escopo de aplicação que vai muito além da UE.

O artigo 3º do GDPR descreve o tipo de elementos de conexão que desencadearão a aplicação do GDPR.[293] Em outras palavras, o GDPR aplica-se a qualquer controlador de dados ou processador com estabelecimento na UE, independentemente de o processamento ocorrer na UE ou não. É igualmente aplicável aos controladores ou processadores não estabelecidos na UE, nos casos em que envolvem os dados pessoais de pessoas físicas que se encontrem na UE — seja oferecendo bens ou serviços a tais pessoas na UE (uma forma de "teste de direcionamento", discutido mais adiante no Capítulo 4.1.5), seja monitorando a sua conduta na UE. Finalmente, o Artigo 3º contém uma regra vaga segundo a qual o GDPR se aplica ao tratamento de dados pessoais por um responsável pelo tratamento não estabelecido na UE, mas em algum lugar onde a lei dos Estados-membros se aplica por força do direito internacional público.

No momento em que o GDPR entrou em vigor, praticamente não havia orientação sobre o alcance exato de sua aplicação. Isso resultou em um grau de incerteza desnecessário entre controladores e processadores não estabelecidos na UE, e isso poderia ser potencialmente afetado pelo escopo de aplicação do GDPR.

PERDA DE ACESSO AO CONTEÚDO

Vários especialistas entrevistados e consultados observaram que serão necessários recursos e custos serão impostos para garantir o cumprimento do GDPR. Em resposta, uma série de pequenas e médias empresas, bem como alguns atores de maior dimensão, em todo o mundo, começaram a utilizar tecnologias de geolocalização (Capítulo 4.2.1) para bloquear o acesso dos usuários aos seus serviços a partir da UE.[294] Europeus que pretendem acessar o site do Chicago Tribune (www.chicagotribune.com), por exemplo, agora se deparam com a seguinte mensagem:

> *"Infelizmente, o nosso site não está disponível na maioria dos países europeus. Estamos trabalhando no assunto e empenhados em analisar opções que apoiem toda a nossa gama de ofertas digitais para o mercado da UE. Continuamos identificando soluções de conformidade técnica que fornecerão a todos os leitores nosso reconhecido jornalismo."*

O vasto âmbito de aplicação "extraterritorial" não é, de modo algum, exclusivo do GDPR. Ele também pode ser encontrado, em várias formas, em leis de privacidade de dados em todo o mundo. No entanto, pelo menos no papel, o GDPR traz uma rede mais ampla do que a maioria das outras leis de privacidade de dados, incluindo a Diretiva de Proteção de Dados (DPD) da UE que o precedeu. Essa ampliação provavelmente se espalhará, já que outras propostas legislativas já estão adotando a linguagem do Artigo 3º[295] do GDPR. Portanto, não seria surpreendente se o GDPR sinalizasse o início de reivindicações cada vez mais amplas de jurisdição nas leis de privacidade de dados em todo o mundo. A segunda razão pela qual o mundo tem prestado tanta atenção ao GDPR é que ele impõe limitações significativas aos fluxos de dados transfronteiriços. Este assunto é explorado mais detalhadamente a seguir.

> **"Não seria surpreendente se o GDPR sinalizasse o início de reivindicações cada vez mais amplas de jurisdição nas leis de privacidade de dados em todo o mundo.**

Em terceiro lugar, embora atualmente seja difícil determinar números exatos, é claro que o GDPR influencia indiretamente as leis de privacidade de dados em todo o mundo, tendo já desencadeado discussões sobre reformas em alguns países fora da UE. Dadas as experiências obtidas com a influência da DPD da UE, pode-se supor com segurança que muitos países ao redor do mundo estarão em condições de recorrer ao GDPR ao criarem ou reformarem suas próprias leis de privacidade de dados (Tailândia, Argentina e Brasil são exemplos dessa tendência). Ao mesmo tempo, um especialista entrevistado observou que é muito difícil para os países em desenvolvimento cumprirem o GDPR devido à necessidade de as autoridades reguladoras nacionais estarem em funcionamento. Muitos países em desenvolvimento simplesmente não dispõem dos recursos, conhecimentos especializados e independência necessários para desempenhar as funções dessas autoridades. Os países desenvolvidos devem ter em conta essas considerações ao formularem os requisitos que impõem a outros Estados que procuram interoperabilidade.

Como o GDPR continua influenciando as leis de privacidade de dados em todo o mundo, podemos esperar certa harmonização.

Ao mesmo tempo, a aplicação real das leis de privacidade de dados é sempre afetada pelos valores subjacentes. A aplicação do GDPR pela UE, por exemplo, será guiada pelo fato de que a Carta dos Direitos Fundamentais da União Europeia consagra especificamente a proteção de dados pessoais.[296] Quando outros Estados adotarem leis baseadas no GDPR, sua aplicação dessas leis será orientada pelos valores subjacentes desses Estados. Isso pode resultar em diferentes aplicações de normas legais aparentemente idênticas ou quase idênticas.

Em quarto lugar, como parte dos mecanismos adotados para aumentar a eficácia da aplicação do GDPR, o Artigo 27 do GDPR exige que um controlador ou processador não estabelecido na União, mas incluído no âmbito de aplicação do GDPR, designe, por escrito, um representante na União. Isto faz parte da tendência da "localização de rep" discutida no Capítulo 4.1.3.

Uma quinta razão pela qual o GDPR ganhou tanta atenção internacional é encontrada nas pesadas multas que podem ser impostas devido a violações. O artigo 83(5) prevê a aplicação de eventuais multas até 20 milhões de euros, ou 4% do volume de negócios anual total do exercício financeiro anterior, o que for mais elevado; isso também faz parte de uma das principais abordagens jurídicas debatidas no Capítulo 4.1.2.

Finalmente, o GDPR ganhou atenção internacional porque algumas multinacionais optaram por adotá-lo como seu padrão global de operação. Nesta "configuração padrão", o GDPR expande os direitos de privacidade de dados de que os usuários gozam em Estados não vinculados pelo GDPR.

Como regulamento, o GDPR é diretamente aplicável nos Estados-membros da UE, ao contrário de sua antecessora, a DPD, que entrou em vigor em 1995.

Como resultado, a UE deve agora ter uma única lei de proteção de dados, em vez de uma colcha de retalhos de leis de proteção de dados com uma origem comum na DPD. Mas o GDPR permite certo número de diferenças nacionais, pelo que a escolha de qual lei dos Estados-membros da UE se aplica continua a ser uma consideração importante em muitas situações.

O Conselho da Europa também modernizou e adotou a Convenção 108 (Convenção 108+) em 2018. A Convenção 108 altera-

da terá uma interação importante com o GDPR, especialmente porque a UE será parte dela. Como um especialista entrevistado observou, isso levará à criação de um fórum multinacional no qual os Estados não pertencentes à UE, que são partes da Convenção 108+, podem discutir o GDPR com a UE em um ambiente de tratados. A interação entre esses instrumentos internacionais exige diálogo, coordenação e cooperação.

3.1.6.2. O direito ao desreferenciamento

As discussões sobre o chamado "direito a ser esquecido" (RTBF, na sigla da expressão em inglês *right to be forgotten*) — hoje denominado "direito ao desreferenciamento" ou "desindexação" — foram largamente desencadeadas pela interpretação do TJUE de certas disposições da DPD 1995 da UE na decisão *Google Espanha* de 2014.[297] Basicamente, ela permite que indivíduos, em determinadas circunstâncias, exijam que os motores de busca excluam links para páginas da Web livremente acessíveis resultantes de pesquisas do seu nome. No entanto, as delimitações exatas do direito ao desreferenciamento variam entre os Estados que o aceitam.

O direito foi transferido para o GDPR. Ganhou também algum reconhecimento fora da Europa, por exemplo, em países como a Argentina, a Índia e a Coreia do Sul. O Comissário de Privacidade do Canadá também considerou que a lei federal de privacidade de dados do Canadá (Personal Information Protection and Electronic Documents Act) prevê o direito de desindexação.[298]

No entanto, o debate sobre as vantagens e desvantagens do direito ao desreferenciamento está longe do fim.[299] Tribunais em alguns Estados, como Japão e China, rejeitaram diretamente reivindicações envolvendo o direito ao desreferenciamento.

Foram levantadas preocupações quanto ao impacto potencial à liberdade de expressão e ao conceito de uma Internet aberta. Em alguns Estados — particularmente na América Latina — as preocupações sobre o direito de desreferenciamento têm sido alimentadas por receios de que ele possa permitir que os autores de recentes violações dos direitos humanos e corrupção ocultem abusos passados. Isto destaca a importância de reconhecer o impacto das origens culturais, sociais, políticas e históricas e dos direitos de exibição em seu contexto mais amplo.

> **Em alguns Estados — particularmente na América Latina — as preocupações sobre o direito de desreferenciamento têm sido alimentadas por receios de que ele possa permitir que os autores de recentes violações dos direitos humanos e corrupção ocultem abusos passados.**

O âmbito da jurisdição do direito de desreferenciamento (isto é, a extensão geográfica da supressão da lista) não foi levantado perante o TJUE no caso do *Google Espanha*. Mas esta importante questão transfronteiriça foi agora apresentada ao TJUE através de uma ação intentada contra o Google LLP pela Commission nationale de l'informatique et des libertés (CNIL), a autoridade de proteção de dados da França. Em sua ação, a CNIL visava a ter as ordens de direito a ser esquecido estendidas globalmente.

Um caso semelhante foi levado aos tribunais da Suécia. Embora, ao contrário da CNIL, a autoridade sueca de proteção de dados (Datainspektionen) tenha argumentado a favor de uma abordagem diferente, segundo a qual o escopo da jurisdição do direito ao desreferenciamento seria guiado pelas circunstâncias em casos individuais.[300]

Em 10 de janeiro de 2019, o advogado-geral Szpunar emitiu as suas conclusões sobre a questão do TJUE. No seu parecer, o advogado-geral concluiu que, em relação ao direito de ser esquecido, os buscadores "devem tomar todas as medidas de que dispõem para garantir um desreferenciamento completo e eficaz na UE."[301] É importante ainda dizer que o advogado-geral acrescentou que o desreferenciamento dos resultados da pesquisa deve aplicar-se apenas no âmbito da UE, porém, ele não excluiu a possibilidade de que "em determinadas situações, um operador de motor de busca possa ser obrigado a tomar medidas de desreferenciamento em nível mundial".[302] Esta abordagem é semelhante à abordagem diferenciada defendida pela APD sueca.

Em 24 de setembro de 2019, o TJUE declarou que:

> *Se um operador de um motor de busca cumprir um pedido de eliminação de referências em conformidade com as disposições [pertinentes], esse operador não é obrigado a efetuar essa eliminação em todas as versões do seu motor de busca, mas sim nas versões desse motor de busca correspondentes a todos os Estados-membros, utilizando, se necessário, medidas que, ao respeitar os requisitos legais, impeçam efetivamente ou, pelo menos, desencorajem seriamente um internauta que efetue uma pesquisa a partir de um dos Estados-membros com base no nome da pessoa em causa de acessar, através da lista dos resultados apresentados na sequência dessa pesquisa, os links que são objeto desse pedido.* [303]

É importante ressaltar que o TJUE salientou a importância dos seguintes aspectos:

- "muitos Estados terceiros não reconhecem o direito ao desreferenciamento ou têm uma abordagem diferente deste direito".[304]
- "o direito à proteção de dados pessoais não é um direito absoluto, mas deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade".[305]
- "o equilíbrio entre o direito à privacidade e a proteção dos dados pessoais, por um lado, e a liberdade de informação dos usuários da Internet, por outro, é provável que varie significativamente em todo o mundo".[306]
- "embora o legislador da UE tenha [...] encontrado um equilíbrio entre esse direito e essa liberdade no que diz respeito à União [...], há que constatar que, pelo contrário, até à data, não encontrou esse equilíbrio no que diz respeito ao alcance do desreferenciamento fora da União".[307]
- "não é de modo algum evidente [...] que o legislador da UE [...] teria optado por conferir um âmbito de aplicação aos [relevantes] direitos [...] de maneira que ultrapassaria o território dos Estados-membros e que teria a intenção de impor a um operador que, como o Google, seja abrangido por essa diretiva ou por esse regulamento uma obrigação de desreferenciamento que diz respeito igualmente às

versões nacionais do seu motor de busca que não correspondem aos Estados-membros."[308]

Por último, é de notar que o TJUE não fechou as portas à abordagem diferenciada prevista pelo Advogado-Geral Szpunar e pela autoridade sueca para a proteção de dados (como acima referido): "embora, tal como mencionado [...] o direito da UE não exige atualmente que o desreferenciamento concedido diga respeito a todas as versões do motor de busca em questão, ele também não proíbe essa prática.

Consequentemente, uma autoridade de supervisão ou judicial de um Estado-membro continua sendo competente para ponderar, à luz das normas nacionais de proteção dos direitos fundamentais [...], o direito à privacidade de um titular de dados e a proteção dos dados pessoais que lhe digam respeito, por um lado, e o direito à liberdade de informações, por outro lado, e, depois de ponderar esses direitos uns contra os outros, ordenar, se for caso disso, ao operador desse motor de busca que proceda a uma remoção de referência relativa a todas as versões desse motor de busca."[309]

As implicações do resultado, bem como o raciocínio que conduziu ao resultado, são altamente significativos, uma vez que se pode esperar que a abordagem da UE se torne influente ou até mesmo uma definição normalizada.

3.1.6.3. Restrição da privacidade dos dados em transferências transfronteiriças de dados

Muitos aspectos da sociedade moderna, tais como transações financeiras internacionais, viagens, comunicação e, até mesmo, pesquisas,[310] dependem de transferências transfronteiriças de dados. Esta dependência só aumentará com a evolução em curso, como a Internet das Coisas (ver Capítulo 3.3.4).

Ao mesmo tempo, as transferências transfronteiriças de dados envolvem normalmente certo grau de perda de controle sobre esses dados e uma erosão da influência direta do organismo encarregado de defender a proteção de dados no país de origem dos dados. Este enigma tem sido uma questão central em iniciativas de proteção de dados internacionais desde 1980, quando foram divulgadas as Orientações da OCDE sobre a Proteção à Privacidade e a Fluxos Transfronteiriços de Dados Pessoais.[311]

O debate de longa data sobre as circunstâncias em que os dados pessoais podem ser transferidos entre fronteiras

prosseguiu nos últimos anos [312] — nomeadamente, no contexto das transferências transatlânticas de dados. Em 2015, o TJUE proferiu uma decisão que invalidou o acordo "porto seguro" que, até então, tinha regido as transferências de dados entre a UE e os EUA.[313] Seguiu-se um período de grande incerteza e, em meados de 2016, o regime "porto seguro" foi substituído por um novo acordo denominado Escudo de Proteção da Privacidade.

Em 2018, a Suprema Corte da Irlanda remeteu ao TJUE questões relativas a outra base para as transferências transfronteiriças de dados: as chamadas Cláusulas Contratuais Padrão (SCC). [314] Essencialmente, a questão diz respeito ao direito da UE de autorizar as SCC, na sua forma atual, como base para a transferência de dados pessoais a partir da UE para os EUA.

> **A conformidade com a Convenção 108+ garante a conformidade com a maioria, mas não todos, dos requisitos do GDPR. Assim, resta saber se o cumprimento de um país com a Convenção 108+ convence a UE a considerar que as leis de privacidade de dados do país cumprem o teste de adequação do GDPR.**

A interação entre o GDPR e a Convenção 108+ do Conselho da Europa suscita questões interessantes no contexto das transferências transfronteiriças de dados e, de um modo mais geral, sobre a interoperabilidade entre diferentes regimes. A conformidade com a Convenção 108+ garante a conformidade com a maioria, mas não todos, dos requisitos do GDPR. Assim, resta saber se o cumprimento de um país com a Convenção 108+ convence a UE a considerar que as leis de privacidade de dados do país cumprem o teste de adequação do GDPR.

No contexto Ásia-Pacífico, a Cooperação Econômica Ásia-Pacífico (APEC) aprovou seu Acordo de Aplicação da Privacidade Transfronteiriça (CPEA) em 2010. [315] A participação no CPEA — um quadro multilateral para a cooperação regional na aplicação das leis de privacidade — está aberta a qualquer autoridade de aplicação da privacidade de uma economia que faça parte da APEC. Os atuais membros são: Austrália, Nova Zelândia, EUA, Japão, Hong Kong, Canadá, Coreia do Sul, México, Singapura, Filipinas e Taipei Chinês.

O sistema de Regras Transfronteiriças de Privacidade (CBPR) da APEC também está ganhando força. O CBPR é um

sistema voluntário, baseado na *accountability*, que facilita o fluxo de dados com respeito à privacidade entre as economias da APEC.[316] Até certo ponto, apresenta semelhanças com o sistema de Regras Corporativas Vinculativas (BCR) do GDPR para transferências transfronteiriças de dados.

Um especialista entrevistado observou que há algumas sugestões de que o sistema CBPR pode ser transformado em um sistema internacional independente, e que o CBPR é reconhecido em outras iniciativas como um bom modelo — por exemplo, no contexto do Acordo Estados Unidos-México sobre comércio digital e no contexto da nova Lei de Proteção de Dados do Japão.

Em junho de 2019, a China lançou um Projeto de Regulamento sobre a Transferência Transfronteiriça de Informações Pessoais, com restrições à transferência de informações pessoais para o exterior, caso tais informações corram o risco de comprometer a segurança nacional e os interesses públicos.[317] A coordenação é urgentemente necessária à medida que vários Estados avançam com a suas próprias avaliações das leis de privacidade de dados de outros Estados. Em 17 de julho de 2017, por exemplo, a APD colombiana lançou uma consulta sobre projetos de regulamentos para reformar as regras de transferências transfronteiriças de dados e identificou países que possuem regras "adequadas" de proteção de dados como condição necessária para permitir tais transferências de dados.[318] Os regulamentos introduzem requisitos que estão em conformidade com a Lei 1581,[319] aprovada em 2012, que introduziu a exigência de proteção adequada dos dados pessoais nas transferências transfronteiriças de dados.[320]

Outra iniciativa recente foi uma proposta do governo japonês durante o G20 em Osaka, em junho de 2019, para a adoção de um conceito de fluxo livre de dados com confiança, exigindo a adoção de regras internacionais para permitir a livre circulação de dados através das fronteiras.[321]

3.2. Segurança

A Internet dá origem a inúmeras questões de segurança, desde a segurança pessoal até a segurança nacional. À medida que a Internet continua a desempenhar um papel cada vez mais central na sociedade, a segurança da Internet só vai se tornar mais importante. Em um mundo onde cada vez mais coisas estão 'conectadas', a interdependência entre segurança on-line da segurança off-line está aumentando.

O significado da cibersegurança está claramente refletido no Relatório de Riscos Globais do Fórum Econômico Mundial de 2018.[322] Entre os 10 principais riscos em termos de probabilidade, os "ciberataques" ficaram em 3º e "fraude ou roubo de dados" ficaram em 4º lugar. Isto é particularmente grave, uma vez que, em termos de impacto, os "ciberataques" também foram classificados em 6º lugar entre os 10 principais riscos. Essa interligação é palpável, uma vez que as ações em um Estado impactam outros Estados, dando origem a muitos desafios jurídicos transfronteiriços no contexto da segurança. Entre eles:

- Países podem ter dificuldades para colaborar e coordenar os esforços de segurança;
- Os criminosos podem se beneficiar significativamente dos obstáculos jurisdicionais à detecção, investigação e repressão dos seus crimes;
- Garantir o acesso a provas digitais muitas vezes depende da cooperação de atores privados, o que desencadeou um reexame do papel que eles desempenham;
- Estados que pretendem colocar os seus cidadãos sob vigilância podem necessitar da cooperação voluntária ou coagida de plataformas estrangeiras operadas por empresas privadas e a quebra da criptografia pode depender da cooperação dos fabricantes de hardware estrangeiros;
- Violações de dados por uma empresa em um Estado podem afetar um grupo mundial de usuários; e
- Os Estados podem adotar soluções de governo eletrônico que envolvam o armazenamento de dados críticos em servidores de países estrangeiros.

É também cada vez mais difícil distinguir entre regulamentação de segurança e outros domínios da regulamentação.

Os requisitos de segurança, por exemplo, são um aspecto padrão de muitos regimes de privacidade de dados. A este respeito, a privacidade e a segurança dos dados são dois lados da mesma moeda, embora os dois sejam frequentemente retratados em oposição uns aos outros.

No campo de segurança on-line, algumas vezes é difícil distinguir entre ilícitos civis, delitos penais, atos de terrorismo e até mesmo agressões militares — e a partir disso, surge uma gama de complicações.[323] Isso contribui para tornar a regulação — e especialmente consenso internacional sobre respostas regulatórias— difíceis de alcançar.

No entanto, algumas distinções estão em andamento. No contexto do acesso a provas digitais, por exemplo, um especialista entrevistado observou que os governos estão cada vez mais enfatizando a necessidade de diferentes processos para questões de segurança nacional, quando comparado com os assuntos criminais tradicionais.

É claro que a área de segurança da Internet é complexa e multifacetada.

Existem alguns exemplos de agentes do setor trabalhando juntos para melhorar a segurança cibernética, incluindo:

- O lançamento do **Conselho para a Segurança da Economia Digital** (CSDE) em **2018** pelos provedores internacionais de serviços de Internet.[324] Os membros da CSDE colaboram com o objetivo de garantir a infraestrutura digital. O CSDE lançou seu Guia Internacional AntiBotnet em 2018.
- A **Cyber Threat Alliance** tem membros do setor que compartilham informações sobre ameaças para melhorar a segurança cibernética e a resiliência.[325]
- O **Cybersecurity Tech Accord** tem mais de 100 membros do setor que procuram para compartilhar capacidades de cibersegurança.[326]
- O **Fórum de Times de Segurança e Resposta a Incidentes (FIRST)** com 400 membros de África, Américas, Ásia, Europa e Oceania.[327]
- O **Grupo de Trabalho Anti-Phishing** envolve autoridades de aplicação da lei, a indústria, ONGs e governos para adotar intercâmbio de dados, pesquisa e sensibilização do público, a fim de responder ao crime cibernético.[328]

- O **Messaging, Malware and Mobile Anti-Abuse Working Group** (M3AAWG) têm membros do setor trabalhando em conjunto para combater os crimes cibernéticos.[329]

No entanto, parece haver necessidade de uma colaboração cada vez mais profunda. Por exemplo, um especialista consultado sugeriu que, dada a natureza sem fronteiras do crime cibernético (em particular, o *malware*), o aumento dos relatórios globais e a criação de um laboratório e biblioteca de *malware* poderiam ser benéficos. Como explicou este especialista, compreender a evolução e tendências, com base nos *big data* que poderiam ser gerados, teria vantagem sobre os inúmeros silos atuais de informações relevantes alojados dentro de governos, universidades e na indústria.

3.2.1. Crime Cibernético

Cada passo, desde a identificação até a investigação, acusação e extradição[330] de cibercrimes e cibercriminosos, levanta questões jurisdicionais. De fato, a luta contra crimes cibernéticos é impossível sem cooperação e coordenação transfronteiriças e, ainda assim, existem muitos obstáculos. O cumprimento eficaz da lei, especialmente se exige cooperação transfronteiriça, exige recursos significativos que raramente estão à disposição dos países em desenvolvimento. Além disso, o direito penal de um Estado está no cerne dos valores e tradições desse Estado, de modo que um ato proibido em um Estado pode ser legal em outro. Ainda há muitos atos que são reconhecidos como crimes em praticamente todos os sistemas jurídicos, e as leis internas de muitos Estados agora lidam especificamente com cibercrimes[331] — e o fazem há algum tempo. Como resultado, os infratores são significativamente menos propensos a confiar em lacunas na lei.

Casos como o infame *worm* de computador "ILOVEYou" 2000 — cujo criador teve que ser libertado porque as Filipinas não tinham leis contra *malware* na época — são muito menos propensos a surgir hoje.

Numa perspectiva futura, o reforço de capacitações e a eliminação de assimetrias devem continuar sendo incluídos entre os objetivos da cooperação e da coordenação transfronteiriças no campo dos crimes cibernéticos.

Através do seu Complexo Global para a Inovação (IGCI) em Singapura, a Interpol busca ser um órgão de coordenação global para a detecção e prevenção de crimes digitais.[332] A Interpol também conta com uma equipe dedicada a Direito das Tecnologias da Informação e das Comunicações (TICs), especializada em projetos jurídicos relacionados com o direito das TIC; e está atualmente envolvida em vários projetos.[333]

No contexto da União Europeia, o Eurojust[334] e o Centro Europeu de Cibercriminalidade da Europol,[335] criados em 2013, juntamente com a sua Força Tarefa Conjunta contra o Cibercrime (J-CAT), lançada em 2014,[336] receberam elogios especiais de alguns dos especialistas entrevistados.

A Convenção do Conselho da Europa sobre Crimes Cibernéticos (a "Convenção de Budapeste") é o mais importante instrumento internacional de combate ao cibercrime.[337] Este importante instrumento serve de orientação para qualquer país que desenvolva legislação nacional abrangente contra crime cibernético e como quadro para a cooperação internacional entre os Estados signatários desse tratado.[338] Em particular, aborda as violações dos direitos autorais, fraude informática, pornografia infantil e violações da segurança de redes. Contém disposições adicionais sobre uma série de poderes e procedimentos, incluindo a procura de redes informáticas e a interceptação. Importante, como salientou um especialista entrevistado, a "Convenção de Budapeste" incorpora salvaguardas dos direitos humanos e faz referência específica aos instrumentos internacionais em matéria de direitos humanos. A partir de 30 de setembro de 2018, a "Convenção de Budapeste" entrou em vigor em 64 países ao redor do mundo.[339]

Outras iniciativas relevantes incluem:

- Projeto de Convenção da União Africana sobre o Estabelecimento de um Arcabouço Jurídico Crível para a Cibersegurança na **África** (**2011**);
- Lei Modelo da **Commonwealth** sobre Crimes Digitais e Relacionados a Computadores (**2002**);[340]
- Convenção das **Nações Unidas** contra o Crime Organizado Transnacional (**2000**) e seus três protocolos;
- Projeto de Convenção Internacional de **Stanford** para Reforçar a Proteção contra Crimes Cibernéticos e o Terrorismo (**1999**);

- Convenção **Interamericana** sobre Assistência Mútua em Matéria Penal (**1992**); e
- Convenção **Europeia** sobre Assistência Mútua em Matéria Penal (**1959**).
- As organizações estabelecidas também estão cada vez mais engajadas nesses problemas.

Em 2018, por exemplo, o Fórum Econômico Mundial criou um Centro se Segurança Cibernética.[341] Há também agências dedicadas à cibersegurança; como a Agência da UE para a Rede e Segurança da Informação (ENISA).[342]

3.2.1.1. Dificuldades de execução devidas à jurisdição como obstáculo

Foi observado que o cibercrime é amplamente subnotificado e que "entre as infrações relatadas e registradas pelas autoridades policiais, apenas uma parte infinitesimal é eventualmente investigada. Destes, apenas uma fração muito pequena é processada, e destes novamente, apenas alguns são julgados."[343]

Diante dessa situação, é natural que alguns comentaristas falem de impunidade *de fato* dos autores de crimes cibernéticos.[344]

Algumas das razões para a baixa taxa de perseguição aos criminosos cibernéticos são destacadas acima, no entanto, desafios jurisdicionais óbvios também desempenham um papel. Tal como salientou o advogado-geral Wathelet no processo C-618/15, "a questão do crime cometido na Internet ("cibercrime") não é simples, uma vez que a Internet é uma rede que é por definição universal, a localização de tal crime, seja o evento causal ou a perda sofrida, é particularmente difícil de determinar."[345] A dificuldade de determinar a localização do crime cometido na Internet pode ser uma grande complicação quanto à aplicação das regras tradicionais de jurisdição. Além disso, nos casos em que o autor da infração se encontra em outro país, a ação penal pode ser limitada pelo grau de extradição dos infratores do país em causa. Esta complicação pode, naturalmente, surgir em relação a qualquer forma de atividade criminosa, mas o cibercrime é particularmente prevalente enquanto atividade transfronteiriça.

O cenário do crime cibernético está mudando para sempre e novas tendências estão surgindo frequentemente.

Por exemplo, a Avaliação da Ameaça do Crime Organizado pela Internet de 2018 da Europol observa que "um volume sig-

nificativo de relatos públicos atribui cada vez mais os ciberataques globais às ações dos Estados-nação".[346] Isso diminui ainda mais a probabilidade de uma ação judicial bem-sucedida.

> **A dificuldade de determinar a localização do crime cometido na Internet pode ser uma grande complicação quanto à aplicação das regras tradicionais de jurisdição.**

3.2.1.2. Darknet — um paraíso criminoso além da jurisdição nacional?

Embora as referências à chamada 'Darknet' sejam comuns, uma compreensão profunda sobre ela é menos comum. O termo "Darknet" tem uma longa história, mas ganhou destaque devido ao comércio ilegal — por exemplo, através da "Silk Road"[347] — realizado em partes da Internet propositadamente fechada à visão pública, ou através de redes ocultas cuja arquitetura é sobreposta na Internet.

As transações realizadas na Darknet podem dificultar a atribuição e complicar a aplicação de fatores de conexão jurisdicional baseados em localização.

A Darknet está desempenhando um papel crescente na distribuição dos materiais mais vis. Como observado pela Avaliação da Ameaça do Crime Organizado na Internet de 2018 da Europol: "Embora a maioria dos CSEM [sigla em inglês para Material de Exploração Sexual de Crianças] ainda seja compartilhada através de plataformas P2P, o material mais radical é cada vez mais encontrado na Darknet."[348] De maneira mais ampla, o mesmo Relatório de Avaliação de Ameaças observa que:

> *A Darknet continuará facilitando os mercados criminosos on-line, em que os criminosos vendem produtos ilícitos, a fim de se envolver em outras atividades criminosas ou evitar a rastreabilidade da rede de superfície. Em 2017, as agências de execução da lei fecharam três dos maiores mercados da Darknet: AlphaBay, Hansa e RAMP. Essas remoções levaram à migração de usuários para mercados existentes ou recém-estabelecidos, ou para outras plataformas, como aplicativos de comunicações criptografadas.*[349]

Embora faltem atualmente estatísticas sobre migração, é possível que, à medida que as principais plataformas on-line imponham regras mais rigorosas sobre os conteúdos publicados pelos seus usuários, os conteúdos ilegais ou censuráveis migrem para plataformas menores, sobre as quais é frequentemente mais difícil reclamar jurisdição.

> **A Darknet está desempenhando um papel crescente na distribuição dos materiais mais vis.**

3.2.2. Acesso a provas digitais

É obrigação do Estado realizar cumprimento efetivo da lei em conformidade com os direitos fundamentais. Para ser eficaz, a execução da lei necessita de um acesso adequado às provas. Esse acesso é essencial tanto para a condenação dos criminosos quanto para a proteção dos acusados injustamente.

Como vários especialistas entrevistados observaram, a importância das evidências digitais aumentou tremendamente ao longo da última década.

Hoje, as informações que podem constituir evidências relevantes — tanto em relação a crimes cibernéticos específicos quanto a crimes tradicionais — são frequentemente armazenadas em estruturas de nuvem fora do Estado da autoridade de execução da lei que precisa de acesso aos dados em questão. Este não é apenas o caso em relação às estruturas de nuvem das principais empresas de Internet, mas também para milhões de provedores de aplicativos diferentes. Além disso, surgem questões específicas em determinados setores.[350] Esta diversidade exerce pressão sobre a escalabilidade de quaisquer soluções propostas.

Determinar a localização dos dados pode ser difícil ou, em alguns casos, impossível. Os problemas que surgem incluem situações em que:

1. a localização dos dados não pode ser determinada num prazo razoável e com medidas razoáveis; e
2. os dados necessários são divididos em servidores em mais de um local.

Mesmo nos casos em que a localização dos dados pode ser verificada, a mobilidade dos dados permite manipular a sua localização a fim de entravar as medidas de execução da lei.

3.2.2.1. Necessidade de reforma do sistema de assistência jurídica mútua (MLA)

O sistema de Assistência Jurídica Mútua (MLA, sigla para o termo em inglês Mutual Legal Assistance) é o principal mecanismo de execução da lei no acesso transfronteiriço a provas[351]. Baseia-se num sistema de acordos entre dois ou mais Estados com o objetivo de recolher e trocar informações para fazer cumprir as leis públicas ou penais.

O sistema MLA é assolado por lacunas, uma vez que nem todos os Estados têm acordos de MLA. Além disso, é amplamente reconhecido — e muitos especialistas entrevistados enfatizaram — que a estrutura do MLA não pode suportar o número de pedidos feitos no seu âmbito. Alguns especialistas entrevistados observaram que faltam orientações para a apresentação dos pedidos, o que conduz à rejeição dos pedidos por erros evitáveis. Os melhoramentos do sistema MLA — e, na verdade, quaisquer outros desenvolvimentos neste domínio — deverão, por conseguinte, incorporar orientações claras e simples para garantir a correta apresentação de arquivos.

Tendo em conta as preocupações acima referidas, mesmo um sistema de MLA melhorado não resolveria os desafios enfrentados para satisfazer a necessidade de os serviços responsáveis pela execução da lei terem acesso transfronteiriço aos elementos de prova. Por exemplo, uma avaliação do Conselho da Europa de 2014 do funcionamento das disposições do MLA concluiu que:

"O processo de assistência jurídica mútua (MLA) é considerado ineficiente em geral, e no que diz respeito à obtenção de provas eletrônicas em particular. Os tempos de resposta aos pedidos de seis a 24 meses parecem ser a norma. Muitos pedidos e, portanto, investigações são abandonados. Isso afeta negativamente a obrigação positiva dos governos de proteger a sociedade e os indivíduos contra o cibercrime e outros crimes envolvendo evidências eletrônicas."[352]

Apesar de seus pontos fracos, há poucos apelos para que a estrutura do MLA seja abandonada. Os pedidos mais comuns são, em vez disso, complementá-lo com um sistema de pedidos diretos aos titulares de dados e tornar o sistema MLA mais eficiente. Os trabalhos sobre este último estão sendo realizados, por exemplo, pelo Conselho da Europa[353] e pela Interpol.[354]

3.2.2.2. Execução de acesso a dados fora da estrutura MLA

As entidades privadas que detêm dados — tipicamente grandes empresas de Internet — estão frequentemente expostas aos requisitos de vários sistemas legais, devido à sua presença em vários mercados. Podem surgir complicações extra se a empresa que detém dados, que são procurados como prova, for uma empresa inteiramente detida por um Estado diferente daquele que pretende acessar os". Um caso em tribunais dos EUA é um exemplo recente disso.[355]

Tal como em muitas outras áreas, a legislação relevante e a forma como a lei é cumprida, difere entre os sistemas jurídicos.

Uma característica comum, no entanto, é que os requisitos de um Estado para quando os seus serviços de execução da lei podem acessar dados transfronteiriços diferem frequentemente dos requisitos impostos aos serviços de execução da lei estrangeiros que procuram acessar dados armazenados por particulares na jurisdição desse mesmo Estado.

As entidades privadas que detêm dados podem ser colocadas em uma posição em que o cumprimento das leis de um Estado resulta inevitavelmente em uma violação direta das leis de outro Estado, porque estão expostas a vários sistemas jurídicos com regras variadas, por exemplo, no que diz respeito aos requisitos de notificação.[356] Tais situações são claramente prejudiciais para todos os atores e existe um amplo consenso de que tais situações devem ser minimizadas ou, se possível, eliminadas.

As regras e os conceitos relevantes do direito internacional (público) são uma parte importante da discussão, embora não sejam bem compreendidos, e muitas vezes formulados em termos injustificadamente absolutistas mais adequados à arena política, do que como orientação sobre questões jurídicas. Esta insegurança jurídica não é sustentável. Em particular, a falta de quadros de cooperação claros dificulta o cumprimento efetivo da lei e prejudica o devido processo. Também incentiva abordagens obrigatórias de localização de dados que são tecnicamente difíceis de implementar e podem ter impactos prejudiciais na economia da nuvem e nos direitos humanos.

Este é um momento crucial, pois vários projetos importantes para lidar com as complicações observadas estão em andamento:

Estão em curso importantes avanços em relação à **Convenção de Budapeste**. De forma mais relevante, estão em curso trabalhos sobre um 2º Protocolo Adicional.[357] Em **2017** foi publicada uma Nota de Orientação relativa às ordens de produção de informação aos signatários,[358] e foram emitidos documentos de trabalho relativos ao acesso da justiça penal aos dados na nuvem.[359] Estão também em curso trabalhos destinados a abordar a relação entre a Convenção de Budapeste, por um lado, e a futura legislação da UE na matéria, por outro.[360]

Em **fevereiro de 2019**, o **Escritório das Nações Unidas sobre Drogas e Crime** (UNODC), a **Diretoria Executiva do Comitê Contra o Terrorismo das Nações Unidas** (CTD) e a **Associação Internacional de Promotores** (IAP) lançaram conjuntamente um Guia Prático para Solicitar Provas Eletrônicas através das Fronteiras.[361]

Em **dezembro de 2018**, o controverso Projeto de Lei de Telecomunicações e Outras Legislações (Assistência e Acesso) de 2018 da **Austrália** recebeu o Parecer Real favorável e tornou-se lei. A lei ganhou atenção mundial devido ao seu impacto negativo de longo alcance na criptografia. Seu amplo alcance jurisdicional ganhou menos atenção: qualquer pessoa, em qualquer lugar do mundo, que opera um site com pelo menos um usuário final na Austrália está sujeita à jurisdição australiana. Além disso, uma parte abrangida pela lei pode ser obrigada a entregar dados sobre os seus usuários ultramarinos e a conceder acesso a dispositivos noutros países.

Em **abril de 2018**, a **Comissão Europeia** publicou a Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece regras harmonizadas para a nomeação de representantes legais para efeitos de recolha de provas em processo penal[362] e a Proposta de Regulamento do Parlamento Europeu e do Conselho sobre as decisões europeias de produção e apreensão relativas a provas eletrônicas em matéria penal.[363] Estes instrumentos propostos complementam-se e devem ser lidos em conjunto. Essencialmente, o efeito combinado da diretiva e do regulamento propostos consiste em implementar um regime ao abrigo do qual os prestadores de serviços — incluindo os prestadores de serviços estrangeiros — seriam obrigados a designar um representante legal na União. Isto se dá com a criação de uma Ordem de Produção Europeia e de uma Ordem Europeia de Conservação. Vários especialistas entrevistados citaram as diferenças existentes entre os Estados-membros da UE como um desafio potencial. No contexto dos instrumentos aqui discutidos, um especialista entrevistado questionou se os países da UE com normas mais fracas, como a Polônia e a Hungria, poderão fazer cumprir as suas exigências noutros países da UE com normas de padrões mais elevados. Em **7 de dezembro de 2018**, o Conselho da UE chegou a acordo sobre a sua posição sobre a proposta de regulamento[364] e, em **8 de março de 2019**, o **Conselho da UE** chegou a acordo sobre a sua posição sobre a diretiva proposta.[365] Conforme observado por um especialista consultado, estas iniciativas da UE não são apenas relevantes do ponto de vista das possibilidades que criam para a aplicação da lei, mas redefinem o papel dos agentes privados (ou seja, os prestadores de serviços) na execução da lei, tornando-os de fato guardiões dos direitos fundamentais; um papel não oficialmente definido na proposta. Esta é uma mudança fundamental na sua posição em relação ao cumprimento da lei e aos seus clientes.

Pelo menos parcialmente impulsionado pela controvérsia em torno da disputa na Microsoft

Corp. v. Estados Unidos,[366] a lei Clarifying Legally Overseas Use of Data Act (CLOUD Act) (H.R.4943) foi promulgada nos **EUA** em **2018**.[367] Uma das principais funções do CLOUD Act é alterar o Stored Communications Act (SCA) de 1986 para permitir que o cumprimento da lei federal obrigue as empresas de tecnologia baseadas nos EUA, através de mandado judicial ou intimação, a fornecer dados solicitados armazenados nos servidores, independentemente de os servidores estarem nos EUA ou em solo estrangeiro. O CLOUD Act também prevê uma estrutura sob a qual governos fora dos EUA podem buscar acesso a dados eletrônicos detidos por prestadores de serviços de comunicação nos EUA, com o objetivo de combater a criminalidade grave. Um especialista entrevistado observou que o CLOUD Act será efetivo em uma base muito limitada, mas pode incentivar outros Estados a elevar ou manter padrões para atender aos seus requisitos. Outro observou que a lei se refere expressamente às normas estabelecidas pela Convenção de Budapeste e, portanto, constitui um incentivo para que os Estados adiram à Convenção de Budapeste. No entanto, outro salientou que o CLOUD Act é calculado para dar ao governo dos EUA a máxima flexibilidade na decisão de quais países terão a oportunidade de fazer exigências diretas aos provedores dos EUA.

Em **9 de janeiro de 2018**, a Corte de Apelação da **Colúmbia Britânica** decidiu que as empresas não-canadenses eram obrigadas a cumprir ordens de produção dos tribunais provinciais e entregar dados às autoridades de execução da lei, desde que a empresa tenha "presença virtual" na província, e mesmo que elas não estejam incorporadas no país.[368] Foi argumentado que a falta de diferença entre presença física e virtual poderia ter implicações importantes além das ordens de produção.[369]

Desde **2012**, as questões jurídicas em torno do acesso de autoridades de execução da lei a evidências digitais tem sido uma área de foco da **Rede de Políticas Internet & Jurisdição**. Como um de seus três Programas Temáticos, o fluxo de trabalho de Dados e Jurisdição tem procurado abordar a questão de como os fluxos de dados transnacionais e a proteção da privacidade são conciliados com os requisitos de acesso legal para combater o crime.[370] Devido ao envolvimento ativo de participantes de uma ampla gama de partes interessadas, avanços significativos foram feitos para o desenvolvimento de um quadro operacional.[371]

Nas discussões de iniciativas como as listadas acima, é importante distinguir entre jurisdição sobre a infração investigada, por um lado, e jurisdição sobre as evidências necessárias para a investigação, por outro. A Convenção de Budapeste articula claramente essa distinção.[372] O artigo 22, a disposição que aborda a jurisdição em termos gerais, diz respeito apenas à jurisdição sobre as infrações previstas na Convenção sobre Crimes Cibernéticos (ou seja, os artigos 2-11), e não regula a jurisdição sobre as provas.

A primeira questão de jurisdição que surge em uma investigação criminal é se o investigador (seja a polícia, um promotor ou um juiz investigativo) tem jurisdição sobre o crime a ser investigado.

Teoricamente, a resposta a esta questão dependerá tanto do direito interno em matéria de jurisdição como do direito internacional. Na prática, porém, os investigadores assumirão (muitas vezes legitimamente) que a lei jurisdicional nacional com que trabalham está em conformidade com o direito internacional. Assim, no nível prático, o direito jurisdicional nacional é tipicamente determinante.

Se for concluído que o investigador tem jurisdição sobre o delito a ser investigado, surge outro tipo de questão jurisdicional: O investigador tem jurisdição para tomar as medidas de investigação que pretende aplicar?

Tradicionalmente, isso tem sido visto como uma questão de "jurisdição de execução" e, portanto, foi agrupado e submetido às mesmas restrições de tipos de ações completamente diferentes, como a de agentes policiais de um país suspeitos de sequestro em outros países, como no famoso Caso *Eichmann*. Mais recentemente, as medidas de investigação foram tratadas como algo marcadamente diferente e o tratamento da "jurisdição de investigação" como uma categoria distinta da jurisdição de execução está ganhando reconhecimento.

Para além destas questões jurisdicionais, as situações em que as autoridades responsáveis pela aplicação da lei procuram o acesso aos dados detidos por entidades privadas, como os intermediários da Internet, dão origem a uma série de outras considerações complexas.

PROGRAMA DE DADOS E JURISDIÇÃO

Os atores da Rede de Políticas Internet & Jurisdição trabalham em conjunto em três programas de políticas: o Programa de Dados e Jurisdição, o Programa de Conteúdo e Jurisdição e o Programa de Domínios e Jurisdição. Os Programas permitem que os membros coordenem informalmente políticas e desenvolvam conjuntamente propostas de Normas, Critérios e Mecanismos Operacionais. O Programa de Dados e Jurisdição concentra-se atualmente no acesso a evidências eletrônicas transfronteiriças para

o objetivo comum de definir normas substantivas e processuais que permitam às autoridades relevantes de países específicos investigações sobre certos tipos de crimes, com clara relação a diretamente apresentar solicitações estruturadas e que respeitam o devido processo legal a empresas privadas de outro país, para obter a divulgação voluntária de dados do usuário.[373] O trabalho atual do Programa de Dados e Jurisdição baseia-se no Roteiro de Ottawa da Rede de Políticas Internet & Jurisdição que produziu propostas concretas para Normas Operacionais, Critérios e Mecanismos em 2019. Ele aborda os seguintes problemas:[374]

- **Normas:** Requisitos estatutários para garantir proteções elevadas e robustas dos direitos humanos, cumprindo simultaneamente os pedidos legais da execução da lei e proporcionando clareza jurídica aos destinatários dos pedidos;
- **Regimes e pedidos de qualificação:** O acesso simplificado aos dados exige um regime de qualificação e pedidos individuais qualificados;
- **Países:** Procedimentos de avaliação e revisão para determinar os países elegíveis, procurando simultaneamente melhorar a prática dos pedidos a todos os países;
- **Autoridades:** Autoridades competentes, definidas por nação ou para unidades dentro de uma nação, para a emissão de pedidos transfronteiriços;
- **Escopo:** Tipos de investigações criminais a considerar no âmbito do tema;
- **Usuários:** Disposições relativas aos usuários que não sejam cidadãos ou residentes do país requerente;
- **Solicitações:** Conteúdo e estrutura dos pedidos devidamente documentados, com a devida autorização legal, incluindo, sempre que possível, a aprovação judicial;
- **Devido processo:** Garantias relativas, entre outras, à notificação do usuário, à capacidade de contestação, ao recurso e à reparação. Apreciação da notificação às nações não requerentes relevantes;
- **Empresas:** Caráter voluntário da divulgação (embora se apliquem fatores semelhantes aos regimes obrigatórios) e procedimentos em caso de dúvida;
- **Dados:** Regras personalizadas para categorias de dados, como dados de conteúdo e não conteúdo, ou para informações especialmente sensíveis;
- **Localização dos dados:** Como lidar com dados armazenados digitalmente, fornecendo peso para fatores além de sua localização física;
- **Escalabilidade:** Extensão do quadro ao longo do tempo, para além dos países participantes iniciais, a fim de responder a uma crescente magnitude e diversidade dos pedidos;
- **Conservação de dados:** Disposições destinadas a preservar os dados relativos a uma investigação individual, antes que um pedido completo de dados possa ser feito; e
- **Capacitação:** Proporcionar formação e pessoal para satisfazer os requisitos do regime.

Isso ilustra a complexidade da execução da lei no acesso a provas armazenadas em nuvem e fora do Estado para obter acesso às provas. Como já foi expresso na literatura e em documentos de política há algum tempo, e como tem sido fortemente enfatizado nas entrevistas realizadas com os atores para este Relatório, há uma clara necessidade de clareza jurídica quanto aos papéis, responsabilidades, autoridades e limitações de todos os interessados na execução da lei com acesso a provas digitais.

As discussões substanciais sobre este tema centraram-se em situações que envolvem organismos responsáveis pela execução da lei que procuram acesso a provas digitais. No entanto, outros organismos governamentais — tais como organismos de defesa do consumidor, organismos de direitos humanos e organismos de proteção de dados — podem procurar esse acesso em circunstâncias semelhantes.

Coloca-se então a questão de saber se as considerações feitas no contexto da execução da lei devem aplicar-se igualmente a esses organismos governamentais. Este é um tema que só vai crescer em importância e que requer atenção urgente.

3.2.2.3. Mudança da localização dos dados como fator de conexão e reconhecimento do papel do equilíbrio de interesses

Até recentemente, as discussões sobre jurisdição no contexto da execução da lei quanto ao acesso aos dados realizados no exterior centraram-se fortemente nas implicações da soberania territorial. Foi comumente assumido que se uma agência de execução da lei no Estado A ganha acesso a provas mantidas em um servidor no Estado B, isso de alguma forma viola a soberania do Estado B, independentemente se o Estado B:

1. tem conhecimento dos dados;
2. pode acessar os dados; ou
3. tem qualquer interesse perceptível nos dados.

Esta interpretação excessivamente zelosa da soberania territorial está em desacordo com a forma como situações semelhantes são abordadas em outras áreas do direito. Considere, por exemplo, uma situação em que um tribunal do Estado A ordena a uma empresa do Estado B que elimine os dados que a empresa detém num servidor do Estado B. Nessas

situações, ninguém parece preocupado com as implicações para a soberania territorial do Estado B. No entanto, neste tipo de situação, o exercício de jurisdição pelo Estado A é mais severo, na medida em que os dados são efetivamente excluídos no Estado B, em vez de meramente acessados.

> **Várias das mais recentes iniciativas neste campo ultrapassaram o foco tradicional na territorialidade.**

Por conseguinte, talvez seja natural que, tal como discutido mais adiante no Capítulo 3.2.2.3, várias das mais recentes iniciativas neste campo ultrapassaram o foco tradicional na territorialidade. O US CLOUD Act inclui disposições que ignoram especificamente a localização dos dados e descrevem as obrigações que se aplicam "independentemente de tal comunicação, registro ou outra informação estar localizada dentro ou fora dos Estados Unidos".[375] Do mesmo modo, tanto o referido Regulamento da UE[376] quanto a Diretiva[377] aplicam-se aos prestadores de serviços "que oferecem serviços" na UE ou num Estado-membro, e nem o regulamento nem a diretiva se concentram na localização dos dados em causa.

O CLOUD Act reconhece explicitamente que os intermediários da Internet podem enfrentar situações em que o cumprimento de uma ordem de produção de dados do governo estrangeiro pode exigir a violação da lei dos EUA, e vice-versa. À luz disso, o CLOUD Act inclui disposições destinadas a garantir que uma análise de cortesia seja realizada em tais situações.

Do mesmo modo, o regulamento e a diretiva da UE incluem um equilíbrio de interesses bastante sofisticado como um aspecto claramente articulado destes instrumentos — em especial no que diz respeito aos artigos 15 e 16 do regulamento. Ele tem por objetivo assegurar a cortesia no que diz respeito aos interesses soberanos de países terceiros, proteger as pessoas em causa e resolver as obrigações conflituosas dos prestadores de serviços, prevendo um mecanismo de controle jurisdicional em caso de conflito com países terceiros.[378] Estas disposições encarregam o tribunal de proceder a um exercício de ponderação de interesses:

Ao pesar um conjunto de elementos que se destinam a verificar a força da conexão com uma das duas jurisdições envolvidas, os respectivos interesses em obter ou, pelo contrário, impedir a divulgação dos dados, e as possíveis consequências para o prestador de serviços de ter de cumprir a Ordem.[379]

3.2.3. Vigilância

A Internet, naturalmente, presta-se à vigilância do setor público e privado. A escala da vigilância estatal — tanto no nível nacional como internacional — ganhou uma atenção considerável na sequência das revelações de Edward Snowden em 2013, particularmente as relativas ao programa de vigilância americano PRISM.[380] No entanto, há constantemente relatos de novas iniciativas de vigilância. Por exemplo, em 20 de dezembro de 2018, o governo indiano emitiu uma ordem permitindo a dez agências públicas interceptar, monitorar ou descriptografar informações geradas, transmitidas, recebidas ou armazenadas em qualquer computador.[381] Indivíduos e organizações que se recusam a cumprir os pedidos de interceptação, monitoramento ou acesso dos dados de cidadãos enfrentam até sete anos de prisão.

Note-se também que certos grupos correm um risco especial de vigilância. Por exemplo, jornalistas e defensores dos direitos civis são frequentemente visados.[382]

Além disso, existe uma ligação direta entre a vigilância e os requisitos de localização de dados. Por exemplo, em 10 de junho de 2017, o New York Times informou sobre uma proposta de lei no Parlamento egípcio que exigiria que serviços de compartilhamento de carros como Uber e o Careem, baseado em Dubai, armazenassem dados de usuários no território do país.[383]

O governo egípcio alegadamente justificou o projeto de lei como necessário para lutar contra terroristas, enquanto ONGs como a Privacy International expressaram preocupação de que a lei pudesse fazer parte de um esforço de vigilância mais amplo.[384]

Vários especialistas entrevistados enfatizaram o "sistema de crédito social" chinês como uma forma particularmente invasiva de vigilância emergente. Ainda há uma incerteza considerável sobre como exatamente o sistema funcionará quando concluído.[385] No entanto, em termos gerais, o crédito social é

como um cartão de avaliação pessoal para cada um dos 1,4 bilhão de cidadãos da China. A pontuação é baseada em informações obtidas a partir de registros governamentais — incluindo educacionais e médicos, avaliações de segurança estadual e registros financeiros — complementadas por vigilância constante via câmeras CCTV e monitoramento de smartphones, bem como o rastreamento de hábitos de navegação na Internet e compras. O escore de crédito social também é afetado pelo comportamento dos amigos e familiares de um indivíduo, bem como com quem eles namoram.[386]

Os cidadãos com uma pontuação elevada podem desfrutar de benefícios como tratamento VIP em hotéis e aeroportos, empréstimos mais baratos e um caminho rápido para as melhores escolas, universidades, cuidados de saúde e empregos.

Aqueles com baixa pontuação podem ser excluídos da sociedade e das mídias sociais, e podem ser impedidos de viajar ou receber crédito ou empregos do governo.[387] Testes estão sendo realizados em várias cidades da China e a intenção parece ser a de que, até 2020, o sistema será implementado nacionalmente.[388] No entanto, o governo chinês ainda não explicou exatamente como o sistema de crédito social irá funcionar, como a pontuação de crédito algorítmica será acumulada e como as diferentes qualidades serão ponderadas umas contra as outras.[389] Embora predominantemente discutida como uma questão doméstica até agora, a dimensão transfronteiriça da vigilância provavelmente aumentará em proeminência nos próximos anos. Por exemplo, pode não ser absurdo imaginar que o referido sistema de crédito social chinês (1) seja adotado de alguma forma por outros Estados, quer voluntariamente, quer como parte de acordos mais amplos com a China, e (2) seja igualmente expandido a pessoas fora da China, de modo a afetar, por exemplo, os pedidos de visto à China. De fato, em setembro de 2019, relatou-se que as autoridades chinesas querem reunir informações de empresas nacionais e estrangeiras que operam na China e integrá-las em uma base de dados digital centralizada destinada a estabelecer um sistema de registro de crédito para os operadores e instituições do mercado.[390]

3.2.3.1. Leis de retenção de dados

O termo retenção de dados refere-se amplamente a dados que estão sendo mantidos para uma variedade de finalidades, incluindo fins legais ou comerciais. Aqui, no entanto, o termo é

usado em um sentido mais restrito. A ideia subjacente às leis de retenção de dados é garantir o acesso a provas, mantendo todas as comunicações para posterior inspeção, caso seja necessário.

Esta prática pode dar origem a desafios jurídicos transfronteiriços, uma vez que os regimes de retenção de dados irão invariavelmente capturar grandes quantidades de dados pessoais sobre estrangeiros, por exemplo, que visitam temporariamente o país ou, potencialmente, sobre estrangeiros que se comunicam com pessoas desse país. Em outras palavras, as leis de retenção de dados em um Estado podem afetar a privacidade de dados dos usuários da Internet em outros Estados.

Dada a dificuldade em prever quais dados podem ser úteis no futuro, os esquemas de retenção de dados exigem a vigilância não direcionada dos dados de *todos*. Isso tem sérias implicações em termos de privacidade de dados que frequentemente têm uma dimensão transnacional.

À luz dessas implicações, as leis de retenção de dados suscitaram controvérsias consideráveis.

O exemplo mais proeminente disso ocorreu em 2014, quando o TJUE declarou inválida a Diretiva de Retenção de Dados da UE (Diretiva 2006/24/CE) por violar direitos fundamentais.[391] Em resposta a esta evolução, vários Estados-membros da UE adotaram novas versões das leis de retenção de dados e a jurisprudência continuou a emergir leis de retenção de dados. Nos Processos Apensos C-203/15 e C698/15, o TJUE observou que a legislação nacional de retenção de dados "deve prever que os dados sejam conservados na União Europeia."[392] Desta forma, as leis de retenção de dados podem introduzir requisitos obrigatórios de localização de dados. Embora estas disputas europeias tenham ganhado de longe a maior atenção internacional, as leis de retenção de dados são generalizadas.

O tipo de retenção de dados acima referido deve ser distinguido da retenção de dados especificamente identificados, como é o caso em situações em que a execução da lei solicita a um titular de dados que garanta a retenção de dados específicos durante um período necessário para a investigação.

Esta última forma de retenção de dados pode desempenhar um papel importante em qualquer estrutura ao abrigo da qual a execução da lei seja incentivada a procurar dados relevantes diretamente do proprietário dos dados, em vez do intermediário da Internet que detém os dados.

Em 2 de outubro de 2018, o TJUE decidiu[393] que as autoridades nacionais responsáveis pela aplicação da lei podem acessar os dados pessoais detidos pelas empresas de telecomunicações, desde que esse acesso não constitua uma violação grave da privacidade.[394] Em particular, o tribunal argumentou que o acesso às informações básicas dos assinantes, conforme necessário para investigar e processar crimes menores, foi justificável. Além disso, no momento da redação do presente relatório, estão em curso processos perante o TJUE relativos à conservação de dados.[395] A legislação sobre conservação de dados não se limita à UE. Por exemplo, em 1 de Julho de 2018, entraram em vigor na Rússia as chamadas "leis de Yarovaya", que introduzem a obrigação de as empresas russas de Internet e de telecomunicações armazenarem a correspondência dos usuários durante seis meses.[396] Os requisitos só se aplicam às empresas listadas no registro de divulgadores de informações na Internet, que não inclui plataformas de Internet estrangeiras.

3.2.3.2. Criptografia e backdoors

Em 17 de agosto de 2018, foi noticiado[397] que o Departamento de Justiça dos EUA tinha pedido ao Facebook para quebrar a criptografia em seu aplicativo Messenger, a fim de que as autoridades policiais pudessem escutar as conversas de voz de um suspeito.[398] Tais solicitações ocorrem tanto internamente quanto além das fronteiras. Questões jurisdicionais óbvias surgem nesta última situação, mas os pedidos internos também podem ter implicações transnacionais, uma vez que podem criar precedentes para pedidos de outros Estados.

A recusa em aderir à descriptografia imposta pelo Estado pode resultar no bloqueio de serviços também em determinados países. Por exemplo, em 1º de maio de 2018, foi relatado que as autoridades judiciais do Irã haviam ordenado que o serviço de mensagens criptografadas Telegram fosse bloqueado no país. O judiciário iraniano justificou a proibição afirmando que o Telegram foi usado para promover propaganda contra a ordem, incentivar atividades terroristas, espalhar mentiras para incitar a opinião pública, provocar protestos antigovernamentais e distribuir pornografia. Em 5 de maio de 2018, em um post no Instagram, o presidente do Irã, Hassan Rouhani, criticou a proibição, indicando que não foi originada por seu

governo.[399] Há uma longa discussão sobre criptografia, mas ela é realizada principalmente em nível nacional. Há uma clara necessidade de uma maior cooperação e coordenação a nível transnacional.[400] As preocupações sobre o impacto da criptografia na eficácia do cumprimento da lei têm sido levantadas há algum tempo. As tecnologias de criptografia são agora baratas e generalizadas, e a criptografia de comunicação e dados armazenados é indiscutivelmente um obstáculo para a detecção, prevenção e investigação de atividades criminosas.

Na ausência de uma análise adicional, pode parecer óbvio fornecer backdoors às autoridades policiais que permitem descriptografia, ou mesmo proibir a criptografia de comunicações e dados completamente.

Para ver os problemas com tais abordagens simplistas, basta considerar até que ponto nossas atividades diárias dependem da criptografia de dados armazenados e comunicações. Imagine fazer transações bancárias on-line sem criptografia, ou fazer uma compra on-line com um número de cartão de crédito não criptografado. Imagine fazer login em seu site de reserva de hotel, programa de milhas aéreas ou conta de e-mail sem que suas credenciais sejam protegidas por criptografia. Em suma, muito do que fazemos on-line depende da criptografia.

Como repetidamente observado no debate sobre criptografia, há um amplo acordo da indústria de que o acesso de terceiros a chaves de criptografia — como backdoors para execução da lei ou outros mecanismos que minam a criptografia — enfraquece a criptografia para todos os usuários, incluindo aqueles não visados pela agência de execução da lei. Apesar disso, o debate continua sendo enquadrado em termos excessivamente simplistas.

Após o tiroteio em massa de 2015 em San Bernardino, Califórnia, o Federal Bureau of Investigation (FBI) procurou acesso a um iPhone 5C dos criminosos protegido por senha. O telefone em questão usava o sistema operacional iOS 8, que tinha recursos avançados de segurança, incluindo criptografia.

A Apple alegou que não poderia quebrar a criptografia sem criar uma backdoor, mas o FBI queria que a empresa alterasse o System Information File (SIF), o que facilitaria a evasão dos recursos de segurança do telefone. A Apple recusou-se. Este confronto terminou quando o FBI conseguiu acessar o iPhone

com assistência de terceiros — supostamente fora dos EUA. No entanto, esta conclusão pouco contribuiu para resolver o importante debate jurídico, ético e técnico a que o processo deu origem.

Em segundo lugar, como observado anteriormente, a controversa Alteração à Lei de Telecomunicações e Outras Legislações (Assistência e Acesso) da Austrália recebeu o Parecer Real favorável e tornou-se lei em dezembro de 2018. A lei ganhou atenção mundial devido ao seu impacto negativo de longo alcance na criptografia. Por exemplo, a Access Now observou que:

> *A legislação permitiria que o governo australiano emitisse ordens secretas para obrigar empresas e fornecedores a fazer 'atos ou coisas' para cumprir ordens judiciais para fornecer informações. Isso poderia significar garantia do acesso a plataformas de mensagens seguras como o WhatsApp. [...] O impacto que isso terá nas empresas pequenas e grandes não pode ser enumerado. Sem dúvida, isso irá minar a confiança dos usuários em seus produtos e serviços não só na Austrália, mas em todo o mundo.*[401]

Como aludido nesta citação, a questão jurisdicional central no debate sobre criptografia decorre do fato de que, como os mesmos produtos são adotados por usuários em vários países, se um Estado toma medidas para minar a criptografia usada nesses produtos, efetivamente enfraquece a criptografia para usuários em todos os Estados em que o produto é usado.

Há também muitos paralelos entre as questões jurisdicionais e processuais que surgem em situações em que as agências de execução da lei procuram o acesso aos dados detidos por entidades privadas, tais como intermediários Internet (discutidas acima no Capítulo 3.2.2), e aqueles que surgem no contexto da criptografia e backdoors.

Considerando o exposto acima, podemos esperar que o debate sobre criptografia persista por um futuro próximo e que mais iniciativas apareçam. Em 6 de outubro de 2017, por exemplo, os Ministérios Públicos da França, Bélgica, Espanha e Marrocos divulgaram uma declaração comum expressando seu desejo de uma legislação para permitir que as autoridades judiciais, no que diz respeito a garantias processuais rigoro-

sas, tenham acesso a dados criptografados quando vidas estão em jogo, como no o caso do terrorismo.[402]

Em julho de 2019, a Five Eyes Security Alliance dos EUA, Reino Unido, Austrália, Canadá e Nova Zelândia alegadamente também apelou às empresas de tecnologia para permitir que as autoridades policiais acessem material criptografado.[403]

> **A questão jurisdicional central no debate sobre criptografia decorre do fato de que, como os mesmos produtos são adotados por usuários em vários países, se um Estado toma medidas para minar a criptografia usada nesses produtos, efetivamente enfraquece a criptografia para usuários em todos os Estados em que o produto é usado.**

3.2.4. Segurança cibernética

Os trabalhos para garantir um grau adequado de segurança cibernética são normalmente realizados em nível nacional. Isto é natural, tendo em conta a forte ligação, e mesmo a sobreposição, entre a cibersegurança e a segurança nacional. Ao mesmo tempo, porém, dado que as ameaças à cibersegurança têm muitas vezes origem no estrangeiro e vários Estados podem ser afetados pela mesma ciberameaça, a dimensão internacional é inegável[404] e a cooperação internacional é natural e necessária. A necessidade de cooperação internacional é aumentada pelo grau em que os Estados usam hardware e software originários de outros Estados.

Alguns exemplos de cooperação internacional incluem:

O **Asia-Pacific Computer Emergency Response Team** (APCERT) que é um grupo nacional de equipes de ponta de resposta a incidentes de segurança informática (CERT) dedicado à proteção da infraestrutura nacional na região Ásia-Pacífico. Além disso, a região da ASEAN está, cada vez mais, coordenando seus esforços para reforçar a cibersegurança regional.[405]

Em **dezembro de 2018,** o **Parlamento Europeu, o Conselho e a Comissão Europeia** chegaram a um acordo político sobre a Lei da UE sobre Cibersegurança.[406] Essa Lei está atualmente em vigor.[407] Além disso, a Diretiva da UE relativa à segurança das redes e dos sistemas de informação (a Diretiva NIS) entrou em vigor em **agosto de 2016**.[408] Os Estados-membros tiveram de transpor a diretiva para as respectivas legislações nacionais até **9 de maio de 2018**.

Normas Mutuamente Acordadas para a Segurança do Roteamento (MANRS), uma iniciativa global apoiada pela Internet Society. Fornece correções cruciais para reduzir as ameaças de roteamento mais comuns; em **dezembro de 2018**, o número de operadores de rede que concordaram com o MANRS ultrapassou 100.[409]

Em **junho de 2018**, a **Global Partners Digital** publicou seu relatório intitulado Multi-Stakeholder Approaches to National Cybersecurity Strategy Development (Abordagens Multissetoriais para o Desenvolvimento de uma Abordagem Nacional à Cibersegurança).[410]

No Fórum de Governança da Internet de **2018**, o Presidente **francês** Macron lançou o Chamado de Paris para a Confiança e Segurança no Ciberespaço.[411]

O **Grupo de Especialistas Governamentais das Nações Unidas** (GGE da ONU) sobre os Desenvolvimentos no Domínio da Informação e das Telecomunicações no Contexto da Segurança Internacional tem trabalhado já há algum tempo no estabelecimento de normas no ciberespaço.[412]

A **Comissão Global para a Estabilidade do Ciberespaço**, que busca estabelecer normas consistentes relacionadas à segurança e estabilidade do ciberespaço.[413]

Liderados por Rússia e China, os Estados-membros da **Organização de Cooperação de Xangai** (SCO) estão buscando o desenvolvimento de normas internacionais universais, regras e princípios relativos ao comportamento responsável dos Estados no espaço da informação: "Especificamente, em 2015, a China distribuiu uma versão atualizada das Regras de Conduta no Campo da Segurança da Informação Internacional em nome dos Estados-membros da SCO como um documento oficial da ONU."[414]

A **Organização para a Segurança e Cooperação na Europa** realizou trabalhos, organizou eventos[415] e emitiu decisões no domínio da cibersegurança.[416]

A **Cybersecurity Initiative by New America**, que visa a construir uma Rede Cibernética Internacional para publicar sobre questões de cibersegurança.[417]

O **Carnegie Endowment for International Peace** realiza uma série de iniciativas na esfera da cibersegurança.[418]

Ao mesmo tempo, a cooperação internacional não deve ser incondicional apenas porque está sob a bandeira da cibersegurança, ou mesmo de crimes cibernéticos. Por exemplo, a Lei de Segurança Cibernética da China entrou em vigor em junho de 2017 e as especulações de que a lei seria amplamente utilizada para fins políticos revelaram-se verdadeiras até agora: "Desde que a lei entrou em vigor, mais de 40% das ações de execução foram para remover "conteúdos politicamente nocivos", e menos de 3% foram para proteger os 'direitos e interesses do 'usuário da Internet'."[419] A Lei de Segurança Cibernética, recentemente aprovada, da Tailândia, também é controversa com algumas preocupações relatadas sobre disposições que permitem ao governo o acesso aos dados dos usuários em uma "emergência nacional".[420] Observadores que acompanharam de perto o desenvolvimento da lei alertaram que, embora a lei seja movida por boas intenções, ela ultrapassa os limites em vários aspectos.[421]

Isto faz parte de uma preocupação mais ampla sobre os mecanismos internacionais de cooperação policial serem abusados para fins de perseguição a dissidentes motivada politicamente. Um artigo da POLITICO de dezembro de 2018, por exemplo, descreve como "o sistema de policiamento internacional já foi sequestrado por autocratas, como o presidente russo Vladimir Putin, que estão usando-o para reprimir seus críticos e têm aliados ocidentais poderosos para ajudá-los".[422]

A necessidade de salvaguardas processuais adequadas não pode ser exagerada.

Além disso, as considerações de segurança cibernética são muitas vezes a fonte dos requisitos de localização forçada de dados (discutidos mais adiante no Capítulo 4.2.7) e, às vezes, também dos requisitos de 'localização de rep' (discutidos mais adiante no Capítulo 4.1.3). Por exemplo, em 2 de novembro de 2018, o governo vietnamita divulgou um projeto de decreto sobre diretrizes para implementar sua Lei de Segurança Cibernética n.º 24/2018/QH14 ("Lei de Segurança Cibernética"), que foi aprovada em 12 de junho de 2018. A lei exige que os prestadores de serviços estabeleçam um escritório local e cumpram os requisitos de localização de dados.[423] Em 24 de fevereiro de 2018, noticiou-se que a Apple começaria a armazenar contas iCloud chinesas e chaves de criptografia na China a partir de 28 de fevereiro de 2018, indicando uma mudança em sua política anterior

de armazenar as chaves de criptografia apenas nos EUA.[424] A decisão de armazenar dados do iCloud chinês em servidores de propriedade e operados pela empresa chinesa Guizhou-Cloud Big Data (GCBD) foi explicada como sendo necessária para cumprir um requisito de localização de dados na Lei de Segurança Cibernética do país, introduzida em 1º de junho de 2017.[425]

A Internet não foi criada com a segurança em mente. Nesse sentido, a segurança cibernética será sempre uma reflexão tardia, a menos que a Internet seja fundamentalmente alterada.

No entanto, do lado positivo, há, sem dúvida, uma maior sensibilização para os riscos envolvidos e essa sensibilização se traduz numa maior preparação para fazer face a esses riscos. Por exemplo, em 9 de outubro de 2019, a UE divulgou uma avaliação dos riscos da segurança das redes 5G.[426] No entanto, a dimensão e a gravidade do desafio da cibersegurança não devem ser subestimadas. O futuro imediato, pelo menos, parece bastante sombrio, sem fim à vista para o constante "jogo de gato-e-rato" entre agressores e aqueles que procuram garantir a segurança cibernética.

Neste contexto, um especialista entrevistado salienta que a infraestrutura originalmente criada por criminosos para atividades criminosas está agora sendo adotada por atividades apoiadas por Estados que visam a, por exemplo, fraudes eleitorais, notícias falsas e discursos de ódio. Isso, salientou o especialista, é um grande desafio para a indústria de segurança cibernética.

> **A necessidade de salvaguardas processuais adequadas não pode ser exagerada.**

3.2.4.1. Violações de dados — uma praga transfronteiriça moderna

Em 2017, uma grande violação de dados na Equifax afetou mais de 100 milhões de usuários de crédito em todo o mundo, expondo implicações globais que são relevantes para os desafios legais transfronteiriços on-line. Com os dados do usuário fluindo para além das fronteiras, o impacto de uma violação de dados em um país raramente fica restrito a esse país. Usuários em todo o mundo são afetados, tornando difícil para as pessoas saberem se seus dados foram vazados. Violações de dados muitas vezes envolvem os dados de titulares de dados em múltiplos Estados, resultando em questões jurisdicionais complexas.

> **Com os dados do usuário fluindo para além das fronteiras, o impacto de uma violação de dados em um país raramente fica restrito a esse país.**

Violações de dados ocorrem por uma série de razões. Sistemas podem ser hackeados, como discutido abaixo, ou pode ocorrer falha humana. Em dezembro de 2018, por exemplo, foi noticiado que um usuário alemão do assistente de voz Alexa da Amazon "obteve acesso a mais de mil gravações de outro usuário por causa de um erro humano da empresa."[427]

"Exemplos como este são comumente relatados e é razoável suspeitar que muitos outros incidentes não sejam relatados. Estes exemplos também ilustram o fato de que pequenos erros podem ter enormes implicações.

Outras violações de dados podem surgir em situações em que os indivíduos sentem que o público merece ter conhecimento de dados confidenciais. As muitas publicações de dados vazados em sites como o WikiLeaks se enquadram nesta categoria.

3.2.4.2. Hackeamento — uma ameaça constante a vários níveis

Tal como acontece com a maioria dos criminosos, aqueles que se envolvem em hackeamento — seja qual for o propósito — podem se beneficiar dos desafios jurídicos transfronteiriços na Internet, na medida em que as fronteiras jurisdicionais podem impedir a detecção, a prevenção, a investigação e a ação penal eficazes. Resulta que é raro que ocorra uma acusação bem-sucedida. No entanto, as acusações transfronteiriças às vezes são apresentadas, como ocorreu quando os EUA acusaram um grupo de hackers chineses de "conspirar para roubar dados tecnológicos comerciais, aeronáuticos e aeroespaciais sensíveis, hackeando computadores nos Estados Unidos e no estrangeiro".[428]

O hackeamento é realizado por uma série de diferentes razões, que vão desde razões financeiras e curiosidade até terrorismo e fins militares. Como enfatizado anteriormente, muitas vezes é difícil distinguir entre pirataria civil e militar, devido, em parte, às dificuldades em garantir uma atribuição precisa. Os agressores muitas vezes visam os pontos mais fracos de um sistema, também. Por exemplo, as tentativas de infiltrar-se nas estruturas nacionais de segurança e defesa visam frequentemente as redes de organizações afiliadas à

defesa, tais como empresas contratadas, em vez de direcionar diretamente as redes governamentais, que são normalmente mais seguras.[429]

Como observado em um relatório recente, a espionagem cibernética representa a ameaça mais avançada para o setor privado e é realizada por uma variedade de razões; "embora seja geralmente associada ao roubo de propriedade intelectual, a espionagem cibernética também pode incluir o roubo de outras informações comercialmente sensíveis, tais como estratégias de negociação da empresa ou planos de negócios."[430]

3.2.4.3. Armazenamento de dados eletrônicos governamentais no exterior

A mudança para soluções de governo eletrônico dá origem aos mesmos tipos de problemas de segurança cibernética que surgem no comércio eletrônico. Mas se o provedor de um site de comércio eletrônico pode sofrer financeiramente, se o site se tornar indisponível, a interrupção de soluções de governo eletrônico pode paralisar a sociedade.

Isso coloca requisitos de segurança cibernética particularmente elevados nas soluções de administração pública on-line. Além disso, as soluções de governo eletrônico devem ser estruturadas de forma suficientemente robusta para permitir que um governo continue operando em estado de emergência, incluindo durante uma invasão de uma potência estrangeira.

Por exemplo, a Estônia — que foi pioneira no domínio do governo eletrônico — afirmou que para "apoiar a independência 'digital' da Estônia e o funcionamento ininterrupto dos serviços públicos de TI em estado de emergência existe um plano de longo prazo para estabelecer embaixadas fora da Estônia em países estrangeiros amigáveis".[431]

Estônia e Luxemburgo chegaram a um acordo, segundo o qual Luxemburgo acolherá uma "embaixada de dados" da Estônia, que terá a mesma proteção e imunidade que as embaixadas tradicionais.[432]

É provável que este tipo de acordo se torne mais comum, dando origem a considerações jurisdicionais complexas. Em caso de litígios, por exemplo, os dados armazenados no exterior podem ser objeto de ações jurisdicionais do estado de acolhimento.

No entanto, o acordo é um exemplo interessante de "extraterritorialidade reversa"; Luxemburgo cede certos direitos que, de outra forma, deteria sobre o território em que se constrói a "embaixada de dados".

3.3. Economia

No contexto econômico, a aplicação transfronteiriça de direitos de propriedade intelectual territorialmente baseados, tributação e tecnologias emergentes como a Internet das Coisas e blockchain. No contexto da expressão e da segurança, como discutido acima, o papel dos intermediários da Internet está sendo reexaminado. De fato, no que diz respeito à economia, parece haver uma mudança mais profunda nas atitudes em relação às plataformas de Internet.

Embora nem sempre tenha sido o caso, as atividades econômicas são agora uma parte natural e importante do ambiente on-line. Por exemplo, estima-se que pelo menos metade de todo o comércio de serviços é fornecido através da Internet;[433] e o Fórum Econômico Mundial estimou que o valor econômico global da transformação digital para empresas e sociedade excederá 100 trilhões de dólares americanos até 2025.[434] Na verdade, mesmo quando oferecido livre de encargos monetários, a maioria dos usos e atividades on-line são comerciais, em grande medida devido à "economia de dados".

O significado da dimensão econômica da Internet continuará aumentando nos próximos anos, graças ao que foi denominado Indústria 4.0. Isto é: "a próxima fase na digitalização do setor manufatureiro, impulsionada por quatro rupturas: o surpreendente aumento dos volumes de dados, do poder computacional e da conectividade, especialmente novas redes de áreas alargadas e baixa potência; o surgimento de capacidades analíticas e de inteligência empresarial; novas formas de interfaces entre homens e máquinas, como interfaces sensíveis ao toque e sistemas de realidade aumentada; e aprimoramento da transferência de instruções digitais para o mundo físico, como robótica avançada e impressão 3D."[435]

A digitalização da economia — através do acesso a uma Internet aberta e da constante evolução tecnológica — é uma força

motriz para o crescimento. Permite que as empresas, em especial as PME, concorram na cena mundial e criem novas oportunidades para desenvolver, encomendar, produzir, comercializar ou entregar seus produtos e serviços.

No entanto, a capacidade de alcançar clientes em todo o mundo em um ritmo mais rápido e a um custo mais baixo do que nunca continua dependendo de um ambiente regulatório gerenciável.

Vários especialistas entrevistados e consultados enfatizaram que o cumprimento de leis muitas vezes complexas de várias fontes exige um grau de sofisticação jurídica que está muitas vezes fora do alcance das PME.

“No entanto, a capacidade de alcançar clientes em todo o mundo em um ritmo mais rápido e a um custo mais baixo do que nunca continua dependendo de um ambiente regulatório gerenciável.

Os especialistas citaram como exemplos específicos a complexidade da regulamentação da proteção da privacidade e dos consumidores e as implicações fiscais. Verificou-se igualmente que as *start-ups* estão expostas à carga regulamentar numa fase em que são menos capazes de suportar tal carga. Para criar uma base de usuários, as novas empresas geralmente devem começar distribuindo seus serviços, antes de construir uma base de usuários comprovada para garantir a receita através de anúncios. No entanto, o custo para garantir a conformidade regulatória é incorrido desde o início — na verdade, mesmo antes do lançamento do serviço.

Os especialistas também observaram que as PME não fazem muitas vezes parte das discussões regulatórias, que se concentram em grande parte nos gigantes da Internet. Simultaneamente, alguns especialistas salientaram que, em comparação com os grandes atores da Internet, as PME estão mais bem colocadas para ignorar as reivindicações de jurisdição de Estados distantes, uma vez que podem mais facilmente evitar colocar pessoas e bens ao alcance dos poderes de execução desses Estados.

OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET CONSTITUEM UM OBSTÁCULO SIGNIFICATIVO PARA AS PEQUENAS E MÉDIAS EMPRESAS (PME)

69% dos especialistas consultados "concordaram", ou "concordaram fortemente", que a complexidade dos desafios jurídicos transfronteiriços na Internet constitui uma barreira significativa para as PME entrarem na economia digital global. 21% "não concordaram nem discordaram" e apenas 10% "discordaram" ou "discordaram fortemente".

Estes números foram, em grande medida, coerentes entre as diferentes regiões e grupos de atores. Alguns, no entanto, afirmaram que a complexidade dos desafios jurídicos transfronteiriços na Internet não constitui tanto uma barreira para as PME *entrarem* na economia digital global, quanto é uma barreira para as PME *que procuram o crescimento* da economia digital global.

> **O comércio transfronteiriço na Internet também tem o potencial de ser um equalizador entre o mundo desenvolvido e o mundo em desenvolvimento.**

O comércio transfronteiriço na Internet também tem o potencial de ser um equalizador entre o mundo desenvolvido e o mundo em desenvolvimento, uma vez que permite aos países em desenvolvimento contornar alguns dos passos pelos quais os países desenvolvidos tiveram de passar. No entanto, enquanto as vantagens potenciais são grandes, também o são alguns dos obstáculos.

OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET CONSTITUEM UM OBSTÁCULO SIGNIFICATIVO PARA OS PAÍSES EM DESENVOLVIMENTO

Durante a pesquisa, 54% dos especialistas pesquisados concordaram, ou "concordaram fortemente", que a complexidade dos desafios jurídicos transfronteiriços na Internet constitui uma barreira significativa para os países em desenvolvimento entrarem na economia digital global. 37,5% "não concordaram nem discordaram", e apenas 8,5% "discordaram", ou "discordaram fortemente", que a complexidade dos desafios jurídicos transfronteiriços na Internet constitui uma barreira significativa para os países em desenvolvimento entrarem na economia digital global.

Um especialista consultado observou que o receio das dificuldades jurídicas associadas à atividade transfronteiriça na Internet dissuade as pessoas nos países em desenvolvimento de se envolverem em tais atividades. Além disso, um especialista entrevistado observou que a principal dificuldade enfrentada pelos países em desenvolvimento é o ritmo significativamente mais rápido em que a Internet evolui hoje, em comparação com o passado. O ritmo de mudança no ambiente regulatório e sua crescente complexidade - devido, em grande parte, ao aumento do apetite e da extraterritorialidade regulatórias - também está aumentando.

No entanto, a pesquisa também revelou uma diferença acentuada de atitudes entre especialistas pesquisados de diferentes regiões. Tanto os especialistas consultados quanto os entrevistados enfatizaram que a pobreza, os níveis de habilidade, o analfabetismo, as barreiras linguísticas, a instabilidade política, a falta de investidores e infraestruturas de má qualidade das TIC são preocupações maiores em regiões como África e algumas partes da América Latina, do que os desafios legais transfronteiriços. Especialistas entrevistados e consultados também observaram que grande parte da atividade on-line nos países em desenvolvimento é de natureza local e, portanto, enfrenta com menos frequência a complexidade dos desafios jurídicos transfronteiriços na Internet. Os especialistas também levantaram a questão de que os países em desenvolvimento muitas vezes não fazem parte, e nem sequer têm conhecimento, dos acordos e outros desenvolvimentos regulatórios discutidos ou concluídos entre os países. Especialistas observaram que os países em desenvolvimento enfrentam dificuldades ao tentar aplicar suas leis de forma extraterritorial que afeta países em desenvolvimento, incluindo empresas e pessoas em países em desenvolvimento. Há também uma percepção de que, em comparação com os países desenvolvidos, os países em desenvolvimento têm menos influência nas abordagens tomadas pelos principais atores da Internet. Este sentimento de desempoderamento é uma tendência clara e, indiscutivelmente, pressiona os países em desenvolvimento a escolherem entre abordagens existentes e parcialmente concorrentes (por exemplo, entre uma "abordagem ocidental" que promove valores democráticos e uma abordagem chinesa de "soberania digital"), em vez de terem a oportunidade de desenvolver suas próprias abordagens.

Em conjunto, isto sugere que, embora a complexidade dos desafios jurídicos transfronteiriços na Internet seja uma barreira importante para os países em desenvolvimento entrarem na economia digital global, é apenas uma das várias — e talvez não a mais aguda. No entanto, não há dúvida de que, uma vez enfrentados os desafios mais prementes, o impacto total dos desafios jurídicos transfronteiriços será inevitavelmente sentido, a menos que possam ser atenuados antecipadamente.

Para além do que é discutido a seguir, devem ser assinaladas numerosas outras iniciativas e avanços:

Em **julho de 2019**, a **Conferência da Haia de Direito Internacional Privado** concluiu a sua Convenção sobre o Reconhecimento e Execução de Decisões Estrangeiras em Matéria Civil ou Comercial (Projeto Julgamentos).[436] Embora seja demasiado cedo para avaliar as suas implicações, este é claramente um instrumento de enorme potencial. Além disso, os Princípios de 2015 da Conferência de Haia sobre a Escolha do Direito nos Contratos Comerciais Internacionais[437] e a Convenção de 2005 sobre os Acordos de Escolha do Foro[438] são de relevância direta para o comércio on-line.

A **APEC** lançou um projeto destinado a identificar tendências globais no comércio digital, bem como oportunidades e desafios para permitir que as PME aproveitem e se beneficiem do comércio digital. O projeto fará igualmente recomendações à APEC sobre como ajudar as PME a tirar partido das oportunidades proporcionadas pelo comércio digital[439] e um relatório foi publicado em **junho de 2019**.[440]

Em **julho de 2018**, o Secretário-Geral da **ONU** convocou um Painel de Alto Nível sobre Cooperação Digital. O resultado será um relatório que visa a sensibilizar para o impacto das tecnologias digitais na economia e na sociedade e apresentar propostas de melhoria da cooperação.[441]

A **Conferência das Nações Unidas sobre Comércio e Desenvolvimento** (CNUCED) demonstrou que **145 países** (dos quais 104 são classificados como economias em desenvolvimento ou em transição) adotaram leis de transações eletrônicas que reconhecem a equivalência jurídica entre as formas de intercâmbio em papel e eletrônica.[442]

O **Fórum Econômico Mundial** está buscando diversos projetos, como sua Iniciativa de Transformação Digital, que visa fornecer uma base de evidências e uma linguagem comum para a colaboração público-privada focada em assegurar que os benefícios da transformação digital sejam compartilhados de forma justa e ampla.[443] O Trade Project apoia o desenvolvimento de quadros políticos que maximizam os benefícios do comércio digital e dos fluxos de dados.[444] Em **2017**, o Fórum Econômico Mundial publicou um livro branco intitulado "Making Deals in Cyberspace: What's the problem?" ("Estabelecendo Acordos no Ciberespaço: qual é o problema?"), que visa a construir o conhecimento das regras atuais de transações e assinaturas eletrônicas.[445] Esse documento concluiu que: "Embora muitos países já tenham leis de referência em matéria de transações eletrônicas [...] divergências nos detalhes são manifestas e nem sempre abordam aspectos transfronteiriços."[446]

Na reunião do **G20** em Düsseldorf, Alemanha, em **2017**, os ministros responsáveis pela economia digital emitiram a Declaração Ministerial sobre a Economia Digital do G20 (ou a Declaração de Dusseldorf), que inclui um Roteiro para a Digitalização que estabelece políticas para a economia digital e as Prioridades do G20 sobre Comércio Digital.[447]

Em **2017**, a **OCDE** divulgou seu relatório bienal sobre desafios emergentes e oportunidades para a economia digital: a Perspectiva sobre a Economia Digital da OCDE de 2017.[448] A OCDE também criou um Grupo Consultivo para a Medição do PIB em uma economia digitalizada.[449]

O **Fórum Econômico Mundial** também está envolvido em uma iniciativa conjunta para Habilitar o Comércio Eletrônico com a **Organização Mundial do Comércio** e a **Plataforma de Comércio Eletrônico Mundial**. A iniciativa visa a incentivar discussões de alto nível sobre a forma como as políticas de comércio eletrônico podem beneficiar as PME.[450]

O **Fórum Global de Expertise Cibernética** considera o que países, organizações internacionais e empresas privadas podem fazer para compartilhar as melhores práticas e iniciativas sobre capacitações cibernéticas.[451] A **União Internacional de Telecomunicações** (UIT) também considerou a capacitação para a economia digital.[452]

A **Organização Mundial do Comércio** (OMC) se envolve com a economia digital em diversos ângulos. Já em **1998**, a OMC reconheceu que o comércio eletrônico global estava crescendo e criando novas oportunidades para o comércio e respondeu adotando sua Declaração sobre o Comércio Eletrônico Global.[453] Várias outras iniciativas também podem ser observadas.[454] A Declaração de Doha endossou o trabalho já realizado em matéria de comércio eletrônico e encarregou o Conselho Geral de considerar as disposições institucionais mais adequadas para o tratamento do programa de trabalho e de informar sobre os progressos realizados na Quinta Conferência Ministerial.[455]

Desde **meados da década de 1990**, a **Comissão das Nações Unidas para o Direito do Comércio Internacional** (UNCITRAL) vem trabalhando para aumentar a uniformidade das leis que regem as transações eletrônicas, as assinaturas e a autenticação digital. Suas principais realizações são: (1) Lei Modelo da UNCITRAL sobre o Comércio Eletrônico (MLEC) (1996), (2) Lei Modelo da UNCITRAL sobre Assinaturas Eletrônicas (MLES) (2001), (3) Convenção das Nações Unidas sobre a Utilização de Comunicações Eletrônicas em Contratos Internacionais (ECC) (2005) e (4) Lei Modelo da UNCITRAL sobre Registros Eletrônicos Transferíveis (MLETR) (2017).

3.3.1. Propriedade intelectual

Vários desafios jurídicos transfronteiriços na Internet relacionam-se com questões de propriedade intelectual. Um estudo de 2013 realizado pelo Fordham Center on Law and Information Policy constatou que a maioria dos casos de jurisdição da Internet nos EUA se centrava em disputas relativas à propriedade intelectual. Desses casos, 43% referiam-se a marcas registradas, 20% a direitos autorais e 9% a patentes.[456]

O domínio da propriedade intelectual provocou muitos dos primeiros casos de jurisdição na Internet, incluindo o conhecido *caso Zippo*,[457] no qual o Tribunal concebeu o famoso teste de "escala móvel" (ver Capítulo 2.2.5), e as questões de propriedade intelectual transfronteiriça atualmente continuam gerando desafios. Estes desafios dizem respeito, por exemplo, aos obstáculos à aplicação efetiva dos direitos de propriedade intelectual, ao equilíbrio desses direitos com outros direitos (por exemplo, privacidade de dados e liberdade de expressão) e à esfera de jurisdição, tais como as que foram submetidas à Suprema Corte do Canadá no Caso *Equustek*.[458]

Nesse caso, o tribunal reafirmou a liminar de um juiz da Colúmbia Britânica forçando o Google a remover os resultados da pesquisa globalmente, em vez de apenas dentro do território canadense,[459] mas a disputa continuou muito além da decisão do Supremo Tribunal do Canadá, proferida em junho de 2017.[460] Em abril de 2018, o Supremo Tribunal da Colúmbia Britânica, Canadá, emitiu uma decisão negando o pedido do Google para alterar uma liminar exigindo que ele removesse os resultados dos motores de busca globalmente no processo Equustek.[461] Além disso, o papel dos intermediários da Internet na prevenção, detecção, investigação e tomada de medidas legais em resposta às infrações à propriedade intelectual ganharam uma atenção considerável — para além das questões relativas à sua responsabilidade. Na verdade, existem vários exemplos recentes sobre essas questões, incluindo a decisão do Tribunal Federal de Justiça da Alemanha, em setembro de 2018, de enviar um processo ao TJUE para saber se o YouTube pode ser responsabilizado por hospedar vídeos que infrinjam direitos autorais.[462]

Em algumas jurisdições, os tribunais determinaram que os provedores não são responsáveis por violar conteúdo. Por

exemplo, o Supremo Tribunal Suíço decidiu recentemente que os provedores de serviços de Internet não poderiam ser obrigados a bloquear sites que incluem filmes que infrinjam direitos autorais.[463] Além disso, o Tribunal de Apelações austríaco anulou uma decisão anterior para declarar que o YouTube não é responsável por material infrator de direitos autorais, alegando que o YouTube não tem um "papel ativo" na violação de direitos autorais.[464] Em outras jurisdições, os tribunais consideraram plataformas de compartilhamento de vídeo (na Itália) e organizações de mídia (na Austrália) como responsáveis pelo conteúdo carregado pelos usuários.[465] Os tribunais indianos descobriram que a questão de saber se uma plataforma de comércio eletrônico é um "intermediário" (e, por conseguinte, protegido por disposições de "porto seguro" ("safe harbor") na legislação indiana) depende do fato de estes desempenharem apenas um papel inativo ou passivo no processo de comercialização e venda. No caso *Christian Louboutin SAS vs Nakul Bajaj e Ors*,[466] a plataforma foi considerada responsável, como tinha um papel ativo na comercialização e venda de produtos infratores.[467]

Outra iniciativa diz respeito a propostas de alterações à lei de direitos autorais da Rússia, que permitiriam aos titulares de direitos solicitar aos servidores web que bloqueiem sites com material pirateado sem um pedido judicial se não houver resposta a pedidos de retirada.[468] A frequência com que as questões de jurisdição da Internet surgem no contexto da propriedade intelectual pode não ser surpreendente, dado o contraste entre a natureza fortemente territorial dos direitos de propriedade intelectual, por um lado, e a natureza global da Internet, por outro.

Conforme apontado por um especialista consultado, os direitos de marca são determinados e limitados por cada jurisdição, o que estabelece, dentro de seus próprios limites territoriais, os pré-requisitos para proteção de marcas e as normas de infração e defesa, como quando uma marca não pode ser a base para excluir outras de usá-la, por exemplo, como funcional, uso justo ou genérico. Uma marca registrada pode, portanto, ser válida ou famosa em uma jurisdição, mas não em outra.

Permitir que uma jurisdição determine a aplicabilidade global de uma marca comercial está, portanto, em contradição com a base territorial dos direitos de marca comercial.

Ao mesmo tempo, observa-se que os direitos de propriedade intelectual "não podem estar vinculados a um território físico e geográfico preciso, mas sim a fenômenos sociais e universais."[469] E que "o risco de apropriação indevida transnacional de DPI levanta uma série de questões sobre como proteger esses direitos universalmente, expondo o princípio territorial a dúvidas crescentes."[470]

Neste contexto, há que assinalar várias iniciativas:

A Diretiva da **UE** sobre Direitos de Autor no Mercado Único Digital[471] (Diretiva de Direitos de Autor da UE 2018) foi adotada pelo Parlamento Europeu em **março de 2019**[472] e foi concebida para atualizar as leis de direitos autorais para o ambiente digital. O artigo 13 da diretiva proposta exige, de forma controversa, que sítios da Web como YouTube, Google e Facebook tomem medidas "adequadas e proporcionais" para impedir que os usuários publiquem conteúdos não autorizados de direitos de autor (conhecida como medida de filtragem ou, por alguns críticos, proibição de memes). No que diz respeito à UE, deve igualmente ser dada atenção à Diretiva relativa à aplicação dos direitos de propriedade intelectual ("IPRED"), tais como direitos de autor e direitos conexos, marcas, desenhos ou modelos ou patentes, adotada em abril de 2004[473] e avaliada em 2017.[474]

Em **maio de 2016**, o Escritório de Propriedade Intelectual do **Reino Unido** publicou o policy paper "Protecting creativity, supporting innovation: IP enforcement 2020".[475]

Em **2010**, a **Associação Internacional de Direito** criou um Comitê de Propriedade Intelectual e Direito Internacional Privado. Os trabalhos do Comitê estão em andamento.

Numerosas instituições, como o Centro de Estudos Internacionais de Propriedade Intelectual (CEIPI) da **Universidade de Estrasburgo**, fornecem comentários pormenorizados sobre a próxima reforma nessa área.[476]

A conhecida Política Uniforme para Resolução de Disputas sobre nomes de domínio (UDRP) da **ICANN**, adotada em todos os gTLDs por registradores credenciados pela ICANN, é uma ferramenta de longa data para resolver disputas de propriedade intelectual na esfera de nomes de domínio (como cybersquatting [ciberocupação]) .[477]

3.3.1.1. Aquisição transfronteiriça agressiva de propriedade intelectual

Uma vez que a propriedade intelectual é uma das principais salvaguardas para proteger a inovação, não é surpreendente que surja uma concorrência feroz à sua volta. Nesse contexto, existe uma clara dimensão transfronteiriça, uma vez que os diferentes Estados competem para obter vantagens orienta-

das para a inovação à medida que o mundo se dirige para uma era da Indústria 4.0. Em poucas palavras, as reivindicações de jurisdição facilitam o controle sobre a propriedade intelectual, o que, por sua vez, permite o controle sobre a inovação, potencialmente levando a vantagens econômicas, sociais e militares.

Grande parte do atual debate neste domínio tem-se centrado na relação entre os EUA e a China. Em 2015, o Presidente Obama reuniu-se com o Presidente chinês Xi Jinping e chegou a um acordo sobre uma série de questões. Entre outras coisas, os dois países concordaram que "nenhum governo do país conduzirá ou apoiará conscientemente o roubo de propriedade intelectual, incluindo segredos comerciais ou outras informações comerciais confidenciais, com a intenção de oferecer vantagens competitivas a empresas ou setores comerciais."[478] No entanto, os EUA continuam preocupados com o fato de a China facilitar injustamente a aquisição sistemática de empresas americanas por empresas chinesas, a fim de obter direitos de propriedade intelectual de ponta. Além disso, os EUA afirmam que a China pratica e apoia a pirataria com o objetivo de obter acesso a informações comerciais sensíveis e segredos comerciais das empresas americanas.[479]

Em poucas palavras, as reivindicações de jurisdição facilitam o controle sobre a propriedade intelectual, o que, por sua vez, permite o controle sobre a inovação, potencialmente levando a vantagens econômicas, sociais e militares.

Os EUA também apontaram como "a China usa restrições de propriedade estrangeira, tais como requisitos de *joint venture* e limitações de capital estrangeiro, e vários processos administrativos de revisão e licenciamento, para exigir ou pressionar a transferência de tecnologia de empresas norte-americanas."[480] Preocupações semelhantes sobre o comportamento da China foram levantadas, por exemplo, na Austrália, Nova Zelândia, Japão, Canadá e na UE.[481] As preocupações sobre a aquisição agressiva da propriedade intelectual por parte da China fazem parte de um quadro mais amplo — aquele em que vários Estados lutam por vantagens através da superioridade tecnológica. A gravidade desta situação não deve ser subestimada, uma vez que o risco de escalada é óbvio. À medida que os Estados maiores

buscam a superioridade tecnológica, existe um risco óbvio de que os Estados menores e os Estados em desenvolvimento, em particular, sejam utilizados como peões neste jogo de apostas altas. Existe também o risco de que os Estados menores e em desenvolvimento possam ter sua autonomia limitada de modo a impedir que esses Estados formulem livremente suas próprias estratégias de Internet.

3.3.1.2. Direitos autorais usados para restringir o discurso com efeitos transfronteiriços

Em 18 de setembro de 2018, o Governo do Japão apresentou um projeto de relatório defendendo a legislação que permitiria que sites fossem bloqueados por oferecerem acesso a conteúdo infrator de direitos autorais.

A proposta, que surgiu depois que o governo pediu aos ISPs que bloqueassem voluntariamente sites mediante aviso prévio em abril de 2018, é controversa e tem sido descrita como contrária às salvaguardas constitucionais de liberdade de expressão.[482]

Os planos controversos do Japão para alterar as leis de direitos autorais para criminalizar o download não licenciado de todo o conteúdo protegido por direitos autorais foram abandonados em março de 2019.[483]

Este é apenas um exemplo do potencial de confrontos entre o cumprimento dos direitos de autor e a liberdade de expressão. Como um especialista entrevistado observou, existem inúmeros exemplos de leis de direitos autorais sendo usadas como ferramenta para restringir conteúdo protegido pela liberdade de expressão.

O complexo *caso Garcia* dos EUA é um exemplo explícito disso. Neste caso, uma atriz de um papel menor em um filme procurou impedir a publicação, no YouTube, de outro filme que incorporou suas cenas. Ao não conseguir a remoção do conteúdo por outros motivos, a atriz buscou, e inicialmente conseguiu, a remoção global baseada em seus supostos direitos de propriedade intelectual por sua atuação.[484] Os tribunais que trataram do caso nunca consideraram a dimensão transnacional do caso, porém, a decisão foi posteriormente anulada por motivos relacionados aos direitos autorais.

Outro exemplo com implicações potenciais de liberdade de expressão é uma proposta da FairPlay Canada para estabelecer

uma organização sem fins lucrativos que identifique sites que se envolvam em pirataria de direitos autorais e exija que os ISPs bloqueiem o acesso a esses sites. A Comissão Canadense de Rádio, Televisão e Telecomunicações rejeitou a proposta em outubro de 2018.[485] Como alguns especialistas entrevistados ressaltaram, a lei de direitos autorais não é globalmente uniforme. Assim, quando a lei de direitos autorais é usada como base para a remoção de conteúdos globalmente, o conteúdo legal em alguns países pode ser removido onde a remoção não é permitida por lei.

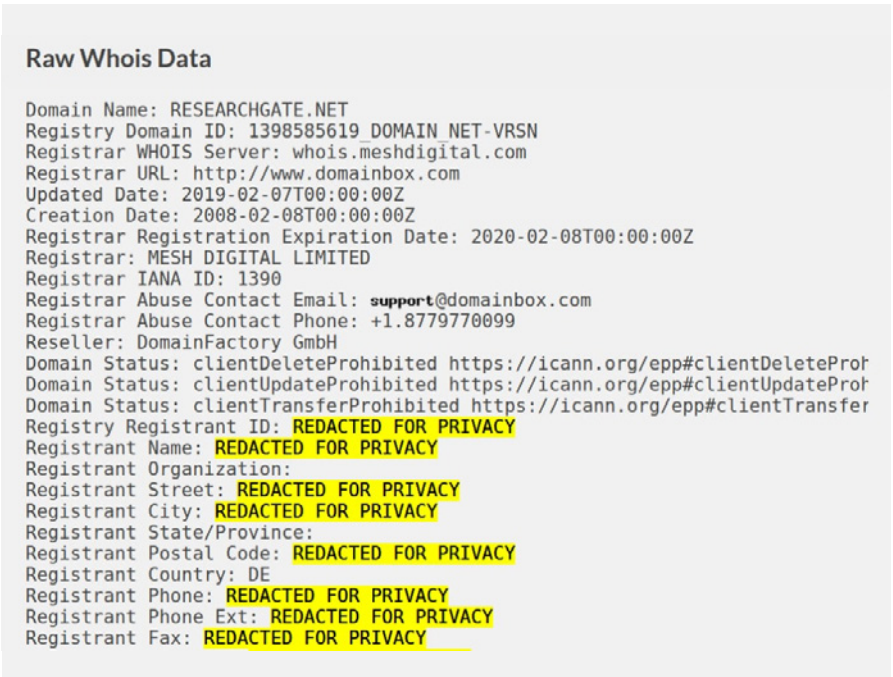
Alguns especialistas entrevistados descreveram as controversas revisões da Diretiva de Direitos de Autor da UE como conferindo poder expandido aos detentores de direitos de autor, o que poderia ser abusado para limitar a liberdade de expressão. Neste contexto, podem ser assinalados os impactos das medidas de filtragem constantes do artigo 13 do projeto de Diretiva de Direitos de Autor da UE de 2018. Outro exemplo é encontrado no Regulamento de Comunicações Eletrônicas e Postais (Conteúdo Online) 2018 da Tanzânia, que regula o conteúdo publicado online com acusações por não remover conteúdo e impõe multas para blogueiros e mídia online. Alguns especialistas entrevistados também disseram que a lei de direitos autorais poderia ser usada para suprimir o desenvolvimento tecnológico e a liberdade de associação.

3.3.1.3. Evolução do WHOIS e seu uso por associações policiais e de direitos autorais

O sistema WHOIS — supervisionado pela Corporação da Internet para Atribuição de Nomes e Números (ICANN) — permite que os usuários identifiquem o proprietário registrado de qualquer domínio. Como tal, tem sido uma ferramenta valiosa para uma vasta gama de atores, incluindo associações de execução da lei e de direitos de autor – e, infelizmente, golpistas e spammers.

Mas as informações disponíveis no sistema WHOIS mudaram recentemente devido aos requisitos descritos no GDPR da UE, com os registradores ocultando informações pessoais através de seu sistema automatizado.

FIGURA 1
PESQUISA WHOIS DO DOMÍNIO RESEARCHGATE.NET EM JANEIRO DE 2019



Raw Whois Data

```
Domain Name: RESEARCHGATE.NET
Registry Domain ID: 1398585619_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.meshdigital.com
Registrar URL: http://www.domainbox.com
Updated Date: 2019-02-07T00:00:00Z
Creation Date: 2008-02-08T00:00:00Z
Registrar Registration Expiration Date: 2020-02-08T00:00:00Z
Registrar: MESH DIGITAL LIMITED
Registrar IANA ID: 1390
Registrar Abuse Contact Email: support@domainbox.com
Registrar Abuse Contact Phone: +1.8779770099
Reseller: DomainFactory GmbH
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProh
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProh
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransfer
Registry Registrant ID: REDACTED FOR PRIVACY
Registrant Name: REDACTED FOR PRIVACY
Registrant Organization:
Registrant Street: REDACTED FOR PRIVACY
Registrant City: REDACTED FOR PRIVACY
Registrant State/Province:
Registrant Postal Code: REDACTED FOR PRIVACY
Registrant Country: DE
Registrant Phone: REDACTED FOR PRIVACY
Registrant Phone Ext: REDACTED FOR PRIVACY
Registrant Fax: REDACTED FOR PRIVACY
```

Tal fato terá impacto na aplicação dos direitos de propriedade intelectual, nomeadamente nos casos em que um titular de direitos procura tomar medidas contra sites que oferecem conteúdos ou mercadorias ilícitas. No entanto, também foi sugerido que o sistema WHOIS é de uso limitado na busca de violações de direitos autorais. Isso se deve, em parte, ao fato não só de que grande parte da informação no sistema é imprecisa, mas também porque a ferramenta IP WHOIS, que mostra quem possui ou controla um endereço IP específico, geralmente é mais útil para essa tarefa.

Esta situação põe em evidência a interpenetração dos três campos de enfoque neste Relatório: expressão, economia e segurança.

Aqui, uma decisão sobre privacidade de dados (expressão) em uma região tem consequências inesperadas tanto para a economia como para a segurança em escala global. Este é um lembrete útil da necessidade de coordenação, cooperação e redação jurídica cuidadosa.

3.3.2. Comércio eletrônico, direito concorrencial, restrições de comercialização e defesa do consumidor

O comércio eletrônico (e-commerce) assume diferentes formas, com uma distinção clássica entre transações entre empresas (B2B), transações entre empresas e consumidores (B2C) e transações entre consumidores (C2C). Há uma tendência emergente de reguladores e legisladores adotarem atitudes mais duras em relação às plataformas de Internet quando se trata de proteção do consumidor. Há também indícios de que escolha das empresas de Internet quanto ao foro e cláusulas legais a serem impostas aos seus usuários não estão sendo cumpridas. Em conjunto, estas duas tendências podem ter um impacto significativo nos próximos anos.

Um tema subjacente e recorrente no comércio eletrônico transfronteiriço é a necessidade de equilibrar a previsibilidade e a flexibilidade. A previsibilidade – por exemplo, na forma de leis aplicáveis e no âmbito geográfico da jurisdição – é necessária para que as empresas se envolvam com confiança no comércio eletrônico.

Isto é particularmente verdadeiro, dado que o comércio eletrônico é caracterizado por mercados globais e leis locais.

> **Há também indícios de que escolha das empresas de Internet quanto ao foro e cláusulas legais a serem impostas aos seus usuários não estão sendo cumpridas.**

Ao mesmo tempo, as partes que normalmente efetuam transações a partir de uma posição relativamente mais fraca, como é o caso dos consumidores, podem exigir um elevado grau de flexibilidade para que a lei tenha em conta os seus interesses, em detrimento das previsíveis escolhas de cláusulas judiciais e de direito por parte das empresas. Em alguns sistemas jurídicos, os consumidores podem invocar a lei e a jurisdição do seu país de origem nas suas relações transfronteiriças com as empresas, desde que sejam respeitados determinados critérios.[486]

No entanto, este grau de proteção dos consumidores continua sendo raro, embora as leis de proteção aos consumidores sejam relativamente comuns. Um estudo da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD)

mostrou que 97 dos 125 países para os quais era possível acessar dados haviam adotado legislação de proteção ao consumidor relacionada ao comércio eletrônico.[487] Destes, 61 foram classificados como economias em desenvolvimento ou em transição. No entanto, o mesmo estudo mostrou que não era possível obter dados para mais 67 países, significando que a proteção dos consumidores on-line nesses países não está sendo plenamente considerada. A incidência das leis de defesa do consumidor mostrou-se particularmente baixa na África.

A Rede Internacional de Controle e Proteção dos Consumidores publicou uma carta aberta às empresas da economia digital sobre a importância da normalização de termos e condições para os consumidores.[488]

3.3.2.1. Atitude mais rígida em relação às plataformas da Internet no campo do comércio eletrônico e da concorrência

Como a maioria das plataformas da Internet está baseada nos EUA, qualquer ação contra essas plataformas em outras partes do mundo dá origem a considerações jurisdicionais potencialmente complexas. É importante ressaltar que as principais plataformas da Internet adotaram diferentes estruturas societárias, o que significa que os fundamentos jurisdicionais que podem ser invocados em um cenário podem não ser suficientes para estabelecer jurisdição em outro cenário. Os pontos de ancoragem jurisdicional disponíveis também variam em função da área do direito material em questão. Durante muito tempo, as discussões sobre a regulação das plataformas digitais foram predominantemente preocupadas com a garantia de que esses atores fossem dotados de proteção suficiente para alcançar seu potencial e florescer. Hoje, há sinais claros de que a atitude em relação às plataformas de Internet está endurecendo, tanto nos países industrializados quanto nos países em desenvolvimento. No contexto das restrições de comercialização e da defesa do consumidor, por exemplo, tal atitude é claramente visível na pesquisa da Comissão Australiana para Concorrência e Consumidor (ACCC, na sigla em inglês) sobre plataformas digitais.[489]

Outro exemplo é a Diretiva de Direitos Autorais da UE de 2018, que impõe maiores responsabilidades em determinadas plataformas digitais para impedir que os usuários publiquem conteúdo protegido por direitos autorais. Além disso, a Coa-

lização Dinâmica sobre Responsabilidade de Plataforma do Fórum de Governança da Internet da ONU está trabalhando para produzir modelos de cláusulas contratuais para plataformas da Internet, com o objetivo final de proteger os direitos humanos dos usuários e aumentar a responsabilidade da plataforma.[490]

Outro exemplo dessa atitude endurecedora foi destacado em 1º de agosto de 2017, quando o vice-ministro de Transportes e Comunicações da Tanzânia afirmou que o país deveria "se proteger contra o mau uso" de plataformas como Facebook, Twitter e Instagram, "para garantir que, enquanto uma pessoa é livre para dizer qualquer coisa, há mecanismos para responsabilizá-la pelo que diz".[491] Em sua declaração, o ministro contrastou a ideia americana de liberdade de expressão on-line ilimitada com a forma como a China regulou a Internet, o que inclui bloquear as plataformas de mídia social americanas e "substituí-las por sites desenvolvidos internamente que são seguros, construtivos e populares".[492] Outra iniciativa governamental é a emissão pelo governo francês de um relatório de missão interina, em maio de 2019, sobre a criação de uma estrutura francesa para tornar as plataformas de mídia social mais responsáveis.[493]

Outro exemplo pode ser visto na ação judicial de dezembro de 2018 movida pelo Procurador Geral dos EUA contra o Facebook por não proteger os dados pessoais de seus clientes e por permitir que a empresa de dados políticos Cambridge Analytica acessasse os dados pessoais dos usuários.[494] Em julho de 2019, a Comissão Federal de Comércio dos EUA (FTC) impôs uma multa de US$ 5 bilhões ao Facebook por violar a privacidade dos consumidores.[495] Medidas reguladoras contra o Facebook pela violação de dados da Cambridge Analytica foram tomadas por outros países, incluindo Itália[496] e Canadá.[497] Uma atitude mais dura em relação aos intermediários da Internet também pode ser vista no campo do direito concorrencial. Por exemplo, em 18 de julho de 2018, a Comissão Europeia anunciou que havia multado o Google em 4,3 bilhões de Euros por violar as leis antitruste da UE, argumentando que a empresa tinha abusado de sua dominância no mercado Android.[498] Além disso, em março de 2019, a Comissão Europeia multou o Google em 1,49 bilhões de Euros por práticas abusivas em publicidade on-line.[499] Fica claro que se pode esperar mais avanços na UE.

Por exemplo, em setembro de 2019, noticiou-se que a Comissária Europeia para Concorrência, Margrethe Vestager, viu razões para "introduzir regras para abranger especificamente as empresas tecnológicas e a sua utilização de dados".[500]

Em fevereiro de 2019, o escritório antitruste da Alemanha decidiu que o Facebook está abusando de seu monopólio virtual nas mídias sociais, combinando dados do Instagram, WhatsApp e sites de terceiros.[501] Outro exemplo de uma abordagem mais rigorosa neste contexto é o anúncio de dezembro de 2018 que "a Índia vai proibir empresas de comércio eletrônico [...] de vender produtos de empresas nas quais elas têm participação acionária".[502]

A Índia publicou um Projeto de Política Nacional de Comércio Eletrônico em fevereiro de 2019, solicitando maior proteção dos direitos dos consumidores e localização dos dados.[503]

Nos EUA, as iniciativas antitruste voltadas para a indústria de tecnologia estão sendo realizadas tanto em nível federal,[504] quanto em nível estadual.[505] Em julho de 2019, a Autoridade de Concorrência e Mercados do Reino Unido estaria alegadamente investigando o domínio do Facebook e do Google sobre o mercado de publicidade no Reino Unido.[506]

Há também medidas para a criação de organismos reguladores específicos. Por exemplo, o governo japonês teria planos de criar um órgão regulador para examinar as práticas competitivas das principais plataformas de mídia social e fazer recomendações antitruste.[507] A Câmara dos Lordes do Reino Unido publicou um relatório "Regulating in a Digital World" recomendando a criação de uma Autoridade Digital para coordenar os reguladores existentes.[508] Além disso, a Comissão Federal de Comércio dos EUA anunciou em 2019 o lançamento de uma força-tarefa para monitorar os mercados de tecnologia.[509]

Em dezembro de 2017, a OCDE realizou uma mesa-redonda sobre o alcance extraterritorial das soluções de concorrência.[510]

3.3.2.2. Indústrias com regulações específicas

Certos produtos, bem como certos setores, estão sujeitos a regulamentações, restrições ou proibições específicas. A venda de armas, álcool, narcóticos, produtos farmacêuticos e produtos químicos perigosos são exemplos disso. A prestação de serviços de jogos de azar é outra área associada à regulação específica.[511]

Esta situação suscita problemas específicos no ambiente on-line, dada a facilidade com que os produtos são comprados e vendidos além-fronteiras.

Em particular, a regulamentação das farmácias on-line obteve um considerável grau de atenção nos últimos anos. Os Princípios de Bruxelas sobre a Venda de Medicamentos pela Internet[512] chamam a atenção para as numerosas considerações políticas contraditórias que estão em jogo, por exemplo:

1. A Organização Mundial da Saúde (OMS) estima que mais de dois bilhões de pessoas não têm acesso regular a produtos médicos essenciais;
2. As grandes preocupações de saúde pública surgem quando o controle da qualidade não pode ser assegurado;
3. Os atores em questão incluem farmácias on-line legítimas e operadores desonestos; e
4. A concorrência transfronteiriça pode beneficiar a disponibilidade e preços mais baixos.

Neste cenário, a coordenação e a cooperação internacionais são uma necessidade.

3.3.2.3. Não cumprimento de cláusulas relativas à escolha do foro e à escolha da lei aplicável

Estudos têm salientado repetidamente que os consumidores raramente leem os termos e condições com os quais, indiscutivelmente, "concordam" — por exemplo, clicando em "Concordo" (contratos digitais, denominados "click-wrap") ou simplesmente utilizando um site da Internet (denominados "browse-wrap agreements"). Alguns referiram este fato ao questionarem a validade das cláusulas de eleição do foro (que determinam onde as partes podem mover ações judiciais) e das cláusulas de escolha da lei aplicável (que determinam a lei do país que regerá os litígios entre as partes) incluídas em tais acordos. Esta questão também se coloca em relação às cláusulas que nomeiam a arbitragem como um processo obrigatório de resolução de litígios, especialmente nos contratos de consumo.[513]

Na decisão da Suprema Corte do Canadá, de junho de 2017, no processo *Douez v. Facebook, Inc.*,[514] a maioria (4-3) do Tribunal considerou a cláusula de eleição de foro do Facebook (que nomeou um tribunal da Califórnia) inexequível. O assunto surgiu de um caso de privacidade de dados trazido por um residente

da Colúmbia Britânica contra o Facebook. O Facebook argumentou que as disputas relativas aos seus termos de uso devem ser resolvidas na Califórnia, mas a Suprema Corte decidiu o contrário, argumentando que seria mais conveniente ter livros e registros do Facebook disponibilizados para inspeção na Colúmbia Britânica, em vez de exigir que o réu viaje para a Califórnia para protocolar sua reivindicação.[515]

Em 2016, o TJUE foi convidado a determinar se a cláusula sobre o direito aplicável da Amazon EU era injusta à luz do direito do consumidor da UE.[516] O advogado-geral Saugmandsgaard Øe concluiu que a cláusula de escolha de lei da Amazon EU não pode prevalecer sobre a opção de litígio ao abrigo do direito do país de origem do consumidor, conforme criado pelo Regulamento Roma I. A cláusula não pode, por conseguinte, ser considerada como excluindo injustamente o consumidor do exercício desta opção. No entanto, a cláusula utilizada pela Amazon EU pode induzir os consumidores a acreditar que não têm o direito ao abrigo do Regulamento Roma I e este potencial de induzir a erro torna o termo injusto ao abrigo do direito comunitário aplicável em matéria de defesa do consumidor. Este raciocínio foi igualmente adotado pelo Tribunal.[517] Importa salientar que o mesmo raciocínio pode ser aplicado a qualquer cláusula de um contrato do consumidor, quando essa expressão não reflete adequadamente as disposições do direito obrigatório.

Resta saber se estes desenvolvimentos são indicativos de uma tendência contra a manutenção de cláusulas de escolha do foro e de escolha da lei aplicável nos acordos on-line, ou se a adesão à denominada "autonomia partidária", que, em última análise, apresenta aos usuários condições contratuais com bases unilateralmente predeterminadas — será reafirmado. No que diz respeito à UE, foi possível obter alguma clareza num caso relativo ao estatuto dos acordos através de uma caixa de verificação prévia, que os usuários devem "desmarcar" para recusar o consentimento.[518]

O advogado-geral Szpunar, do TJUE, manifestou, em março de 2019, que essas caixas pré-assinaladas não contam como consentimento válido.[519] Em 1º de outubro de 2019, o TJUE decidiu que: "o consentimento referido nessas disposições [Artigo 2 (f) e Artigo 5(3) da Diretiva 2002/58/CE do Parlamento e do Conselho Europeu, de 12 de julho de 2002, relativa ao tratamento

de dados pessoais e à proteção da privacidade no setor das comunicações eletrônicas] não é validamente constituído se, sob a forma de cookies, o armazenamento de informações ou o acesso a informações já armazenadas no terminal de um usuário do site for permitido através de uma caixa pré-assinalada que o usuário deve desmarcar para recusar o seu consentimento."[520]

A autoridade de proteção de dados francesa (CNIL) também emitiu novas Diretrizes sobre Cookies e Dispositivos de Rastreamento para ser consistente com o requisito de consentimento válido nos termos do GDPR.[521]

Tal como observado por um especialista consultado, a complexidade aumenta pelo fato de não existir uma definição universal sobre quem é o "consumidor".

3.3.3. Tributação — a interseção entre as complexidades jurisdicionais e a economia nacional

Vários especialistas consultados e entrevistados apontaram para a tributação como uma área em desenvolvimento particularmente significativo para os próximos anos e que merece especial atenção numa perspectiva transfronteiriça. Complicações jurisdicionais surgem, por exemplo, devido à presença de múltiplos pontos de ancoragem que podem ser potencialmente utilizados para fins tributários; a tributação pode ser baseada na localização dos usuários, escritórios (filiais), sedes, servidores, etc. Dá-se uma atenção crescente à tributação das principais plataformas da Internet, em particular. São igualmente tomadas medidas para assegurar a cobrança efetiva dos impostos on-line.[522] A tributação é também uma área em que vemos uma tendência emergente de uma maior cooperação internacional. Por exemplo, em julho de 2018, foi anunciada a criação do Joint Chiefs of Global Tax Enforcement (conhecido como J5).[523]

Composto por autoridades da Austrália, Canadá, Países Baixos, Reino Unido e EUA, o J5 visa a combater o crime fiscal transnacional através de uma maior colaboração entre autoridades. Entre outras áreas, seu trabalho se concentrará em identificar crimes cibernéticos como uma estratégia de evasão fiscal e nas criptomoedas da Darknet. Este fato chama a atenção para a relação entre os trabalhos relacionados à tributação, por um lado, e a investigação e repressão aos crimes cibernéticos - incluindo o confisco de bens -, por outro

lado.[524] As questões jurisdicionais constituem preocupações fundamentais neste contexto.

A questão subjacente é que, à medida que mais transações ocorrem on-line, tributar o comércio tradicional não gerará tanta receita como antes. Se um governo deseja manter seus níveis de receita, ele deve aumentar o imposto sobre transações off-line ou tributar atividades comerciais on-line.

Muito está em jogo e o debate sobre a tributação do comércio eletrônico desencadeou discussões com vista a uma reforma global do sistema fiscal internacional.

Alguns argumentaram contra estes pontos, afirmando que a tributação retarda o desenvolvimento da Internet em geral, e o comércio eletrônico em particular. Tendo em conta a natureza complexa do sistema fiscal internacional, existe um risco óbvio de que os comerciantes inexperientes não cumpram a lei devido ao desconhecimento. Embora o desconhecimento da lei não seja uma defesa, como tal, alguma forma de avaliação da razoabilidade pode ser apropriada. Também foi sugerido que o ritmo lento da evolução fiscal não pode acompanhar o rápido desenvolvimento da tecnologia, o que pode conduzir a resultados indesejáveis.

3.3.3.1. A tributação dos dados e a procura de uma nova base fiscal

Como observou a OCDE, as estruturas fiscais internacionais em funcionamento hoje foram projetadas há mais de um século.[525] Modernização, incluindo a busca de uma nova base de tributação é, portanto, um desenvolvimento natural destinado a abordar a erosão de base e a mudança de lucro (BEPS, do termo em inglês *base erosion and profit shifting*). Em fevereiro de 2019, a OCDE divulgou um Documento de Consulta Pública: Enfrentando os desafios fiscais da digitalização da Economia.[526]

A ideia de tributar os dados não é nova e, tendo em conta as dificuldades na aplicação de regimes fiscais tradicionais ao comércio eletrônico e a outras atividades on-line, vários novos regimes fiscais foram sugeridos. Todos esses regimes procuram tributar a tecnologia por trás das transações.

Sugestões mais recentes incluem tributação baseada no volume de negócios, tributação baseada na oferta de serviços, tributação baseada na localização e tributação baseada na segmentação, incorporação ou usuários atendidos.

Uma das propostas recentes mais debatidas é a atual proposta da Comissão Europeia de um imposto sobre os serviços digitais (DST, do termo em inglês *digital services tax*).[527] A incapacidade desta iniciativa em obter um apoio suficientemente amplo levou os Estados-membros da UE, como a França, a prosseguirem com suas próprias iniciativas de reforma fiscal.[528] A iniciativa fiscal da França tem sido criticada por empresas de tecnologia norte-americanas que alertam para o aumento dos preços e danos à economia digital.[529] A Lei Multinacional Contra a Evasão Fiscal (MAAL, na sigla em inglês) da Austrália, que entrou em vigor em 11 de dezembro de 2015, é outro exemplo de uma recente iniciativa de reforma tributária voltada para o setor de tecnologia.[530] Exemplos de desenvolvimentos neste domínio podem ser encontrados em todo o mundo.

Por exemplo, em 9 de setembro de 2019, foi noticiado que o México está considerando ampliar um imposto sobre vendas para empresas on-line estrangeiras.[531] Uganda, em uma abordagem única, optou por testar um método que tributa o uso de plataformas de mídias sociais, como Facebook, Skype, Twitter e WhatsApp por seus cidadãos.[532] Nos Camarões, a Lei de Finanças de 2019 impõe um imposto sobre downloads de software e aplicativos produzidos fora do país.[533] Além disso, vários Estados da Ásia — incluindo Indonésia,[534] Singapura,[535] Tailândia,[536] Vietnã,[537] e Malásia[538] — estão trabalhando na implementação de iniciativas fiscais de comércio eletrônico.

Em junho de 2019 os Ministros das Finanças do G20 concordaram em desenvolver regras para eliminar as lacunas empregadas pelas empresas globais de tecnologia para reduzir os tributos.[539]

3.3.3.2. Tributação e localização dos dados

Existem, pelo menos, dois pontos de ligação entre tributação e localização dos dados. Em primeiro lugar, a tributação pode ser uma força motriz para a localização dos dados (ver mais: Capítulo 4.2.7) nos casos em que a tributação se baseia na localização dos dados, ou seja, as empresas podem optar por localizar os seus centros de dados em locais específicos para obter vantagens fiscais.

Em segundo lugar, a tributação pode ser uma força motriz para a localização dos dados nos casos em que a legislação fiscal dos países exige que determinados registros fiscais e contabi-

lísticos sejam mantidos nas instalações da empresa. Algumas dessas leis são recentes. Em abril de 2018, por exemplo, o Banco Central da Índia divulgou uma diretiva que obrigava todas as entidades a armazenar dados de sistemas de pagamentos relacionados a transações de usuários somente dentro dos limites nacionais da Índia.[540]

O objetivo anunciado consistia em assegurar melhor acompanhamento e acesso livre e permanente aos dados armazenados junto dos prestadores de sistemas de pagamento. Tais leis, no entanto, são anteriores ao uso generalizado da computação em nuvem e podem, de fato, ser anteriores ao uso generalizado da Internet. No entanto, continua a ser um fato que as restrições ao acesso aos sistemas e aos dados de pagamento podem ser utilizadas como instrumentos de política externa.

3.3.4. Internet das Coisas (IoT) — tudo transferindo dados em todos os lugares

O conceito de Internet das Coisas (IoT, do inglês *Internet of Things*) refere-se a situações em que a conectividade à Internet é estendida além de dispositivos tradicionais em rede (como computadores e smartphones) até objetos físicos, anteriormente desconectados (como refrigeradores, lâmpadas e carros). Embora muitos aspectos da IoT continuem cristalizados, não há dúvida de que a revolução da IoT causará um aumento maciço nos fluxos transfronteiriços de dados pessoais e não pessoais, incluindo fluxos de dados máquina-a-máquina (M2M).

Especialistas entrevistados fizeram uma série de observações interessantes em relação à IoT. Por exemplo, um especialista entrevistado apontou para os benefícios para a execução da lei de poder rastrear veículos, mesmo quando estes atravessam fronteiras. Outro observou que a IoT pode facilitar a imputação em investigações criminais. No entanto, o mesmo especialista entrevistado também observou que, se os dados gerados pela IoT forem armazenados em nuvem — o que é comumente o caso — isso levará a um volume ainda maior de solicitações de dados por parte das autoridades de execução da lei.

Alguns especialistas entrevistados observaram que a IoT está fazendo com que as empresas de Internet orientadas por dados se expandam para mercados que anteriormente não eram digitais. Os sistemas de fabricação de automóveis e de abastecimento de

água são dois exemplos desta tendência. Esta fusão das esferas off-line e on-line expande o papel dos dados — incluindo os fluxos de dados transfronteiriços — e, como observou um especialista entrevistado, dará origem a problemas jurídicos transfronteiriços.

A IoT tem registrado um rápido progresso e muitos dos seus aspectos já estão em funcionamento. Por exemplo, a McKinsey estima que 127 novos dispositivos estejam se conectando à Internet a cada segundo.[541] No entanto, a IoT ainda enfrenta vários desafios e a comunidade empresarial parece estar mal preparada. Um estudo da PwC de 2018, Global State of Information Security Survey, mostrou que apenas 34% de seus especialistas pesquisados "dizem que suas organizações planejam avaliar os riscos de segurança da Internet das Coisas (IoT) em todo o ecossistema de negócios."[542]

Alguns dos principais desafios que a IoT enfrenta incluem:

- preocupações em matéria de segurança e privacidade;
- falta de normas técnicas;
- problemas de segurança dos produtos;
- preocupações sobre a largura de banda inadequada;
- preocupações em matéria de sustentabilidade ambiental;
- questões de controle, responsabilidade e responsabilização
- preocupações sobre a propriedade dos dados; e
- limitações de interoperabilidade.

Várias destas preocupações salientam a necessidade de cooperação e coordenação transfronteiriças.

Além disso, como o desenvolvimento da IoT depende de redes móveis mais rápidas, a velocidade com que as redes 5G ficam disponíveis é de grande importância e pode, de fato, definir o ritmo para absorção da IoT. Nisto, encontramos uma convergência de várias das principais tendências atuais discutidas no Capítulo 3. O conflito comercial EUA-China, envolvendo tanto o protecionismo digital (Capítulo 3.3.6.1) quanto a aquisição transfronteiriça agressiva de propriedade intelectual (Capítulo 3.3.1.1), centrou-se em parte nas práticas comerciais da gigante tecnológica chinesa Huawei.

Isso, juntamente com as preocupações de segurança cibernética (Capítulo 3.2.4) sobre os produtos da Huawei levaram alguns países a proibir os produtos da empresa, o que poderá atrasar a implantação do 5G, que é um elemento necessário para a adoção generalizada da IoT.

Esta complexa matriz de interesses e preocupações transfronteiriços põe em evidência a interligação das questões discutidas no presente capítulo.

Chama igualmente a atenção para a tensão entre, por um lado, a rápida implantação tecnológica e, por outro, a ponderação cuidadosa das implicações de cibersegurança.

Algumas iniciativas e desenvolvimentos notáveis na esfera da IoT incluem as seguintes:

Em **setembro de 2019**, a **Internet Society** publicou um policy brief sobre privacidade e Internet das Coisas.[543]

Em resposta ao apelo dos atores envolvidos na **Rede de Políticas Internet & Jurisdição**, um workshop de um dia sobre a Internet das Coisas foi organizado em Berlim, Alemanha, em **abril de 2019**. A reunião teve por objetivo ajudar a enquadrar e promover um entendimento comum dos desafios jurídicos transfronteiriços no que diz respeito à Internet das Coisas, explorar a necessidade e os benefícios da coordenação e cooperação entre os vários atores e explorar potenciais vias para desenvolver soluções operacionais e normas políticas para enfrentar os novos desafios jurídicos transfronteiriços no âmbito da Internet das Coisas, Inteligência Artificial e a Quarta Revolução Industrial.

A **Comissão Federal de Comércio dos EUA** (FTC) emitiu um relatório da equipe da FTC sobre privacidade na IoT intitulado Internet das Coisas: Privacidade e Segurança em um Mundo Conectado.[544]

Em **fevereiro de 2018**, a **Siemens** começou a trabalhar com parceiros da indústria, governo e sociedade para assinar uma "Carta de Confiança" visando três objetivos: (1) Proteger os dados de pessoas e empresas; (2) Prevenir danos a pessoas, empresas e infraestruturas; e (3) Estabelecer uma base confiável sobre a qual a confiança num mundo digital em rede possa criar raízes e crescer.[545]

Em **2017**, o **Grupo Banco Mundial** publicou um Relatório intitulado Internet das Coisas: a nova plataforma governo-empresas - uma revisão das oportunidades, práticas e desafios.[546]

A **Coalizão Dinâmica do Fórum de Governança da Internet (IGF) sobre a Internet das Coisas** está buscando alcançar as melhores práticas em relação à IoT, particularmente abordando a segurança pessoal, segurança patrimonial e privacidade.[547]

Em **2017**, a **Google Cloud** anunciou a disponibilidade global de seu serviço IoT Core.[548]

Num exemplo de cooperação transfronteiriça na Internet no domínio da Internet das coisas, em **2016**, um grupo de grandes fornecedores de telecomunicações formou a **Aliança Mundial da Internet das Coisas**.[549]

3.3.4.1. Casas inteligentes conectadas em cidades inteligentes conectadas

Muito se pode ganhar com o desenvolvimento das chamadas cidades inteligentes, incluindo redes inteligentes de energia e água. Maior eficiência, por exemplo, pode gerar economia de custos e proporcionar benefícios ambientais. Avanços como carros autônomos podem reduzir custos, ajudar a salvar o ambiente e minimizar acidentes.

As casas inteligentes equipadas com termostatos inteligentes, aparelhos inteligentes e dispositivos de aquecimento, iluminação e eletrônicos ligados podem ser controlados remotamente através de computadores, smartphones ou outros dispositivos móveis. Isso pode minimizar os custos, ao mesmo tempo em que oferece conveniência e vantagens ambientais.

Dispositivos vestíveis conectados com sensores podem coletar, analisar e comunicar dados do usuário para fornecer vários benefícios ao usuário e também podem ser usados para aumentar a segurança pública.

> **Como qualquer aumento nos contatos internacionais vem com um provável aumento nas disputas internacionais, a mudança para casas inteligentes e cidades inteligentes provavelmente criará outras pressões sobre os mecanismos internacionais de resolução de litígios e poderá até desencadear a criação de novos pontos de ancoragem jurisdicionais.**

Com a Internet sendo uma rede global, essa interconectividade cria ligações diretas entre casas e cidades em diferentes países e com provedores que podem estar baseados em qualquer lugar do mundo. Como qualquer aumento nos contatos internacionais vem com um provável aumento nas disputas internacionais, a mudança para casas inteligentes e cidades inteligentes provavelmente criará outras pressões sobre os mecanismos internacionais de resolução de litígios e poderá até desencadear a criação de novos pontos de ancoragem jurisdicionais.

Alguns especialistas entrevistados observaram que, à medida que as empresas de tecnologia migram para novas indústrias, como a fabricação de automóveis, sistemas de mobilidade e gestão de abastecimento de água, elas entram em um ambiente caracterizado por um nível muito maior de regulação e diferentes considerações de segurança e proteção.

3.3.4.2. Saúde on-line vestível

A tecnologia vestível, como os relógios inteligentes, pode registrar com precisão uma ampla gama de dados sensíveis de saúde. Dados importantes do usuário são normalmente armazenados em soluções de computação em nuvem. Consequentemente, as transferências transfronteiriças de dados são comuns e podem surgir questões jurisdicionais em caso de vazamentos de dados, como as reportadas em relação ao Fitbit em janeiro de 2016[550], PumpUp em junho de 2018[551] e a Garmin em outubro de 2018.[552]

No contexto tanto das cidades inteligentes quanto das questões mais pessoais aqui debatidas, deve ser dada especial atenção ao respeito dos direitos à privacidade dos dados, à garantia da cibersegurança e à não asfixia da inovação.

Uma vez que os fornecedores e usuários de dispositivos inteligentes não estão frequentemente estabelecidos no mesmo país, é evidente a necessidade de coordenação e cooperação internacionais.

3.3.5. Blockchain — ainda uma solução à procura de um problema?

Desde a publicação do livro branco original de Satoshi Nakamoto em 2008,[553] a tecnologia de blockchain capturou a imaginação do mundo e é amplamente discutida na literatura acadêmica, em documentos de política e na mídia. Até o momento, no entanto, poucas questões jurisdicionais foram destacadas e o tópico da tecnologia de blockchain atraiu atenção limitada durante as entrevistas para este Relatório.

Em termos básicos, a tecnologia de blockchain pode ser descrita como uma planilha distribuída global ou como um "livro público confiável" — ou, de fato, como preferido por alguns, um "livro público sem confiança". O objetivo de remover o 'intermediário' tem sido uma força motriz central por trás da tecnologia de blockchain.

A principal razão para o bitcoin, por exemplo, como descrito no livro branco original de Nakamoto, foi a necessidade de um sistema de pagamento eletrônico que permitisse duas partes dispostas a negociar diretamente uma com a outra, sem a necessidade de um terceiro confiável. No *blockchain*, a prova criptográfica remove a necessidade de confiança.

Devido à forte absorção da Bitcoin, a tecnologia blockchain é por vezes descrita como análoga à bitcoin. Mas a bitcoin é ape-

nas uma das muitas criptomoedas, e as criptomoedas são apenas um dos muitos usos da tecnologia blockchain. Os chamados contratos inteligentes (discutidos abaixo) são outro exemplo de um uso comumente discutido da tecnologia blockchain e também existem blockchains públicas e privadas.

Na verdade, o potencial do blockchain é tal que uma equipe de desenvolvedores em 2014 anunciou planos para uma rede ponta-a-ponta (*peer-to-peer*), que funcionaria sem servidores centralizados.[554] Semelhante à rede TOR, ou o princípio de mineração por trás do bitcoin, computadores individuais serviriam como nós que encaminhariam o tráfego de rede em uma maneira descentralizada e criptografada sem ISPs.[555]

A infraestrutura seria financiada através de micro-pagamentos em relação ao tráfego gerido por nós individuais. Uma empresa escocesa afirma já ter desenvolvido uma rede semelhante chamada MaidSafe.[556]

Em 2018, os Tribunais do Dubai International Financial Centre (DIFC), juntamente com a Smart Dubai, começaram a trabalhar para criar o primeiro tribunal mundial habilitado para blockchain, incluindo um esquema habilitado com blockchain para a verificação de sentenças judiciais monetárias que podem ser executadas além das fronteiras.[557] Em setembro de 2018, o Supremo Tribunal Popular da China (SPC) emitiu uma interpretação judicial sobre audiências de casos por tribunais da Internet. A interpretação judicial deixou claro que as evidências autenticadas e apresentadas usando a tecnologia blockchain são vinculativas em disputas legais ouvidas pelos três tribunais de Internet em Hangzhou, Pequim e Guangzhou.[558] Apesar da rápida absorção e enorme interesse, criptomoedas e tecnologia blockchain em geral enfrentam vários desafios técnicos e econômicos. A escalabilidade é muitas vezes citada como um desafio, no entanto, também pode ser uma vantagem, pois quanto maior o número de usuários, maior a segurança do blockchain. Problemas de privacidade de dados também são frequentemente levantados.[559] Por exemplo, embora as soluções para esta questão possam evoluir, há um conflito fundamental entre o direito de alterar dados pessoais incorretos comumente encontrados nas leis de privacidade de dados e a natureza "imutável" do blockchain.

Esta natureza imutável é exemplificada pelo fato de que cada transação bitcoin que já foi realizada é armazenada publicamen-

te, por padrão, na rede bitcoin *peer-to-peer* (P2P). E no que diz respeito às criptomoedas, a volatilidade continua a ser um problema sério. Por exemplo, em setembro de 2019, diversas moedas criptográficas populares caíram 1entre 15 e 22% em valor.[560]

Além disso, o poder de computação que o blockchain requer tem sérias implicações ambientais. Um estudo de 2018 publicado na revista *Nature Climate Change* estimou que, só em 2017, o uso de bitcoins emitiu 69 milhões de toneladas métricas de CO2.[561] Os pesquisadores por trás do estudo descobriram que "se Bitcoin for incorporado, ainda que na taxa mais lenta em que outras tecnologias foram incorporadas, suas emissões cumulativas serão suficientes para aquecer o planeta acima de 2°C em apenas 22 anos. Se incorporado à taxa média de outras tecnologias, está mais próximo de 16 anos."[562] Esta é uma ilustração interessante da interseção dos mundos on-line e off-line, com as atividades on-line em um Estado, ou um grupo de Estados, tendo efeitos extraterritoriais no ambiente off-line em outros Estados.

3.3.5.1. Criptomoedas como facilitadores do comércio e do crime transfronteiriço

Uma vez que uma criptomoeda como o Bitcoin não conhece fronteiras nacionais, ela é um facilitador óbvio do comércio transfronteiriço — tanto legal quanto ilegal.

Na verdade, o Bitcoin é frequentemente discutido no contexto da venda on-line de produtos ilegais, como armas e drogas, bem como outras atividades criminosas.

Como observado pela Avaliação da Ameaça do Crime Organizado na Internet de 2018 da Europol:

> *Relatórios anteriores indicavam que os criminosos abusam cada vez mais de criptografia para financiar atividades criminosas. Embora o Bitcoin tenha perdido a maior parte da quota de mercado global de criptomoedas, ele ainda é a principal criptomoeda encontrada pelas autoridades de execução da lei. Em uma tendência de espelhamento de ataques a bancos e seus clientes, usuários e facilitadores de criptografia tornaram-se vítimas de crimes cibernéticos. Permutadores de moedas, serviços de mineração e outros detentores de carteira es-*

tão enfrentando tentativas de hackeamento, bem como extorsão de dados pessoais e furto.
Lavadores de dinheiro evoluíram para usar criptomoedas em suas operações e são cada vez mais facilitados por novos desenvolvimentos, como trocas descentralizadas que permitem trocas sem quaisquer requisitos do tipo Conheça seu Cliente. É provável que as moedas criptográficas de alta privacidade tornem obsoletos os atuais "tumblers" e serviços de mistura.[563]

Além disso, o aspecto de mineração das criptomoedas gerou uma nova forma de cibercrime. De acordo com a Avaliação da Ameaça do Crime Organizado na Internet de 2018 da Europol, o "cryptojacking" (sequestro de criptomoedas) é uma tendência emergente de crime cibernético, em que a largura de banda e o poder de processamento dos usuários da Internet são explorados para minerar moedas criptográficas.[564]

Uma característica importante das criptomoedas é que elas criam oportunidades para transações confiáveis entre partes distantes sem a necessidade de um verificador ou autoridade de certificação de terceiros, no sentido tradicional. Através de uma combinação seleta de técnicas, o bitcoin e outras moedas criptográficas conseguiram superar a questão da 'duplicação de gastos' que afligiu tentativas anteriores de criação de moedas digitais.

De qualquer forma, está claro que o cenário da moeda criptográfica continuará a se desenvolver e mudar em muitos pequenos passos, tanto via lei[565] quanto pela via da tecnologia, mas também através de grandes saltos, como exemplificado pelo lançamento controverso e iminente da Libra[566], do Facebook.

3.3.5.2. Nenhum órgão central como ponto focal para a jurisdição?

Dada a natureza distribuída da tecnologia blockchain, argumenta-se frequentemente que não existe um organismo central que a controle. Se for esse o caso, isso tem implicações para a questão da jurisdição. Em tais situações, a falta de um órgão central de controle elimina alguns dos pontos focais frequentemente invocados para reivindicações de jurisdição como o local de constituição ou estabelecimento.

No entanto, apesar da natureza distribuída da tecnologia blockchain, a ausência de uma autoridade central não é uma necessidade.

> **A introdução de intermediários no ambiente blockchain ativa questões jurisdicionais tradicionais e pontos de conexão.**

Na verdade, para vários dos principais usos da tecnologia blockchain, é essencial que haja um órgão central com algum grau de controle. Este seria o caso em situações em que os registros de saúde de uma população são armazenados em um blockchain. Atualmente, pelo menos, parece inimaginável que a autoridade responsável pelos registros de saúde possa abdicar completamente de suas responsabilidades. É importante ressaltar que, como um especialista entrevistado observou, a introdução de intermediários no ambiente de blockchain ativa questões jurisdicionais tradicionais e pontos de conexão.

3.3.5.3. Contratos inteligentes

Enquanto as criptomoedas, e particularmente o bitcoin, atraíram a maior parte da atenção em torno dos usos de blockchain, os contratos inteligentes baseados em blockchain são cada vez mais discutidos. O termo "contrato inteligente", porém, remonta pelo menos a 1994.[567]

Um contrato inteligente é um protocolo de transação informatizado que satisfaz todos os critérios comuns para ser um contrato (por exemplo, deve ser celebrado entre duas ou mais partes) e executa os termos de um contrato para que, uma vez concluído o contrato inteligente, sua implementação não requeira qualquer envolvimento humano direto.

Não existem obstáculos à execução de tais contratos além-fronteiras. Com efeito, devido à sua natureza auto executória, os contratos inteligentes podem ser particularmente úteis nas transações transfronteiriças, uma vez que evitam quaisquer incertezas associadas à execução.

3.3.6. Questões digitais em acordos comerciais internacionais e regionais

Sendo o ambiente on-line um componente central da vida comercial, tanto nacional como internacionalmente, é natural que surjam questões digitais nas negociações comerciais internacionais. Com efeito, com o crescimento da economia digital, as questões digitais só aumentarão de importância nessas negociações. Por exemplo, o comércio transfronteiriço

de serviços que pode ser realizado on-line está a aumentar e a expandir-se para áreas que têm sido tradicionalmente consideradas como atividades nacionais. Como observou a Organização Mundial do Comércio (OMC), serviços como serviços bancários, de saúde e educação, que estavam em grande parte limitados às atividades nacionais, estão agora cada vez mais internacionalmente móveis graças aos serviços de bancos digitais, telessaúde ou tele-educação.[568] Tendo isso em conta, é natural que os acordos comerciais também abranjam questões digitais. Por exemplo, vários acordos comerciais — como a Parceria Transpacifica (TPP)[569] — exigem que as partes adotem e mantenham um quadro jurídico para transações eletrônicas compatível com os princípios da Lei Modelo da UNCITRAL sobre Comércio Eletrônico ou da Convenção das Nações Unidas sobre a Utilização de Comunicações Eletrônicas em Contratos Internacionais.[570]

Além disso, o Acordo de Parceria Econômica UE-Japão celebrado em abril de 2018 fornece regras pormenorizadas sobre o comércio eletrônico[571] e o recém-assinado Acordo entre os Estados Unidos e o México inclui um capítulo sobre o comércio digital, bem como restrições às políticas de localização de dados.[572]

Ao mesmo tempo, com a proteção de dados consagrada como um direito fundamental na UE e um direito humano fundamental implícito em grande parte do mundo, qualquer acordo comercial que implique dados pessoais suscita complexidades significativas. Em reconhecimento a isso, alguns acordos comerciais importantes reconhecem explicitamente o papel da proteção da privacidade de dados, e a OMC declarou categoricamente que "a OMC não teve nada a ver com a privacidade na Internet".[573]

O Acordo Geral sobre o Comércio de Serviços (GATS) declara explicitamente que não impede a adoção ou execução de medidas destinadas a proteger a privacidade das pessoas em relação ao tratamento e divulgação de dados pessoais e a proteger a confidencialidade dos registros e das contas individuais. No entanto, a liberdade dos membros de adotarem tais medidas está "sujeita às condições de que tais medidas não são aplicadas de forma a constituir um meio de discriminação arbitrária ou injustificável entre países em que prevalecem condições semelhantes, ou uma

restrição dissimulada ao comércio de serviços".[574] As restrições aos fluxos transfronteiriços de dados podem, por conseguinte, ser contestadas com base na afirmação de que equivalem a discriminações arbitrárias ou injustificáveis.

O impacto que os acordos comerciais terão na privacidade dos dados e noutros direitos centrais das atividades on-line continua sendo um desafio. Embora os direitos fundamentais não sejam absolutos e precisem muitas vezes ser equilibrados com outros direitos fundamentais, eles não são negociáveis. Por conseguinte, da mesma forma que os EUA não negociariam sua Primeira Emenda sobre proteção da liberdade de expressão como parte de um acordo comercial, a UE não negocia o direito à proteção dos dados.[575]

Como um especialista entrevistado salientou, a inclusão de questões de direitos humanos nas negociações comerciais levanta questões de transparência. Embora as negociações comerciais opacas possam ser defensáveis, ou mesmo naturais, no contexto das tarifas comerciais, não o são quando a matéria em negociação é a aplicação dos direitos fundamentais.

3.3.6.1. Protecionismo digital

O termo protecionismo digital é frequentemente usado para descrever quaisquer atividades destinadas a controlar a Internet (e no contexto do comércio, a economia da Internet) dentro das fronteiras do Estado — tipicamente com o efeito de impor restrições aos estrangeiros que entram no mercado. Isso pode ser feito de várias maneiras e sob uma gama de pretextos.

Tanto na literatura como entre os especialistas entrevistados, foi sugerido que o GDPR da UE foi introduzido, pelo menos em parte, como medida protecionista. Se a UE quisesse evitar que o GDPR aparecesse como protecionista, poderia ter feito mais, por exemplo, para limitar o alcance extraterritorial do GDPR.

> **Os requisitos de localização de dados podem ser vistos como um aspecto do protecionismo digital e podem despertar debates relacionados com o comércio no mais alto nível.**

Além disso, os requisitos de localização de dados podem ser vistos como um aspecto do protecionismo digital e podem despertar debates relacionados com o comércio no mais alto

nível. Por exemplo, em 12 de outubro de 2018, dois senadores dos EUA enviaram uma carta aberta ao primeiro-ministro indiano Narendra Modi, pedindo que o governo indiano suavize sua posição sobre a localização de dados e argumentando que é fundamental para o desenvolvimento do comércio digital.[576] Em particular, os senadores visaram um requisito do Reserve Bank of India, o banco central do país, para armazenar dados financeiros dentro do território indiano.[577]

Outro exemplo da interseção entre o comércio internacional e o protecionismo digital pode ser encontrado quando são impostas sanções para impedir o comércio transfronteiriço. Por exemplo, em 24 de agosto de 2017, a Apple supostamente removeu aplicativos populares usados no Irã de sua App Store e emitiu uma declaração especificando que, de acordo com os regulamentos de sanções dos EUA, a App Store não pode hospedar, distribuir ou fazer negócios com aplicativos ou desenvolvedores conectados a determinados países embargados pelos EUA.[578]

A remoção de aplicativos iranianos foi recebida com críticas do ministro iraniano das Telecomunicações, que anunciou sua vontade de contestar a decisão.[579] Da mesma forma, em 15 de maio de 2017, o presidente ucraniano Petro Poroshenko assinou um decreto instruindo os ISPs locais para bloquear sites russos, mídias on-line e plataformas de mídias sociais na jurisdição como parte de uma nova rodada de sanções econômicas contra a Rússia, que anexou a Crimeia da Ucrânia em 2014.[580] A lista de blocos incluiu, nomeadamente, o motor de busca Yandex, bem como a rede de mídia social VK, que é usada por 20 milhões de ucranianos.[581]

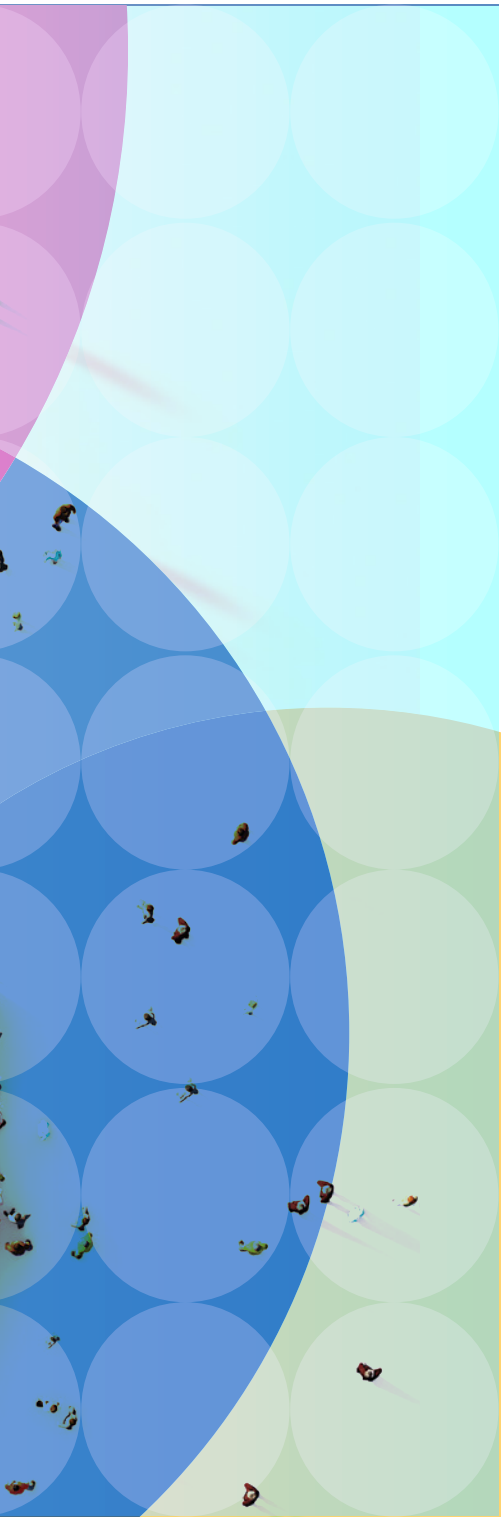
No longo prazo, é provável que o protecionismo digital comprometa significativamente a natureza internacional da Internet e constitua uma ameaça potencial à interoperabilidade.

> **É provável que o protecionismo digital comprometa significativamente a natureza internacional da Internet e constitua uma ameaça potencial à interoperabilidade.**

3.3.6.2. Regionalização

Quando a regionalização cria normas legais e/ou técnicas enraizadas e diversas, isso pode tornar-se um obstáculo a soluções globais. Ao mesmo tempo, as normas legais e/ou técni-

cas regionais podem lançar as bases para soluções escaláveis que podem ser transferidas de um nível regional para um nível global (ou quase global). Desta forma, a regionalização pode contribuir para o estabelecimento de normas globais. A política comercial tem potencial para aumentar a regionalização, mas formas mais profundas de cooperação e coordenação regionais constituem uma força motriz ainda mais forte. A UE é uma ilustração óbvia disso, mas há também muitos outros exemplos: a Cooperação Econômica Ásia-Pacífico (APEC), a Associação das Nações do Sudeste Asiático (ASEAN), a União Africana, a Comunidade dos Estados da América Latina e Caribe (CELAC), a Liga Árabe e a Associação dos Estados do Caribe (ACS) e o Mercado Comum para a África Oriental e Austral (COMESA).



04.
Abordagens jurídicas e técnicas

- Expressão
- Segurança
- Economia

Após um longo período de relativa inação, há agora uma infinidade de abordagens jurídicas para enfrentar os desafios jurídicos transfronteiriços na Internet. Particularmente nos últimos cinco anos, tanto os países em desenvolvimento quanto os países industrializados deixaram de procrastinar e tomaram uma multiplicidade de ações descoordenadas. Algumas jurisdições avançaram com uma velocidade notável, estabelecendo normas globais que competem, pelo menos em parte, com iniciativas globais de normalização de outras jurisdições. Na verdade, pode não ser exagero falar de uma corrida em curso rumo ao estabelecimento de normas globais entre a UE, os EUA, a China e, em menor medida, a Rússia.

Os Estados buscam vantagens competitivas na corrida à supremacia regulatória de várias maneiras. As iniciativas vão desde medidas políticas, como o desenvolvimento de capacidade e a criação de dependência financeira e de segurança entre outros países, ao uso de ferramentas legais como extraterritorialidade e tratados. Neste cenário, há agora uma clara distinção entre aqueles que estabelecem normas e aqueles que, em grande parte, adotam as normas estabelecidas por outros. Não é de surpreender que os países menores e em desenvolvimento estejam quase exclusivamente na ponta receptora.

> **Nos últimos cinco anos, tanto os países em desenvolvimento quanto os países industrializados deixaram de procrastinar e tomaram uma multiplicidade de ações descoordenadas.**

Embora as leis ofereçam algumas soluções, há o reconhecimento de que as normas público-privadas, outras formas de *soft law* e a autorregulação industrial também podem oferecer soluções.

Além disso, várias soluções técnicas avançaram, cada uma com um impacto substancial nos desafios jurídicos transfronteiriços na Internet. A referida corrida para o estabelecimento de normas globais também se desenrola neste contexto, com medidas como desligamentos de Internet, o bloqueio e a aquisição forçada de facilitadores de inovação que fazem manchetes nos noticiários.

Este capítulo descreve e analisa uma seleção de grandes abordagens jurídicas e técnicas para soluções que especialistas enfatizaram em pesquisas e entrevistas, ou que ganharam especial atenção na literatura.

Como um especialista entrevistado observou, o fato de que as questões com as quais os atores agora lutam não são novas pode ser visto como uma fonte de tranquilidade, ou um motivo de preocupação.

4.1. Principais abordagens jurídicas para soluções

Os Estados adotam uma vasta gama de abordagens jurídicas na busca daquilo que consideram ser soluções para os desafios jurídicos transfronteiriços na Internet.

Existe claramente um maior apetite pelas chamadas ordens de retirada (*takedown*) e manutenção da retirada (*staydown*) pelos tribunais. Há também sinais de uma corrida a potenciais multas mais elevadas - os Estados estão aumentando as sanções que impõem a fim de dar prioridade ao cumprimento das suas leis específicas (em detrimento do cumprimento de quadros jurídicos concorrentes impostos por outros Estados).

Outra ferramenta emergente usada para garantir a executabilidade do direito estatal é chamada de "localização de representantes" ("rep localization") — ou seja, leis que exigem que as empresas nomeiem um representante local dentro do Estado que impõe o requisito. Além disso, os Estados estão cada vez mais empenhados no que pode ser descrito como atração jurisdicional, através do qual eles fazem reivindicações excessivamente amplas de jurisdição, dando-lhes um poder discricionário considerável para decidir contra quem dirigir os seus esforços de execução. Existe também uma dependência persistente, e talvez crescente, em testes jurisdicionais focados no assim chamado "direcionamento".

Ao mesmo tempo, no entanto, existem alguns sinais de contenção. Embora continue a ser um conceito contestado no nível internacional, a cortesia e outros apelos ao equilíbrio são discerníveis em vários níveis. Além disso, a questão de como os Estados abordam o escopo de jurisdição ainda está em jogo.

Será que a prática emergente dos Estados que procuram dar às suas sentenças efeito global se tornará consolidada? Ou irá prevalecer uma abordagem mais matizada? Este será um importante campo de batalha nos próximos anos.

Finalmente, até que ponto os termos de serviço e as diretrizes de comunidade, e não as leis, moldam o comportamento on-line, continua sendo um problema real.

Conforme discutido na parte introdutória do relatório (Capítulo 1.5), as tentativas de encontrar abordagens jurídicas para resolver as questões jurídicas transfronteiras enfrentadas pela Internet são dificultadas por "desafios regulamentórios artificiais" - ou seja, os quadros e conceitos contemporâneos são insuficientes para abordar com êxito estas questões.

A superação de tais desafios regulatórios artificiais pode exigir mudanças nos quadros e conceitos tradicionais. Mas também requer capacitação, que se encaixa com a necessidade de inclusão — uma questão-chave a ser considerada no contexto de abordagens de soluções, e tema recorrente citado por especialistas pesquisados e entrevistados.

Tanto os países em desenvolvimento quanto muitos Estados menores em todo o mundo são vistos como sendo "aqueles que aceitam o preço determinado pelos outros" — ou seja, eles devem aceitar soluções e abordagens prevalecentes de países maiores, sem fornecer uma contribuição significativa. Um especialista entrevistado sugeriu que isso leva a um sentimento de colonização tecnológica, que causa ressentimento, particularmente em países com história colonial.

Embora este ponto seja levantado em vários contextos ao longo do relatório, deve certamente ser considerado na análise das abordagens atuais das soluções. É importante avaliar não só o quão bem estas abordagens funcionam nos países que estão na vanguarda das tecnologias da Internet, mas também o seu impacto nos países em desenvolvimento e nos países menores. Além disso, não basta considerar o quão bem essas abordagens para soluções funcionam hoje. Também é necessário considerar como elas funcionarão no futuro, quando o ambiente on-line for ainda mais diversificado.

4.1.1. Ordens de tribunais para retirada ("takedown"), manutenção da retirada ("stay-down") e permanência ("stay-up")[de conteúdo]

Centenas de milhões de posts e centenas de milhares de horas de vídeos são carregados todos os dias e tornados globalmente acessíveis nas principais plataformas de Internet. Isso facilita grandemente a liberdade de expressão e fornece acesso a informações que enriquecem a vida das pessoas. Como muitos especialistas entrevistados observaram, no entanto, a Internet espelha o mundo off-line, e assim, juntamente com o conteúdo que educa, informa e entretém está conteúdo que ofende, ameaça e prejudica. Isso leva a preocupações legítimas sobre o tipo de conteúdo disponível on-line.

> **Na ausência de quadros substantivos e processuais acordados para lidar com a disparidade das leis nacionais, proteger a liberdade de expressão e outros direitos humanos para tratar de abusos na Internet constitui um grande desafio transnacional.**

Na ausência de quadros substantivos e processuais acordados para lidar com a disparidade das leis nacionais, proteger a liberdade de expressão e outros direitos humanos para tratar de abusos na Internet constitui um grande desafio transnacional. O conteúdo legal em um país pode ser ilegal em outro. No entanto, "os Estados que regulam ou influenciam plataformas muitas vezes também, intencionalmente ou não, moldam regras de discurso que as plataformas aplicam em outros países."[582] O Capítulo 3 delineou as principais tendências atuais e destacou a prevalência de ordens que exigem a remoção, exclusão da lista, desindexação, desreferenciamento, exclusão, bloqueio, ou remoção de conteúdo. Tais ordens parecem particularmente comuns no contexto do extremismo e do discurso de ódio (Capítulo 3.1.1), privacidade dos dados (Capítulo 3.1.6), bullying on-line (Capítulo 3.1.3), distribuição não consensual de mídia sexualmente explícita (Capítulo 3.1.4), notícias falsas e desinformação (Capítulo 3.1.5), propriedade intelectual (Capítulo 3.3.1), pornografia infantil (Capítulo 3.2.1), conteúdos fraudulentos (Capítulo 3.2.1) e conteúdos que representem um risco para a segurança (Capítulo 3.2.4). Em muitos países, tais ordens são usadas para suprimir a dissidência política, restrin-

gir a liberdade de expressão, restringir a liberdade de religião e impor restrições de conteúdo de motivação religiosa. Em 20 de agosto de 2018, a Apple anunciou[583] que havia removido 25.000 aplicativos ilegais de jogo de sua App Store chinesa, depois de ter sido criticada pela mídia chinesa por não restringir o acesso aos aplicativos.[584] Em 4 de julho de 2018, o ministro das Comunicações e Informação da Indonésia anunciou que o aplicativo de vídeo chinês TikTok foi banido no país porque continha pornografia, conteúdo inadequado e blasfêmia.[585] Em 11 de julho de 2018, o Ministério declarou [586] que a proibição tinha sido anulada, depois que a plataforma concordou em censurar o "conteúdo negativo".[587] Isso ocorreu após o governo indonésio bloquear o acesso ao Tumblr em março de 2018.[588]

Em 22 de junho de 2018, o regulador de conteúdo da Internet sul-coreano (Korea Communications Standards Commission – KCSC) anunciou que o Tumblr tinha concordado em monitorar melhor o conteúdo adulto ilegal em sua plataforma.[589] O KCSC exigiu que o Tumblr atuasse sobre conteúdo adulto ilegal em setembro de 2017 e a empresa se recusou, argumentando que estava sujeita às leis dos EUA, onde está baseada, levando o regulador a ameaçar a proibição da plataforma no país.[590]

Como este exemplo sul-coreano demonstra, o não monitoramento e/ou bloqueio de conteúdo podem resultar em ameaças de proibição do serviço em questão. E como discutido no Capítulo 4.2.5, em algumas ocasiões, tais proibições são de fato introduzidas.

Em dezembro de 2018, o regulador russo de telecomunicações *Roskomnadzor* multou a Google em 500.000 rublos (cerca de 6.500 euros) por não cumprir um requisito para remover entradas de seus resultados de busca.[591]

A Roskomnadzor multou novamente a Google em julho de 2019[592] e em agosto de 2019 exigiu que a Google parasse de anunciar eventos "ilegais" em massa no YouTube.[593] De fato, a Rússia é particularmente ativa em pressionar os intermediários da Internet para que removam conteúdo. Em 13 de dezembro de 2018, o Twitter publicou seu relatório de transparência para o primeiro semestre de 2018, destacando um aumento de 80% nas solicitações globais de remoção de conteúdo, com 87% das solicitações provenientes da Rússia e da Turquia.[594] E em 9 de setembro de 2018, foi relatado que[595] o YouTube tinha atendido um pedido de funcionários russos para remover vídeos publicados pelo dissidente russo Alexei Navalny, uma

vez que eles eram ilegais de acordo com as leis eleitorais do país.[596] Essa extrema diversidade nas questões subjacentes que podem levar a ordens para excluir, retirar da lista, desindexar, desreferenciar, apagar, bloquear ou remover conteúdo dificulta a discussão de tais ordens dissociadas da lei material subjacente, conduzindo à decisão em causa.

Há uma atenção crescente direcionada a pedidos de manutenção da retirada (*stay-down*) e pedidos de permanência do conteúdo (*stay-up*). A primeira é a mais forte das duas tendências, com uma mudança de restrições de conteúdo para moderação de conteúdo e detecção proativa. Por exemplo, no momento em que este Relatório é escrito, um processo em curso perante o TJUE (Processo C18/18) envolve uma política austríaca que procurou fazer com que o Facebook Ireland Ltd retirasse comentários desfavoráveis sobre ela.[597] Pediu também ao TJUE que considerasse se o Facebook pode ser obrigado a remover informações redigidas de forma idêntica e com um significado equivalente. A política austríaca em questão está procurando garantir que o Facebook seja forçado a monitorar o conteúdo, ao remover continuamente as postagens com comentários desfavoráveis sobre ela, incluindo informações com a mesma redação e com um significado equivalente. A política deseja que estas medidas sejam implementadas em todo o mundo.

Há uma atenção crescente direcionada a pedidos de manutenção da retirada (stay-down) e pedidos de permanência do conteúdo (stay-up).

Em 13 de outubro de 2017, o Tribunal Constitucional da Colômbia ordenou à Google que excluísse um blog hospedado pelo Blogger.com da Google, sob o argumento de que um post anônimo alegou falsamente que um indivíduo era culpado de fraude.[598] O Tribunal também decidiu que a Google deveria excluir qualquer blog futuro fazendo as mesmas alegações difamatórias contra o reclamante. Além disso, o Tribunal Constitucional pediu ao Ministério das TIC que introduzisse um novo regulamento para proteger melhor os direitos dos usuários da Internet.[599] Em 2017, um tribunal australiano deu um passo de longo alcance ao ordenar que o Twitter aplicasse filtragem, ou verificação, para garantir que a informação em disputa não seja publicada ou, se for publicada, seja removida.[600] O Tribunal não considerou injustificado que

esta ordem de suspensão se estendesse a tweets futuros (independentemente do tema) e a contas futuras detidas por qualquer pessoa ou pessoas que utilizem uma ou mais das contas ofensivas.[601] Esta é uma medida extraordinária, na medida em que impõe uma obrigação sobre uma empresa estrangeira para garantir uma proibição vitalícia de pessoas potencialmente estrangeiras de usar a plataforma da empresa para se expressar sobre qualquer assunto.

A sentença é ainda mais notável tendo em conta a aparentemente fraca ligação jurisdicional com a Austrália.[602] Exemplos como o processo C18/18 perante o TJUE e a decisão do Supremo Tribunal de Nova Gales do Sul contra o Twitter, chamam a atenção para as implicações significativas das ordens de manutenção da retirada (*stay-down*) em comparação com as ordens de exclusão (*take-down*). Embora a fraqueza das ordens de exclusão *(take-down)* seja óbvia, na medida em que o conteúdo ofensivo pode ser carregado novamente, ordens de manutenção da retirada *(stay-down)* têm enormes implicações para a liberdade de expressão — o impacto de impedir a publicação de conteúdo é muito diferente do impacto de punir o editor do conteúdo. Por exemplo, se a publicação de conteúdo for impedida, não poderá haver escrutínio público de seu potencial valor e legitimidade. Além disso, o alto volume de trabalho manual envolvido no monitoramento de conteúdo incentiva plataformas de Internet a automatizar a filtragem de conteúdo. Tudo isso tem o potencial de tornar essa filtragem automatizada precisa, mas não impecável.

Seja automatizada ou não, a filtragem de conteúdo dá origem a questões importantes de transparência, devido processo e a falta de procedimentos de recurso. Em um nível mais profundo, suscita questões em torno da distribuição de direitos e deveres entre os setores privado e público e pode ser visto como uma privatização das prerrogativas estatais.

Pedidos de permanência (*stay-up),* ou postagem obrigatória (*must carry*) até agora ganharam menos atenção e foram seguidos em menor grau.[603] Tais pedidos geralmente exigem plataformas de Internet para reintegrar conteúdo que foi retirado, excluído da lista, desindexado, desreferenciado, excluído, bloqueado ou removido.

Até a data, as ordens de permanência (*stay-up*) têm sido discutidas principalmente no contexto das legislações americana, alemã e brasileira. Nos casos em que essas ordens tenham sido solicitadas ao abrigo da legislação dos EUA, elas falharam:

> *Duas dúzias ou mais de peticionários tentaram processar plataformas por derrubarem seus posts ou contas e as plataformas ganharam todos os casos. Para começar, os Termos de Serviço das plataformas e as imunidades estatutárias sob o CDA 230 as protegem de ter que hospedar discursos com os quais discordam. Mais importante ainda, os tribunais têm sustentado consistentemente que os direitos da Primeira Emenda das próprias plataformas as protegem de leis que as forçariam a hospedar ou indexar conteúdo contra sua vontade. Isso significa que mesmo a legislação de postagem obrigatória ("must-carry"), que alguns políticos ameaçaram aprovar, provavelmente não sobreviveria a um desafio constitucional.*[604]

Em contrapartida, os tribunais do Brasil e da Alemanha ordenaram que plataformas de Internet reintegrassem o conteúdo que as plataformas julgaram violar suas diretrizes de comunidade.[605] Ordens como essas têm, pelo menos, um potencial tão grande para criar conflitos de leis quanto as ordens de retirada. Um estudioso que trabalhou questões de permanência/publicação obrigatória (*stay-up/must-carry*) em detalhes apontou para a necessidade de os tribunais encontrarem ferramentas doutrinárias para dissociar a questão da publicação obrigatória 'must-carry' da questão de remoção global [de conteúdo] (discutida no Capítulo 4.1.7).[606]

Um acontecimento recente significativo ocorreu em um acórdão de 4 de dezembro de 2018, em que o Tribunal Europeu dos Direitos Humanos considerou que a liberdade de expressão de um portal de notícias ligado a declarações difamatórias tinha sido violada por uma ordem dos tribunais húngaros para remover esses links.[607] O Tribunal argumentou que não poderia concordar com a abordagem dos tribunais nacionais, que equiparou a mera publicação de um hiperlink com a divulgação de informações difamatórias, impondo automaticamente a responsabilidade pelo próprio conteúdo.[608]

Um dos três programas temáticos da Rede de Políticas Internet & Jurisdição — o Programa Conteúdo e Jurisdição — está desenvolvendo soluções para gerenciar conteúdo globalmente disponível, considerando a diversidade de leis e normas locais aplicáveis na Internet.

PROGRAMA DE CONTEÚDO E JURISDIÇÃO

Os atores da Rede de Políticas Internet & Jurisdição trabalham em conjunto em três programas de política: o Programa de Dados e Jurisdição, o Programa de Conteúdo e Jurisdição e o Programa de Domínios e Jurisdição. Os Programas permitem que os membros coordenem informalmente políticas e desenvolvam conjuntamente propostas de Normas, Critérios e Mecanismos operacionais. O Programa Conteúdo e Jurisdição atualmente se concentra na moderação e restrições de conteúdo transfronteiriças com o objetivo de abordar as normas materiais aplicáveis, incluindo a interação entre direitos humanos internacionais e regionais acordados, leis nacionais e diretrizes de comunidade das empresas; as obrigações respectivas dos Estados e as respectivas responsabilidades e proteções de outros intervenientes, incluindo a identificação de conteúdos alegadamente ilegais; tomada de decisões, normas e procedimentos, incluindo a trajetória de escalada para decisões individuais e mecanismos de recurso; finalidades legítimas, necessidade e proporcionalidade no que se refere ao âmbito geográfico das restrições, bem como aos procedimentos e normas de transparência necessários que devem ser aplicados além-fronteiras. Os participantes do Programa estão focados nos seguintes tópicos:[609]

- Normas – Abordar conflitos de diferentes normas materiais para identificar conteúdo alegadamente ilegal e determinar a relação ou natureza hierárquica da relação.
- Convergência – Nível de convergência global alcançável ou desejável em tais definições.
- Tempo de resposta – Prazos de reação adequados por parte dos intermediários após o recebimento das notificações.
- Tomada de decisões – A arquitetura da tomada de decisões e o papel dos diferentes tipos de atores estatais e não-estatais (incluindo intermediários, governos, tribunais, reguladores e indivíduos que apresentam pedidos).
- Algoritmos – Combinação adequada de ferramentas algorítmicas e revisão humana considerando os limites das ferramentas algorítmicas.
- Normas processuais – Normas processuais que avaliam a legalidade do conteúdo: normas de avaliação, garantia e verificação, funções e soluções.
- Escopo geográfico – Situações, se houver, que poderiam, excepcionalmente, justificar restrições globais, incluindo medidas que abordem ações contraditórias de diferentes Estados.
- Transparência – Expandir os esforços existentes e reforçar a coordenação entre eles.
- Formatos de solicitação – Documentar e divulgar o que as solicitações do governo devem conter.
- Notificação – Tratamento da notificação dos usuários e sua capacidade de objetar.
- Remediação – Mecanismos para a rápida restauração de conteúdo abusivamente restringido.
- Tipos de conteúdo — Características do conteúdo, incluindo intenção e possíveis efeitos; determinação de medidas adequadas para abordar diferentes tipos de conteúdo.
- Tipos de atores — Funções e responsabilidades.

4.1.2. Corrida para as multas potencialmente mais elevadas

A perspectiva de impor multas de alto potencial é uma poderosa arma reguladora. É provável que um Estado que ameace impor multas elevadas atraia a atenção dos meios de comunicação social, o que contribui para aumentar a sensibilização para a lei em questão. Mais importante ainda, quanto mais elevadas forem as multas potenciais por descumprimento, maior será o "incentivo empresarial" para assegurar o cumprimento. Isto é particularmente importante nos casos em que o objeto do regulamento — como uma empresa multinacional — está sujeito a regulamentação concorrente de outro Estado ou de outros Estados. Por exemplo, uma empresa apanhada por leis contraditórias pode optar por cumprir a lei do Estado que imponha multas mais elevadas, à custa de não cumprir a lei de outro Estado com multas mais baixas.

Contra este pano de fundo, não é surpreendente ver uma espécie de corrida para multas potencialmente mais elevadas. Em novembro de 2018, por exemplo,[610] o governo russo estava considerando alterar um requisito legal de 2017 para que os mecanismos de busca removam os links de resultados de pesquisa para sites proibidos, a fim de aumentar as multas máximas por descumprimento de 700.000 rublos (cerca de € 9.000) para 1% da receita local da empresa.[611]

Além disso, o setor de tecnologia enfrenta multas cada vez mais elevadas no domínio do direito da concorrência (legislação antitruste), tanto nos EUA quanto na UE.[612]

Em 6 de novembro de 2018, o Parlamento da Maurícia adotou[613] alterações à Lei de Tecnologias da Informação e Comunicação (ICTA) do país, que visa a regular e reduzir conteúdos e atividades prejudiciais e ilegais perpetrados através de qualquer serviço de informação e comunicação — incluindo serviços de telecomunicações — através do aumento de multas e da pena de prisão dos infratores.[614]

No campo da privacidade de dados, pode-se notar que a proposta de lei de privacidade de dados da Índia inclui multas de até aproximadamente US$2,7 milhões ou 4% do volume de negócios global de uma empresa.[615] A Austrália está tentando aumentar suas sanções[616] e a referência às altas multas potenciais no âmbito do GDPR da UE foi feita no Capítulo 3.1.6.1. Mas as multas de até €20 milhões, ou seja, 4% do volume de

negócios anual global previsto no GDPR, são minimizadas pela ameaça de multas de até 10% do volume de negócios anual da parte infratora encontrada na Lei de Proteção de Dados de Trinidad e Tobago de 2011 (s. 69). Em julho de 2019, o Facebook chegou a um acordo de US$ 5 bilhões com a Comissão Federal de Comércio em relação a violações de privacidade dos consumidores.[617]

O RISCO DE MULTAS ELEVADAS — UM OBSTÁCULO SIGNIFICATIVO PARA AS PME

Alguns especialistas entrevistados enfatizaram que o risco de multas de alto potencial é uma barreira significativa para as PME, uma vez que o seu acesso a aconselhamento jurídico sofisticado sobre questões jurídicas complexas e à conformidade associada é frequentemente limitado.

O nível das multas, embora importante, é apenas um dos, pelo menos, três fatores centrais nesta discussão. Outro fator central é o grau de risco da aplicação efetiva. A ameaça de multas elevadas pode ser insuficiente se não for acompanhada de processos de fiscalização realistas — por exemplo, através de requisitos de localização de representantes (Capítulo 4.1.3). Neste contexto, um especialista entrevistado apontou para uma prática emergente segundo a qual os tribunais ordenam que os fundos das empresas sejam congelados como um mecanismo que garanta uma execução eficaz.

No entanto, outro fator central diz respeito ao valor do mercado em questão. Se existe um risco prático de aplicação efetiva de multas elevadas num mercado de pouco valor para o objeto da regulação, como uma empresa multinacional, essa empresa pode determinar que os riscos superam os benefícios e simplesmente abandonar completamente o mercado. Neste contexto, a complexidade, a clareza e a certeza da lei em questão poderão afetar o cálculo. A combinação de multas elevadas e leis imprevisíveis e complexas cria riscos mais elevados que são mais difíceis de mitigar.

Neste contexto, os países menores — industrializados ou em desenvolvimento — estão em desvantagem competitiva porque o valor de seus mercados é menor. Os países em desenvolvimento, que dispõem de instrumentos de aplicação fracos, podem ficar ainda mais desfavorecidos.

4.1.3. "Localização do representante" — representação local forçada

Nos últimos anos tem havido uma tendência para o que pode ser chamado de "localização forçada do representante". A localização do representante envolve requisitos que obrigam uma organização estrangeira a manter uma representação física no Estado que impõe o requisito. Neste sentido, existem paralelos entre "localização do representante" e "localização de dados" — ambos visam a garantir uma vantagem de execução.

O GDPR e outros regulamentos da UE, por exemplo, exigem que os estrangeiros designem, por escrito, um representante na UE sob determinadas circunstâncias. Esta abordagem é autoaperfeiçoada, na medida em que quanto mais instrumentos da UE adotarem esta abordagem, mais fácil será justificá-la num contexto novo. A proposta de diretiva sobre evidências eletrônicas do Parlamento e do Conselho Europeu, por exemplo, sublinha que a obrigação de designar um representante legal para prestadores de serviços não pertencentes à UE já existe em certos atos da legislação da UE.[618]

A localização do representante é claramente um requisito oneroso para todas as empresas estrangeiras que de outra forma não teriam uma presença física na UE e até que ponto a UE pode fazer cumprir esta situação em larga , é algo ainda incerto. Existe ainda o risco de a execução arbitrária comprometer a legitimidade do regime. Há também uma questão prática a considerar: como uma empresa estrangeira de dimensão pequena ou média tomará decisões informadas sobre o recrutamento de alguém de confiança para ser o seu representante na UE? E aqueles na UE que concordam em assumir este papel enfrentam o risco de serem responsabilizados pelo incumprimento do prestador de serviços.[619] A menos que um representante legal designado possa ser plenamente responsabilizado, o valor de todo o sistema de localização forçada deve ser questionado. Embora a UE pareça estar impulsionando este avanço no campo da privacidade de dados, Estados não pertencentes à UE começaram também a adotar a mesma abordagem. Por exemplo, a lei de proteção de dados proposta pela Tailândia incorpora um requisito de localização de representante inspirado na UE e potencialmente mais amplo.[620] A ameaça potencial de penas de prisão por violações de privacidade de dados na Tailândia pode complicar ainda

mais questões práticas associadas a encontrar representantes locais confiáveis e dispostos. Tal como a Tailândia, outros Estados em todo o mundo provavelmente seguirão a liderança da UE nesta abordagem. A teia regulatória resultante - com requisitos de localização de representantes em um grande número de Estados - será difícil e dispendiosa de navegar.

Além disso, a China exige que um representante local se envolva em negócios on-line, e em 26 de outubro de 2018, durante uma reunião de representantes de vários ministérios indianos e representantes de empresas do Facebook, Google e WhatsApp, o Ministério do Interior indiano ordenou que as plataformas nomeassem funcionários locais para reclamações como parte de um esforço para garantir a remoção de conteúdo censurável ou malicioso da vista do público.[621]

O governo do Vietnã, ao mesmo tempo, pediu ao Facebook que abrisse um escritório no país para cumprir uma lei de segurança cibernética de 2018 que altera os requisitos para o processamento de dados pessoais dos usuários vietnamitas.[622] A lei exige que todas as plataformas que oferecem serviços no Vietnã removam conteúdo ofensivo dentro de um dia após a apresentação de uma solicitação, armazenem dados no território do país e operem um escritório local.[623]

A agência de comunicações sul-coreana, Korea Communications Commission, também anunciou seus planos para 2019, que inclui o desenvolvimento de "Orientações sobre a utilização da rede" que exige que operadores ultramarinos apontem um representante local.[624]

Dada a natureza global da Internet, é difícil ver como a localização de representantes pode ser escalável. A abordagem da UE pode ganhar alguma aceitação entre as partes afetadas, uma vez que estas só precisam ter representação em um Estado-membro da UE — um preço que muitos atores on-line podem estar dispostos a pagar — mas como isso se traduz para o resto do mundo? Se o Afeganistão, a Argentina e a Austrália adotarem a mesma abordagem, será vantajoso para as empresas de Internet também terem representantes em cada um desses Estados?

Pode-se responder a esta preocupação argumentando que a forma como as empresas de tecnologia (em grande parte baseadas nos EUA) interagem com o Afeganistão, a Argentina e a Austrália não é problema da UE; e essa resposta não é despro-

vida de mérito. No entanto, mesmo na medida em que funciona para a UE, a localização de representante não é claramente a solução para a maioria das outras jurisdições ao redor do mundo. Com efeito, poder-se-ia afirmar que a UE e outros organismos que procuram ativamente inspirar desenvolvimentos jurídicos noutros Estados devem tentar assegurar que as suas abordagens sejam escaláveis.

4.1.4. Atração jurisdicional como abordagem regulatória

Como observado anteriormente, muitos Estados se envolvem no que pode ser chamado de "atração jurisdicional", ou seja, fazem amplas reivindicações de jurisdição sobre atividades na Internet - reivindicações que não podem ser apoiadas por uma execução efetiva – e buscam apenas algumas das atividades na Internet sobre as quais eles reivindicam jurisdição. Dos instrumentos regulatórios discutidos durante as entrevistas, o Artigo 3 do GDPR da UE (discutido no Capítulo 3.1.6.1) é um exemplo primordial e frequentemente citado desta prática.

O Marco Civil do Brasil é outro exemplo.[625] De acordo com a lei adotada, os dados brasileiros são considerados sujeitos à jurisdição brasileira, independentemente do local onde estejam armazenados fisicamente. O artigo 11 do Marco Civil afirma que "[i] Em 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"[626]; e o §2 acrescenta que "[o] estabelecido no Art.11 aplica-se mesmo que as atividades 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".[627]

Esta abordagem - também conhecida como "excesso de regulação" – tem sido amplamente criticada. Pode argumentar-se que só é defensável em situações em que tanto a reivindicação extraterritorial quanto o direito material a que diz respeito podem ser justificados como uma marcação adequada de valores sociais importantes.[628] Por exemplo, amplas reivindicações de jurisdição que não podem ser apoiadas com execução efetiva podem, no entanto, ser justificadas se um

Estado fizer a alegação tão limitada quanto as circunstâncias permitirem; e se a lei material à qual ela se refere for limitada a uma expressão de valores sociais que se alinhem com os padrões internacionais de direitos humanos e sejam centrais para o Estado em questão.

Aplicando isto ao artigo 3º do GDPR da UE e ao Marco Civil do Brasil, é evidente que as respectivas reivindicações jurisdicionais são demasiado amplas e que algumas das regras materiais (por exemplo, o requisito do GDPR de um responsável pela proteção de dados) são demasiado onerosas.

A atração jurisdicional conduz à execução arbitrária da lei, que os especialistas entrevistados descreveram como uma infração ao Estado de Direito. Também contribui para a meta-tendência da hiper-regulação discutida no Capítulo 2.2.2.

4.1.5. Direcionamento / direcionamento de atividades / exercício da atividade comercial /"doutrina dos efeitos"

Existe um reconhecimento generalizado de que um Estado pode ter jurisdição resultante de atividades iniciadas fora de suas fronteiras, nos casos em que as atividades têm uma ligação substancial com esse Estado – por exemplo, visando os consumidores nesse Estado ou causando danos nesse Estado. Este pensamento é discutido de forma variada em termos de "direcionamento", "direcionamento de atividades", "exercício da atividade comercial" ou, no contexto do direito internacional público, como "doutrina dos efeitos" (por conveniência, é referido como "teste de direcionamento" abaixo).

Um dos primeiros exemplos do teste de direcionamento (doutrina dos efeitos) expressamente aplicado no contexto da Internet encontra-se num caso de difamação na Internet nos EUA em 2002. Em *Young v. New Haven Advocate,*[629] dois jornais baseados fora da Virgínia publicaram artigos, em parte, discutindo a conduta de moradores da Virgínia. Os artigos estavam disponíveis off-line e on-line.

Apesar disso, o Tribunal de Apelação do Quarto Circuito dos EUA concluiu:

> *Os jornais não publicaram materiais na Internet com a intenção manifesta de visar os leitores da Virgínia. Assim, os jornais não poderiam "ter razoavelmente antecipado que seriam levados ao tribunal [na Virgínia]*

> *para responder pela verdade das declarações feitas em seus artigos". Calder, 465 EUA em 790 (citação omitida). Em suma, os jornais não têm contatos suficientes na Internet com a Virgínia para permitir que o tribunal distrital exerça jurisdição específica sobre eles.*[630]

Outro caso de direcionamento inicial foi apresentado ao Tribunal Federal da Austrália no processo *Ward Group Pty Ltd contra Brodie & Stone plc.* Neste caso, a Austrália, juntamente com vários outros países, foi listada em um conjunto de países suspensos *(drop list)* como um destino para o qual os produtos poderiam ser enviados de um site estrangeiro e os preços poderiam ser obtidos em dólares australianos. Apesar disso, o Tribunal concluiu que: "A publicidade dos proprietários do site na Internet de produtos para venda era uma comercialização desses produtos para o mundo em geral e eu não estou convencido de que se tratasse de um marketing especificamente direcionado ou dirigido a consumidores na Austrália."[631] Sob este raciocínio, visar ao mundo inteiro significa não ter como alvo nenhum Estado em particular. No entanto, a imparcialidade de uma empresa que vende para o mundo em geral, sendo vista como não tendo como alvo nenhum Estado, é altamente questionável quando um negócio que tem como alvo um punhado de Estados é capturado pelo teste de direcionamento de todos esses Estados. Em contrapartida, os preços de cotação numa moeda local que difere do que uma empresa utiliza comumente é explicitamente mencionado como um indicador relevante de segmentação no teste de direcionamento da UE, tal como articulado pelo TJUE nos casos apensos do *Hotel Alpenhof/ Pammer*.[632] Este modelo foi transplantado para o GDPR da UE,[633] bem como na proposta de diretiva e regulamento da UE em matéria de evidência.[634]

O fato de o teste de direcionamento fazer parte de instrumentos que já estão sendo copiados em outros sistemas jurídicos sugere que agora vai se espalhar ainda mais. Por exemplo, o teste de direcionamento é agora encontrado em propostas de proteção de dados na Argentina e na Tailândia, que adotaram a abordagem do GDPR.

> **Deve-se determinar caso a caso, se um site tem ou não como alvo um determinado Estado e tal avaliação invariavelmente envolve um alto grau de arbitrariedade.**

Apesar de seu reconhecimento generalizado, o teste de direcionamento é controverso devido à dificuldade em determinar o que equivale a direcionamento. Por exemplo, deve-se determinar caso a caso, se um site tem ou não como alvo um determinado Estado e tal avaliação invariavelmente envolve um alto grau de arbitrariedade. Assim, as dificuldades práticas em garantir uma aplicação consistente do teste de direcionamento resultam em imprevisibilidade para as partes. Isto mina o valor do teste de direcionamento ou cria um obstáculo intransponível à sua utilização eficaz. Afinal, não são apenas reivindicações jurisdicionais exorbitantes que são problemáticas, mas também reivindicações jurisdicionais arbitrárias.

No caso *Argos* no Reino Unido de 2018, o Tribunal Superior do Reino Unido declarou que a corporação dos EUA que vende software de construção (Argos Systems) estava visando a consumidores no Reino Unido através do uso do Google Ads, que direcionou mal os consumidores do Reino Unido que procuram o varejista baseado no Reino Unido com o mesmo nome. A Argos Systems recebeu receitas provenientes do volume de tráfego.

Apesar disso, a Argos UK não conseguiu, em última análise, estabelecer uma vantagem injusta.[635] Uma alternativa ao teste de direcionamento é a abordagem relacionada, mas menos frequentemente discutida, a "abordagem de desdirecionamento" (*distargeting approach*),[636] que obriga as empresas a regular ativamente as jurisdições onde atuam. Esta abordagem pressupõe que as empresas visam ao mundo em geral; mas esta presunção é refutada nos casos em que uma empresa demonstra que tomou medidas adequadas, mas talvez simples, para evitar o risco de se envolver com usuários em Estados considerados "indesejáveis" para a exposição. O ônus que isto representa pode ser compensado pelo maior grau de previsibilidade que proporciona, em relação ao teste de direcionamento.

4.1.6. Um enfoque comum em cortesia, mas uma falta de acordo.

É natural que as atividades on-line se conectem com múltiplas jurisdições; na verdade, essa é a posição padrão. Como resultado, os Estados têm de prestar contas por outros interesses que não os seus.

No direito internacional, o conceito de cortesia tem sido utilizado há muito tempo como um instrumento para contabilizar

os interesses de outros Estados; e vários avanços recentes que afetam os desafios jurídicos transfronteiriços na Internet colocaram o conceito em maior destaque. A análise de cortesia é parte importante do CLOUD Act dos EUA e o equilíbrio de interesses é central, por exemplo, na proposta de Diretiva e Regulamento da UE sobre provas online.[637] Considerações de cortesia também desempenharam um papel central no caso *Microsoft Corp. v. Estados Unidos,*[638] julgado na Suprema Corte dos EUA em 27 de fevereiro de 2018, bem como nos muitos pareceres de *amicus* apresentados sobre o assunto. A Comissão Europeia abraçou claramente o papel da cortesia em seu parecer de *amicus,* proclamando que:

> *Qualquer lei nacional que crie obrigações transfronteiriças — seja promulgada pelos Estados Unidos, pela União Europeia ou por outro Estado — deve ser aplicada e interpretada de forma consciente com as restrições do direito internacional e as considerações de cortesia internacional. Os tratados fundamentais da União Europeia e a jurisprudência consagram os princípios do "respeito mútuo às esferas de jurisdição" dos Estados soberanos e da necessidade de interpretar e aplicar a legislação da UE de forma coerente com o direito internacional.*[639]

No contexto dos desafios jurídicos transfronteiriços na Internet, o conceito de cortesia é uma importante lembrança de que, mesmo que um Estado que faz uma reivindicação de jurisdição tenha interesse e uma forte ligação com o assunto em questão, deve ainda considerar os direitos e interesses de outros Estados antes de, em última análise, decidir reivindicar jurisdição.

Um especialista entrevistado observou que colegas nos EUA muitas vezes falam de cortesia, mas que existem outras ferramentas importantes no direito internacional (privado), também. Embora o conceito de cortesia possa ser encontrado tanto no direito internacional quanto nas leis de vários Estados, carece de uma definição uniforme. Esta ambiguidade nem sempre é apreciada e, por vezes, os comentadores parecem pressupor que o conceito bem desenvolvido de cortesia na legislação dos EUA representa a sua compreensão global.

Ainda recentemente em 2005, no entanto, os juízes do Supremo Tribunal da Austrália afirmaram que a cortesia é "sem sentido ou enganosa" e "uma questão para os soberanos, não para os juízes obrigados a decidir um caso de acordo com os direitos das partes".[640] Claramente, as atitudes em relação à cortesia variam muito. Este é apenas um exemplo da confusão em torno deste conceito e ilustra claramente a importância de garantir um entendimento comum.

4.1.7. Escopo da jurisdição — ordens judiciais locais com implicações globais

Sempre que um tribunal ordena que um ator da Internet bloqueie, remova da lista, desindexe, desreferencie, exclua, remova ou retire o conteúdo, ele precisará considerar se a sentença deve ser aplicada apenas em relação a publicações no Estado onde o tribunal está localizado, ou se deve ser aplicada de forma mais ampla — e talvez até globalmente. Esta questão – "alcance da jurisdição" ou, talvez, "alcance da jurisdição de reparação"[641] – é atualmente um "campo de batalha" fundamental, onde múltiplos litígios jurídicos de grande visibilidade estão sendo travados.

Assim, o alcance de jurisdição diz respeito ao âmbito geográfico adequado das decisões proferidas por um tribunal com jurisdição pessoal e do assunto em questão — como nas situações de bloqueio, supressão, desindexação, anulação da referência, exclusão, remoção ou retirada acima mencionadas. A mesma questão se coloca quando um tribunal determina a indenização a ser concedida por publicações online. O tribunal só pode conceder indenizações por perdas e danos em relação aos efeitos sentidos no Estado em que se situa o tribunal, ou alargar a decisão de indenização a outros Estados (talvez até mesmo a nível mundial).

O alcance da jurisdição em relação aos conteúdos da Internet não é uma questão nova, no entanto, tem sido largamente ignorada até recentemente. Já em 1999, o Supremo Tribunal de Nova Gales do Sul (Austrália) expressou a opinião de que:

> *Uma liminar para restringir a difamação na NSW [Nova Gales do Sul] é projetada para garantir o cumprimento das leis da NSW e para proteger os direitos dos demandantes, uma vez que esses direitos são definidos pela lei da NSW. Tal injunção não se destina a*

> *sobrepor a lei da NSW relativa à difamação em todos os outros Estados, territórios e países do mundo. No entanto, esse seria o efeito de uma ordem de restrição da publicação na Internet.*[642]

Este tipo de autocontenção judicial parece menos comum hoje em dia. O alcance da jurisdição ganhou uma atenção considerável à luz de litígios de alta visibilidade, como o processo *Equustek*[643] da Suprema Corte do Canadá, de 2016 (ver Capítulo 3.3.1), o acórdão do TJUE de 2017 proferido no processo *Bolagsupplysningen OÜ*[644] (ver Capítulo 3.1.2.1), o direito de ser esquecido — *Google France* — (ver Capítulo 3.1.6 .2) e o processo *Glawischnig-Piesczek*[645] (ver Capítulo 3.1.2.1).

No entanto, esta questão parece atrair menos atenção em muitas outras partes do mundo. Por exemplo, em sua decisão no processo *Hassel v. Bird* em julho de 2018, o Supremo Tribunal da Califórnia reverteu uma ordem do Tribunal de Apelações, garantindo, assim, que as plataformas possam continuar a contar com a proteção oferecida pela seção 230 da Lei de Decência das Comunicações.[646] Significativamente, nem o Supremo Tribunal da Califórnia nem o Tribunal de Apelações viram motivos para abordar as implicações internacionais do caso, embora os demandantes tenham procurado a remoção de todas as análises difamatórias publicadas pelo réu no Yelp.com e em qualquer outro lugar onde elas aparecessem na Internet.[647]

Embora os casos do TJUE que discutem a questão do alcance da jurisdição tenham merecido uma atenção considerável nas discussões acadêmicas e políticas, decisões como *Hassell v. Bird*, que envolvem reivindicações implícitas de âmbito global de jurisdição — por exemplo, através da remoção de conteúdo com efeito global — são praticamente ignoradas nos debates.

Entre os atores da Rede de Políticas Internet & Jurisdição, há uma preocupação generalizada sobre os tribunais fazerem reivindicações excessivamente amplas quanto ao alcance da jurisdição.

AS RESTRIÇÕES DE CONTEÚDO DEVEM SER GLOBAIS EM DETERMINADAS CIRCUNSTÂNCIAS

Entre os especialistas pesquisados, a maioria (64%) considerou que as restrições de conteúdo deveriam ser globais em determinadas circunstâncias. 27% consideraram que as restrições de conteúdo nunca deveriam ser globais e apenas 9% argumentaram que as restrições de conteúdo deveriam ser globais por padrão.

Os especialistas pesquisados concordaram amplamente que as restrições globais de conteúdo são apropriadas em relação a conteúdo que é universalmente ilegal, com um grande número apontando para proibições de conteúdo de abuso sexual de crianças, como um exemplo de tal conteúdo. Conforme observado por vários entrevistados, praticamente todas as outras formas de conteúdo estão sujeitas a leis e normas diferentes. Alguns, no entanto, mencionaram algumas outras áreas, incluindo conteúdos que promovem o terrorismo, conteúdos que violam direitos de autor e conteúdos que apelam ao genocídio, como áreas com um grau relativamente elevado de harmonização.

> **Entre os atores da Rede de Políticas Internet & Jurisdição, há uma preocupação generalizada sobre os tribunais fazerem reivindicações excessivamente amplas quanto ao alcance da jurisdição.**

Alguns especialistas pesquisados consideraram que as restrições de conteúdo deveriam ser globais para dissuadir plataformas de ceder a regimes repressivos, oferecendo bloqueio seletivo, e para que os usuários em países livres possam ver e desafiar os bloqueios. Conforme observado por outro especialista pesquisado, no entanto, restrições globais de conteúdo podem levar à adoção das abordagens mais restritivas e desafiar ordens de bloqueio estrangeiras pode ser difícil.

Também parece provável que os Estados já dominantes tenham mais sucesso na execução de ordens de âmbito global do que os Estados menores e em desenvolvimento. Desta forma, as reivindicações de âmbito global de jurisdição dos principais Estados podem impedir os países em desenvolvimento de estabelecerem suas próprias agendas. Para determinados

fins, tais como prevenir a criação de paraísos para materiais de abuso infantil, esta intervenção de Estados dominantes pode ser adequada. Em outros contextos, pode ser inapropriado.

Várias observações salientaram igualmente que o alcance da jurisdição deveria ser determinado com base nos fatos de um caso individual. Por exemplo, um especialista consultado observou que as restrições globais de conteúdo são motivadas, quando é claro que uma restrição não global causaria danos reais.

Vários especialistas entrevistados também comentaram sobre a questão do âmbito de jurisdição para restrição de conteúdo. Um especialista entrevistado observou que alguns provedores tomam decisões regionais ou baseadas no idioma nos casos em que as restrições de conteúdo se aplicam apenas a regiões, e não a países ou ao mundo, ou ao conteúdo em determinados idiomas.

Alguns especialistas entrevistados expressaram preocupações sobre as tendências atuais das restrições de conteúdo global, sendo que um deles alegou que pode ser necessário um conflito de leis para que esse desafio seja tratado como uma prioridade a ser resolvida em nível governamental, e não como uma questão acadêmica. Outro especialista entrevistado discutiu os desafios para se chegar a um consenso sobre as normas para determinados conteúdos. Isto é particularmente difícil numa perspectiva global, uma vez que se tratam de zonas cinzentas, como os discursos de ódio e os conteúdos neonazistas, mas seria possível chegar a um acordo sobre os procedimentos adequados, pelo menos.

Para resumir as respostas, os atores da Rede de Políticas Internet & Jurisdição são geralmente da opinião de que:

1. Restrições globais de conteúdo são justificadas para determinado conteúdo, pelo menos, para materiais de abuso infantil.
2. Além desse conteúdo, a violação da lei local não deve, por padrão, ser cumprida com restrições globais de conteúdo.
3. O alcance apropriado de jurisdição para restrições de conteúdo é do contexto específico. Não existe uma solução de "tamanho único".
4. Há valor no monitoramento das restrições de conteúdo, a fim de proporcionar transparência e oportunidades para desafiar as restrições de conteúdo.

Estas são observações importantes que, segundo se espera, informarão os tribunais, à medida que evolui um quadro coerente para o âmbito da jurisdição.

Além disso, foram sugeridas melhorias estruturais. Um especialista consultado sugeriu que, para reforçar a boa-fé entre jurisdições, uma opção é criar uma Liga de Juízes, semelhante à Convenção de 25 de outubro de 1980 sobre os Aspectos Civis de Rapto Internacional de Crianças. Os juízes conhecer-se-iam previamente, o que reforçaria suas relações e a execução das decisões judiciais poderia ser mais eficaz.

4.1.8. Termos de serviço e diretrizes de comunidade

As plataformas da Internet e os termos de serviço e os padrões de comunidade que impõem aos seus usuários têm um enorme impacto na regulação do conteúdo da Internet. De fato, devido ao número de termos de serviço e padrões de comunidade aos quais os usuários de Internet estão expostos, as pessoas agora celebram mais contratos do que nunca. Mais importante ainda, esses contratos incluem cláusulas de escolha de foro e escolha de lei que apontam para tribunais estrangeiros e leis estrangeiras.

Algumas das principais meta-tendências exploradas no Capítulo 2 referem-se diretamente às plataformas da Internet. Aqui, a tônica está nos termos de serviço e nos padrões de comunidade enquanto tais, bem como no papel que estes desempenham nos desafios jurídicos transfronteiriços na Internet.

Os termos de serviço e os padrões de comunidade normalmente abordam questões como políticas de moderação de conteúdo, questões de propriedade intelectual, limitações de responsabilidade e o uso, compartilhamento e proteção de dados do usuário. É importante ressaltar que muitas vezes eles também descrevem como resolver possíveis disputas. Podem, por exemplo, incluir cláusulas que especifiquem qual a lei do país que deve ser aplicada em caso de litígio e em que tribunal(is) o litígio pode ser instaurado. Podem igualmente nomear mecanismos específicos de resolução extrajudicial de litígios, tais como a arbitragem, a mediação ou qualquer outra forma.

Apesar da falta de negociações e de sua imposição unilateral, os termos de serviço e os padrões de comunidade são, do ponto de vista jurídico, contratos entre plataformas de Internet e seus usuários. Bygrave escreveu longamente sobre o papel central

que os contratos desempenham na regulação da Internet. Ele ilustra, por exemplo, que a descrição clássica de Lessig das quatro forças regulatórias (lei, código, mercado e normas)[648], que tem guiado e de fato dominado muito o pensamento sobre governança da Internet, não leva em conta o papel distinto dos contratos.[649] Isso é significativo, pois os contratos, incluindo termos de serviço e padrões de comunidade, geralmente têm um impacto mais direto sobre as atividades dos usuários da Internet do que a legislação.

Uma vez que os termos de serviço e as normas comunitárias são normalmente estabelecidos entre empresas e consumidores, a legislação de proteção do consumidor muitas vezes afeta os termos que eles podem incluir e como eles podem ser aplicados. Por exemplo — tal como referido no Capítulo 3.3.2 sobre comércio eletrônico, restrições de comercialização e proteção dos consumidores — as recentes decisões judiciais no Canadá e na UE sugeriram uma possível tendência contra a manutenção de cláusulas de escolha do foro e do direito aplicável nos contratos on-line. Apesar de seu futuro como ferramenta de imposição da escolha da legislação e da escolha do foro continua não sendo claro, não há dúvida de que os termos de serviço e os padrões de comunidade continuarão sendo um instrumento importante para a moderação dos conteúdos - e continuarão a ter impacto nos desafios jurídicos transfronteiriços na Internet nesse contexto. Se o direito deixar o assunto para plataformas de Internet, por exemplo, elas podem usar seus termos de serviço e padrões de comunidade para delinear o alcance de jurisdição que considerarem apropriado e remover ou bloquear conteúdo com base nos padrões que estabeleceram.

Os termos de serviço também desempenham um papel central no contexto dos nomes de domínio. De cima para baixo, a atribuição de nomes de domínio é orientada por disposições contratuais no que têm sido designadas por regulação privada transnacional baseada em contratos.[650] O processo de resolução de litígios prescrito nos acordos com os registrantes de nomes de domínio é frequentemente apresentado como um exemplo de autorregulação bem-sucedida.

Finalmente, enquanto os termos de serviço, como ferramenta reguladora, podem ser vistos como um produto e uma reiteração moderna da ideia de padrões de comunidade e au-

torregulação que caracterizavam os primeiros dias da Internet, eles não englobam necessariamente os ideais libertários que coloriram os padrões de comunidade e a autorregulação.

4.2. Principais abordagens técnicas para soluções

Muitas das questões jurídicas que surgem no contexto da tecnologia da Internet também podem ser resolvidas através dessa mesma tecnologia. Esta seção descreve e examina o papel de uma série de abordagens técnicas particularmente significativas para soluções com impacto nos desafios jurídicos transfronteiriços na Internet.[651] *Um tema que une muitas destas abordagens técnicas é o fato de se centrarem na limitação do acesso aos conteúdos.*

A primeira abordagem técnica para soluções — a utilização das chamadas tecnologias de geolocalização — é atualmente um importante "campo de batalha". A pesquisa realizada para este Relatório abordou especificamente as tecnologias de geolocalização e lança luz sobre uma divergência de pontos de vista dos atores da Rede de Políticas Internet & Jurisdição. Outras medidas técnicas destinadas a limitar o acesso aos conteúdos incluem:

- Filtragem de conteúdos no nível da rede nacional;
- Ordem judicial de suspensão, supressão, não resolução, confisco e transferência no contexto do sistema de nomes de domínio;
- Ordem judicial de bloqueio do DNS, o bloqueio ou reencaminhamento do endereço IP e o bloqueio do URL no contexto do sistema de nomes de domínio;
- Paralisações de serviço; e
- Desligamentos da Internet.

Todas estas medidas técnicas de bloqueio, pelo menos na sua forma atual, têm potencial para serem enfraquecidas, ou até mesmo inutilizadas, pelo desenvolvimento da conectividade Internet via satélite, como os projetos OneWeb[652] e Iridium[653], que fornecem conectividade em banda larga via satélite em nível mundial.

A tendência dos requisitos de localização forçada de dados também é examinada e dá-se atenção ao impacto multifacetado da inteligência artificial.

A complexidade tecnológica constitui um obstáculo à procura de abordagens técnicas úteis para encontrar soluções para os desafios jurídicos transfronteiriços na Internet. Portanto, tal como no contexto das abordagens legais às soluções, há necessidade de capacitação a todos os níveis. É necessário reforçar as capacidades técnicas tanto dos usuários da Internet quanto das PME, bem como dos administradores, dos serviços responsáveis pela execução da lei, dos tribunais, dos governos e de outros atores. Esta necessidade é particularmente aguda nos países em desenvolvimento, mas também existe nos mais altos níveis nos países desenvolvidos.[654]

4.2.1. Tecnologias de geolocalização — sacrificando a "ausência de fronteiras" para salvaguardar a diversidade regulatória

Embora a natureza "sem fronteiras" da Internet seja uma das suas características distintivas, a geografia – e a localização física dos usuários da Internet - continua a ser relevante para muitos fins. Por exemplo, determinar a localização física de um usuário da Internet pode ajudar aqueles que fornecem resultados de pesquisa direcionados ou publicidade, bem como aqueles que procuram se envolver em segregação de mercado. Isso também pode colaborar para a execução da lei, ajudar na prevenção da fraude e aumentar a segurança cibernética.

As tecnologias de geolocalização e as informações que fornecem também podem ser importantes para fins jurisdicionais. Elas oferecem aos provedores de serviços e conteúdo a oportunidade de personalizar suas ofertas de acordo com as leis aplicáveis no local do usuário da Internet. Elas também oferecem a opção de evitar o contato com usuários de Internet de locais específicos para evitar a exposição às leis aplicáveis nesses locais.

As tecnologias de geolocalização são meios técnicos para determinar a localização física dos usuários da Internet. Elas são, portanto, diversas por definição e incluem técnicas como a dependência de endereços IP, informações Wi-Fi, informações de GPS e triangulação. Hoje, o uso da geolocalização é mais comumente discutido como *geo-blocking* (bloqueio geográfico), embora o bloqueio seja apenas uma função das tecnologias de geolocalização. Além disso, as tecnologias de geolocalização parecem ter ultrapassado a utilização de ccTLDs baseada na diversificação de conteúdo.

As discussões detalhadas sobre o papel que a tecnologia de geolocalização pode desempenhar na jurisdição da Internet remontam à primeira metade dos anos 2000.[655] No conhecido processo francês Yahoo! de 2000 (Capítulo 3.1), o Tribunal concluiu que "na prática, pode estimar-se que mais de 70% dos endereços IP dos usuários residentes em território francês podem ser identificados como sendo franceses."[656] No entanto, em um caso contemporâneo da Suprema Corte de Nova Gales do Sul, a Corte enfatizou que "não havia nenhum meio pelo qual o material, uma vez publicado na Internet, pudesse ser excluído da transmissão ou recebimento em qualquer área geográfica".[657] Tais visões opostas das tecnologias de geolocalização – com alguns tribunais enfatizando o papel das tecnologias de geolocalização e outros ignorando-o completamente – persistem até hoje. Vários tribunais e legisladores hoje em dia consideram as tecnologias de geolocalização como algo garantido e, de fato, enfatizam a importância de seu uso. Por exemplo, no caso *Plixer International Inc. v Scrutinizer GmbH*, de setembro de 2018, um tribunal dos EUA enfatizou que a empresa alemã em questão poderia ter projetado seu site para não interagir com usuários dos EUA. Rejeitou igualmente a alegação da empresa alemã de que o tribunal não deveria considerar se um réu bloqueia o acesso ao seu site, uma vez que, na opinião da empresa, o software de bloqueio de acesso é uma tecnologia imperfeita.[658]

O TJUE, contudo, tem uma longa tradição de ignorar as tecnologias de geolocalização.[659] Ainda em 2017, tanto o Tribunal de Justiça como o advogado-geral Bobek sublinharam "a natureza ubíqua das informações e conteúdos colocados on-line em um site e o fato de o âmbito da sua distribuição ser, em princípio, universal".[660] Esta declaração ignora claramente o papel que as tecnologias de geolocalização podem ter na limitação da distribuição geográfica dos conteúdos on-line.

Este raciocínio chama a atenção para uma questão mais ampla. Para chegar às suas conclusões, tanto o advogado-geral Bobek quanto o Tribunal de Justiça basearam-se numa avaliação da tecnologia da Internet realizada em 2011. Ao decidir um caso em 2017, um tribunal não deve ser guiado por uma avaliação do Estado da tecnologia feita há seis anos. Em vez disso, ao avaliar as taxas de precisão da tecnologia de geolocalização, é importante estar ciente de que elas são:

1. temporais;
2. localizadas; e
3. contextualizadas.

Consequentemente, os tribunais devem proceder a tais apreciações caso a caso e não ser desviados por estimativas feitas em decisões anteriores ou em contextos diferentes.[661]

Em setembro-outubro de 2019, o TJUE abordou dois casos diretamente relacionados com o papel das tecnologias de geolocalização.[662] Nos seus Pareceres, o Advogado Geral Szpunar enfatizou o papel das tecnologias de geolocalização.[663]

Quanto ao papel das tecnologias de geolocalização, o TJUE no Processo C-507/17 enfatizou o seu uso e concluiu que: "cabe ao operador do motor de busca tomar, se necessário, as medidas indispensáveis e suficientemente eficazes para assegurar a proteção efetiva dos direitos fundamentais da pessoa a quem os dados dizem respeito. Essas medidas devem elas próprias cumprir todos os requisitos legais e ter o efeito de impedir ou, no mínimo, desencorajar seriamente os utilizadores da Internet nos Estados-membros de acessarem os links em questão utilizando uma pesquisa efetuada com base no nome da pessoa em causa".[664]

Ao mesmo tempo, o uso de tecnologias de geolocalização é severamente restringido por um Regulamento da UE em vigor desde 3 de dezembro de 2018 e que faz parte da Estratégia do Mercado Único Digital da UE.[665]

O Regulamento de Geo-bloqueio procura endereçar o "bloqueio geográfico injustificado e outras formas de discriminação baseadas na nacionalidade, local de residência ou local de estabelecimento dos clientes no mercado interno". É digno de nota que o Regulamento se justifica principalmente por referência aos males da discriminação com base na nacionalidade, local de residência ou local de estabelecimento do cliente; no entanto, visa ao geo-bloqueio que, pela sua própria natureza, não pode reconhecer a nacionalidade, o local de residência ou o local de estabelecimento. A localização pode servir apenas como uma procuração não confiável da nacionalidade, do local de residência ou do local de estabelecimento.

O Regulamento de Geo-bloqueio delineia três circunstâncias específicas sob as quais o uso de geo-bloqueio não pode ser justificado:

- A venda de mercadorias sem entrega física.
- A venda de serviços fornecidos eletronicamente, que não

sejam aqueles que prioritariamente dão acesso a obras protegidas por direitos autorais ou outros assuntos protegidos (incluindo a venda de obras protegidas por direitos autorais ou assuntos protegidos de uma forma intangível).
- A venda de serviços prestados em um local físico específico.[666]

O Regulamento também proíbe o bloqueio do acesso a websites e a utilização de reencaminhamento automático se o cliente não tiver dado o seu consentimento prévio.

> **É de se esperar que a forma como a legislação da UE se desenvolve sobre o tema da geolocalização influencie outras jurisdições.**

A tensão entre os objetivos políticos perseguidos pelo Regulamento de Geo-Bloqueio e os que levaram o Advogado-Geral Szpunar a realçar a utilização das tecnologias de geolocalização não se limita ao contexto da UE. É de se esperar que a forma como a legislação da UE se desenvolve sobre o tema da geolocalização influencie outras jurisdições.

Este resultado da pesquisa foi distribuído de forma relativamente equitativa do ponto de vista geográfico, embora diferentes grupos de atores tenham expressado uma divergência significativa em atitudes.

Enquanto os atores da academia e da sociedade civil foram predominantemente positivos sobre o papel da geolocalização, a comunidade técnica foi esmagadoramente negativa.

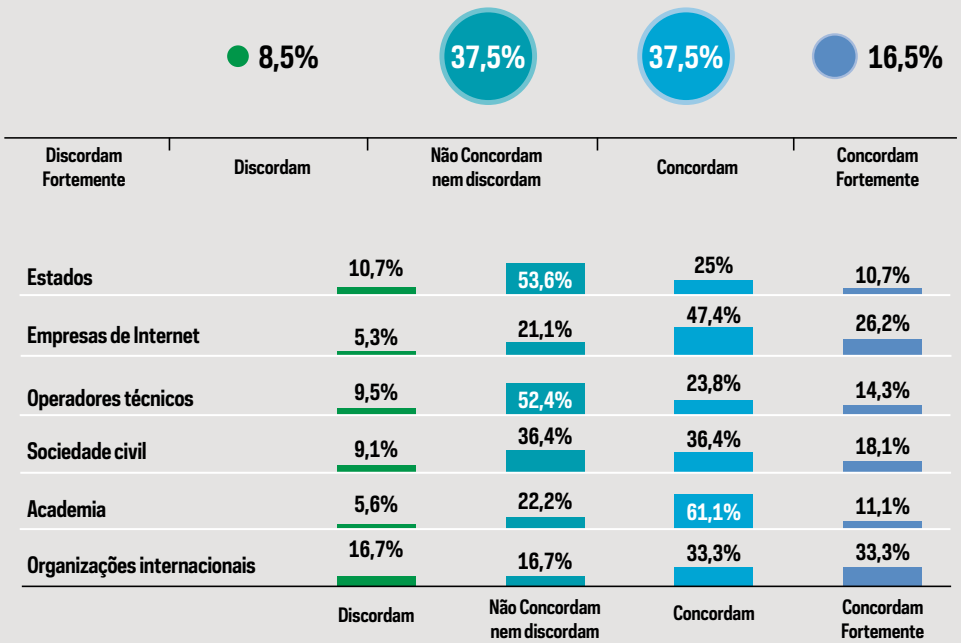
Nos comentários de especialistas pesquisados, destacaram-se três temas recorrentes. A primeira é que as tecnologias de geolocalização podem ser facilmente ignoradas. Um entrevistado, por exemplo, observou que as redes privadas virtuais (VPNs) são muito prevalentes, baratas, fáceis de usar e eficazes para que as tecnologias de geolocalização sejam uma técnica verdadeiramente poderosa para determinar quais usuários bloquear.

ATITUDES DIVERGENTES DOS ATORES EM RELAÇÃO ÀS TECNOLOGIAS DE GEOLOCALIZAÇÃO

Foi apresentada aos especialistas pesquisados a declaração de que a geolocalização, usada por plataformas de Internet ou provedores de conteúdo para bloquear o acesso a conteúdo de certos países, é uma ferramenta eficaz para garantir o cumprimento da legislação nacional localmente, sem recorrer à exclusão, remoção, bloqueio, etc. globais. Entre os entrevistados, 5% "concordaram fortemente" com a afirmação, enquanto 29,5% "concordaram". Apenas 1% "discordaram fortemente", 29,5% "discordaram" e 35% "não concordaram nem discordaram".

INFOGRÁFICO 13

OS DESAFIOS JURÍDICOS TRANSFRONTEIRIÇOS NA INTERNET CONSTITUEM UM OBSTÁCULO SIGNIFICATIVO PARA OS PAÍSES EM DESENVOLVIMENTO?



FONTE: REDE DE POLÍTICAS INTERNET & JURISDIÇÃO: INTERNET & JURISDIÇÃO: RELATÓRIO DE STATUS GLOBAL 2019

VPNs E ANONIMIZADORES – UMA "FACA DE DOIS GUMES"

As VPNs e os anonimizadores são frequentemente discutidos no contexto de desafios jurídicos transfronteiriços na Internet. Sua capacidade de atender à evasão das tecnologias de geolocalização ganhou especial atenção. São também frequentemente discutidos no contexto da sua capacidade de proteger a identidade e a localização física reais dos usuários da Internet, a fim de proteger a privacidade.

Um especialista entrevistado destacou o papel do anonimato como protetor dos direitos humanos em regimes autoritários. Tecnologias como VPNs devem, portanto, ser avaliadas não apenas como ferramentas de contornar o geo-bloqueio, mas como ferramentas de liberdade de expressão.

As VPN e os anonimizadores são verdadeiramente "facas de dois gumes", na medida em que, embora possam ser utilizados por criminosos para evitar serem levados à justiça, são também instrumentos essenciais para os defensores dos direitos humanos em regimes repressivos - e, na verdade, para o usuário médio da Internet que procura manter certo grau de privacidade ao ligar-se a uma rede Wi-Fi pública.

Em algumas partes do mundo, como Dubai, apenas VPNs licenciados pelo Estado são permitidas. Alguns países banem as VPNs completamente. Por exemplo, em 1º de novembro de 2017, por exemplo, a Lei Federal nº 276-FZ - que proíbe o uso de VPNs e outras ferramentas técnicas para contornar restrições de acesso a sites - entrou em vigor na Rússia.[667] A lei proíbe que os mecanismos de busca exibam resultados contendo informações sobre, ou links para, sites bloqueados e dá poderes à agência reguladora de telecomunicações da Rússia, Roskomnadzor, para exigir que ISPs para identificar os proprietários de ferramentas de evasão.[668]

Além disso, em 31 de março de 2018, entrou em vigor na China uma proibição de VPNs não sancionadas pelo Estado.[669] A medida foi anunciada em janeiro de 2017 e, em julho do mesmo ano, o Ministério da Indústria e Tecnologia da Informação da China (MIIT) ordenou que os operadores governamentais de telecomunicações bloqueassem as VPNs até fevereiro de 2018. O engenheiro-chefe do MIIT, Zhang Feng, especificou que as empresas estrangeiras que pretendam criar uma operação transfronteiriça para uso privado terão de criar uma linha dedicada para esse efeito, que pode ser legalmente alugada junto da agência de importação e exportação de telecomunicações.[670]

Embora seja verdade que a evasão através de VPNs prejudica a precisão das tecnologias de geolocalização, tal evasão normalmente requer intenção. Em outras palavras, o uso de ferramentas de evasão normalmente pressupõe uma consciência de que conteúdo pode ser acessado usando essas ferramentas. Isso limita severamente o impacto real das VPNs em muitos casos.

Um especialista entrevistado salientou ainda a importância de distinguir entre as questões da eficiência técnica, por um lado, e a adequação jurídica, por outro. Enquanto descrevendo a geolocalização como algo eficaz no sentido técnico, este entrevistado considerou que as tecnologias de geolocalização deveriam ser consideradas juridicamente adequadas, dadas as considerações gerais, como a cortesia e a margem de apreciação dos direitos humanos. Isso ilustra uma diferença de pensamento entre os entrevistados, com alguns pensando principalmente na eficiência técnica das tecnologias de geolocalização e outros focando na adequação jurídica dessas tecnologias. Isto poderia explicar a diferença de atitudes observadas em diferentes grupos de atores.

Um segundo tema recorrente é que as tecnologias de geolocalização podem impactar negativamente a liberdade de expressão on-line e que os usuários da Internet podem nem sequer estar cientes de que a sua liberdade de expressão e acesso à informação são afetados.

O terceiro tema recorrente é que, embora as tecnologias de geolocalização não sejam uma forma infalível para as plataformas de Internet assegurarem o cumprimento das leis locais, elas ainda são preferíveis à eliminação da lista, remoção e bloqueio globais na maioria das circunstâncias.

Além desses três temas principais, os especialistas pesquisados comentaram que as tecnologias de geolocalização devem ser aplicadas cuidadosamente para limitar o número de falsos negativos e evitar afetar negativamente o desempenho do DNS. Um especialista pesquisado também observou que, embora o uso de tecnologias de geolocalização para bloquear o acesso a conteúdo de certos países possa funcionar muito bem para conteúdo pago de mídia,[671] ele impõe custos para a maioria do conteúdo gratuito e não está claro quem deve cobrir esses custos.

Em última análise, é impossível avaliar a conveniência das tecnologias de geolocalização sem um contexto. Essa deter-

minação deve, em vez disso, ser realizada como um exercício comparativo, sempre que as vantagens e desvantagens sejam comparadas com as de alternativas relevantes. Ao comparar uma Internet baseada em um amplo uso de tecnologias de geolocalização com uma Internet aberta, global e irrestrita, muitos podem favorecer esta última. No entanto, essa Internet utópica não existe hoje e talvez nunca tenha existido.

Portanto, parece mais realista e mais relevante comparar uma Internet baseada em um amplo uso de tecnologias de geolocalização com uma caracterizada por bloqueio, remoção e exclusão globais com base em reivindicações de jurisdição – em outras palavras, uma Internet onde o único conteúdo que permanece on-line é aquele que não ofende nenhuma lei em nenhum lugar do mundo. Nesta última comparação — como sugerido em comentários de especialistas pesquisados — uma Internet baseada no uso extensivo de tecnologias de geolocalização pode talvez ser favorecida devido ao seu potencial de manter o mundo conectado, ao mesmo tempo em que permite a diversidade regulatória.

Nos domínios da privacidade dos dados e da cibersegurança, é comum falar de privacidade e segurança desde a concepção *(by design)*, respectivamente. Olhando para o futuro, talvez um aumento no uso adequado de tecnologias de geolocalização possa ser descrito como "interoperabilidade jurisdicional desde a concepção" – ou seja, interoperabilidade jurisdicional, na forma de conformidade com leis locais diversas e potencialmente conflitantes, que é mais claramente incorporada em projetos técnicos.

4.2.2. Filtragem de conteúdos na rede em nível nacional

O bloqueio e a censura têm implicações óbvias e profundas para a Internet transfronteiriça. Contribuem para a fragmentação e sugerem que a Internet não é tão sem fronteiras quanto parece. No entanto, em comparação com reivindicações de âmbito global de jurisdição feitas para garantir que o conteúdo seja bloqueado, eliminado ou removido de lista na Internet como um todo, a filtragem de conteúdo no nível da rede nacional tem um impacto mais limitado.

As tecnologias de geolocalização discutidas na seção acima não devem ser confundidas com a filtragem de conteúdo na

rede nacional — do tipo realizado, e mais famoso, através do chamado "Grande Firewall da China". Ao bloquear o acesso a conteúdo e sites estrangeiros selecionados, a Grande Muralha engloba as restrições legislativas e técnicas que o governo chinês usa para regular a Internet internamente. Estruturas semelhantes foram adotadas e testadas em vários outros Estados com governos repressivos que mantêm atitudes hostis em relação ao tipo de liberdade de expressão que é desfrutada em outro lugar.[672] Além disso, há esforços de empresas chinesas para exportar parte da funcionalidade da Grande Muralha para outros países, dos quais nem todos têm governos repressivos.

4.2.3. Sistema de Nomes de Domínio: suspensão, supressão, não resolução, apreensão e transferência ordenadas por tribunais

O sistema de nomes de domínio (DNS), como um sistema de endereçamento, é uma camada técnica neutra, vital para o bom funcionamento da Internet. No entanto, os pedidos transfronteiriços de suspensão de nomes de domínio são cada vez mais enviados aos operadores técnicos relativos a conteúdos ou atividades alegadamente abusivas nos sites subjacentes.

Do ponto de vista dos requerentes, o recurso a tais pedidos é óbvio - a suspensão do domínio tem, por definição, um impacto global instantâneo. Ao mesmo tempo, esse potencial de impacto global instantâneo significa que os pedidos de suspensão de nome de domínio só devem ser considerados quando se pode determinar de forma confiável que um domínio é usado com uma intenção clara de conduta abusiva significativa; apenas um nível particularmente elevado de abusos e/ou prejuízos poderia justificar o recurso a tal medida. Esses pedidos devem também ser moldados com amplas garantias processuais para todas as partes envolvidas. A proteção do núcleo da Internet — incluindo o DNS — é, e deve ser, uma prioridade fundamental. Isto compromete a utilização dos pedidos de suspensão de nomes de domínio como ferramenta para combater conteúdo abusivo ou atividade em sites subjacentes.

A proteção do núcleo da Internet — incluindo o DNS — é, e deve ser, uma prioridade fundamental.

Para garantir a proteção do DNS, é importante ter uma grande compreensão dos impactos de ações específicas no nível do DNS. No entanto, especialistas entrevistados observaram que o DNS é mal compreendido e que sua complexidade é muitas vezes subestimada. Por exemplo, há uma incapacidade generalizada de apreciar as diferentes estruturas dos domínios de topo genéricos (gTLDs) e dos domínios de topo de código de país (ccTLDs). Isso resulta em uma subapreciarão das distinções fundamentais entre a forma como a estrutura da Internet Corporation for Assigned Names and Numbers (ICANN) e as leis ou autoridades nacionais se aplicam a diferentes entidades que recebem solicitações de suspensões de nomes de domínio.

Em uma observação espirituosa, um especialista entrevistado observou que tentar usar a camada de protocolo para afetar um resultado desejado na camada de aplicação é como tentar prevenir o tráfico de drogas nas rodovias, regulando os fabricantes de asfalto para retardar os veículos. O especialista entrevistado acrescentou que, embora seja verdade que veículos portadores de drogas seriam retardados, os traficantes encontrariam modos alternativos de transporte, enquanto o dano causado a outros veículos (inocentes) seria extenso. Embora a capacitação ocorra nesta esfera, a arquitetura de domínio está se tornando cada vez mais complexa. Isso ocorreu devido ao comportamento de ccTLDs como gTLDs, bem como a introdução de novos gTLDs.

Todos os atores são confrontados com os mesmos desafios: definir quando seria apropriado agir no nível do DNS em relação ao conteúdo ou comportamento de um endereço de domínio e identificar as respectivas funções que os tribunais e os chamados “notificadores” devem exercer. Estes assuntos são examinados em um dos três Programas Temáticos da Rede de Políticas Internet & Jurisdição.

PROGRAMA DE DOMÍNIOS E JURISDIÇÃO

Os atores da Rede de Políticas Internet & Jurisdição trabalham em conjunto em três programas de políticas: o Programa de Dados e Jurisdição, o Programa de Conteúdo e Jurisdição e o Programa de Domínios e Jurisdição. Os Programas permitem que os membros coordenem informalmente políticas e desenvolvam conjuntamente propostas de Normas, Critérios e Mecanismos operacionais. O Programa de Domínios e Jurisdição atualmente se concentra em definir em uma base temática sob cujas condições estritas podem ser previstas interrupções de um nome de domínio sem o consentimento do registrante; quais ações os operadores de nomes de domínio devem ou estariam dispostos e capazes de exercer; que regras e procedimentos podem ajudar a estabelecer ou reforçar a credibilidade das notificações dos notificadores (para fins de informação ou ação) e quais os mecanismos que podem contribuir para melhorar a transparência desses processos.

O trabalho atual do Programa de Domínios e Jurisdição baseia-se no Roteiro de Ottawa da Rede de Políticas Internet & Jurisdição, que produziu propostas concretas para Normas, Critérios e Mecanismos operacionais em 2019.[673] Ele aborda as seguintes questões:

- Padrões – Taxonomia e limiares relevantes de ação para cada tipo de comportamento e conteúdo abusivo.
- Ordens judiciais – O papel das ordens judiciais, incluindo o seu alcance territorial, a sua eficácia e a sua proporcionalidade.
- Notificações – Critérios relevantes para avaliar a credibilidade de uma notificação, sendo a fonte (ou seja, o notificador) apenas um elemento.
- Devida diligência – Os procedimentos que notificadores devem, idealmente, seguir antes de enviar notificações e o conteúdo de seus pedidos.
- Garantias processuais – Proteções para os registrantes (notificação e procedimento contraditório, proporcionalidade).
- Reparação – Mecanismos de recurso e precauções técnicas que permitem a reparação.
- Validação de pedidos – Opções para certificação de notificações.
- Responsabilidade – Potenciais proteções para os operadores quando é realizada a devida diligência.
- Transparência – Mecanismos para garantir a transparência adequada, nomeadamente no que diz respeito à forma como os operadores lidam com as notificações e à forma como os notificadores asseguram o devido processo antes da notificação.
- Educação – Informações acessíveis e de alta qualidade para legisladores, tribunais e autoridades responsáveis pela execução da lei, a fim de evitar consequências indesejadas das decisões, bem como para os usuários finais, que podem desempenhar um papel crucial na prevenção de abusos.
- Ferramentas – Software e/ou procedimentos para permitir medidas efetivas, proporcionais e escaláveis.

4.2.4. Sistema de Nomes de Domínio: bloqueios de DNS, de endereços IP ou redirecionamento e bloqueio de URL ordenados por tribunais

O bloqueio de DNS é uma abordagem que se relaciona com a suspensão, exclusão, não resolução, apreensão e transferência de nomes de domínio discutidos acima. Uma ordem de bloqueio de DNS normalmente requer um ou vários ISPs para implementar um sistema que desabilita o acesso a um ou vários "locais on-line de destino".

Este procedimento é exemplificado em um Acórdão 2018 do Tribunal Federal da Austrália.

Em *Roadshow Films Pty Limited v Telstra Corporation Limited*, o tribunal ordenou que um grupo de ISPs tomasse medidas para impedir o acesso a um grande número de sites. O tribunal especificou que, para dar cumprimento a esta decisão, os ISPs teriam de implementar uma ou mais das seguintes medidas:

> *(a) Bloqueio de DNS no que diz respeito aos Nomes de Domínio de Destino;*
> *(b) Bloqueio de Endereço IP ou reencaminhamento no que diz respeito aos endereços IP de destino;*
> *(c) Bloqueio de URL em relação aos URLs de Destino e aos Nomes de Domínio de Destino; ou*
> *(d) Quaisquer meios técnicos alternativos para desabilitar o acesso ao Local de Destino on-line conforme acordado por escrito entre os Demandantes e um Demandado.*[674]

Tal como as suspensões ordenadas pelo tribunal e a exclusão, não resolução, apreensão e transferência de nomes de domínio, este tipo de ordem é controverso.

O risco de discriminação e de bloqueio excessivo é óbvio e existem questões claras de responsabilidade, remédio e reparação. Um especialista entrevistado chamou a atenção para um caso de alta visibilidade de bloqueio excessivo ocorrido em 2016, quando o ISP francês Orange bloqueou erradamente o tráfego para o Google, Wikipédia e vários outros sites para seus 11 milhões de clientes de linha fixa.[675] Essas questões crescerão nos casos em que o bloqueio é complementado por algoritmos e inteligência artificial. No entanto, há áreas em que essas ordens podem receber apoio. Por exemplo, um especialista entrevis-

tado observou que os requisitos para bloquear URLs fraudulentos ou aqueles que automaticamente instalam *malware*, na verdade, deveriam ser globais.

> **O risco de discriminação e de bloqueio excessivo é óbvio e existem questões claras de responsabilidade, remédio e reparação.**

4.2.5. Paralisação de serviço

Os governos frequentemente ameaçam paralisar serviços específicos da Internet e, em algumas ocasiões, essas ameaças são efetivamente levadas a cabo. Quando isso acontece, e o prestador de serviços é uma empresa local, a questão é em grande parte interna. No entanto, surgem impactos transfronteiriços se o prestador de serviços for uma empresa estrangeira, o que muitas vezes acontece. As situações em que um prestador de serviços nacional está bloqueado podem também ter dimensões transfronteiriças. Esse serviço, por exemplo, pode ter usuários em outros países afetados e pode haver várias obrigações internacionais.

No entanto, apesar das graves implicações de tais medidas, os serviços são frequentemente bloqueados e as paradas de serviços ocorrem em todo o mundo:

- A **China** bloqueia regularmente vários serviços e sua censura é particularmente rigorosa em torno de datas de significado histórico.[676] Por exemplo, os sites de 12 importantes veículos de notícias internacionais de cinco países diferentes foram bloqueados especificamente no período que antecedeu o 30º aniversário do massacre da Praça Tiananmen.[677]
- Em **julho de 2019**, o governo do **Chade** levantou uma proibição de 16 meses sobre mídias sociais que o governo declarou ser necessária por razões de segurança.[678]
- Em **29 de maio de 2018**, o ministro das Comunicações da **Papua Nova Guiné** (PNG), Sam Basil, anunciou que o país iria bloquear o acesso ao Facebook por um mês, a fim de coletar informações para identificar, filtrar e remover usuários que se escondem atrás de contas falsas, carregam imagens pornográficas ou publicam informações falsas e enganosas no Facebook. O Ministro citou a Lei de Crimes Cibernéticos de 2016 como base para o bloqueio e mencionou que o governo também estava "verificando a possibilidade de criar um novo site de rede social para cidadãos da PNG com perfis verdadeiros."[679]
- Em **26 de maio de 2018**, o tribunal administrativo superior do Egito decidiu que o YouTube deveria ser bloqueado por um mês devido à "Inocência dos Muçulmanos", um vídeo anti-islâmico de 2012 que provocou protestos no Oriente Médio após o seu lançamento.[680] Uma esfera inferior da administração havia ordenado o bloqueio em 2013, após o qual o caso foi alvo de apelações até a decisão de 26 de maio de 2018.[681]
- Em **13 de abril de 2018**, um tribunal russo ordenou que o acesso ao serviço de mensagens Telegram fosse bloqueado na Rússia, seguindo repetidas recusas da plataforma de entregar suas chaves de criptografia para o FSB, a agência de segurança russa.[682] Isso foi recebido com considerável oposição.[683] Poucos dias depois, em **17 de abril de 2018**, Roskomnadzor solicitou que o Google e a Apple removessem o Telegram de suas lojas de aplicativos. No mesmo dia, o regulador anunciou que havia bloqueado milhões de endereços IP pertencentes a Amazon Web Services e Google Cloud, em uma tentativa de bloquear o acesso ao Telegram. Isso resultou em interrupções de outros serviços, incluindo o mecanismo de pesquisa e o serviço de e-mail.[684]
- Em **8 de março de 2018**, o governo do **Sri Lanka** ordenou aos ISPs que bloqueassem temporariamente o acesso ao Facebook, WhatsApp e Instagram porque eles estavam espalhando e amplificando o discurso de ódio em meio a protestos

violentos no país, de acordo com um porta-voz do governo.[685] A proibição foi suspensa uma semana depois, após reuniões entre autoridades do Sri Lanka e representantes da plataforma.[686] As mídias sociais e os aplicativos de mensagens foram novamente bloqueados temporariamente pelo governo do Sri Lanka em **abril de 2019** para evitar desinformação e incitação à violência na esteira de ataques terroristas.[687]

- Em **8 de novembro de 2017**, o Ministério das Comunicações da Indonésia anunciou que iria lançar, em **janeiro de 2018**, um sistema automatizado para sinalizar e bloquear sites ou serviços de mensagens exibindo pornografia ou conteúdo extremista.[688] O governo também afirmou que iria convocar executivos de serviços de mensagens e motores de busca para exigir que eles moderassem conteúdo obsceno. O anúncio seguiu-se à ameaça do governo indonésio de proibir o WhatsApp se este não bloqueasse GIFs obscenos na sua plataforma.[689] Em **maio de 2019**, o governo indonésio restringiu temporariamente o acesso a plataformas de mídia social, incluindo Facebook, WhatsApp e Instagram, buscando evitar informações erradas e provocação após motins violentos em Jacarta.[690]
- Em **6 de setembro de 2017**, foi noticiado que o acesso ao Facebook e ao WhatsApp era difícil em **Togo**, antes de toda a Internet móvel supostamente ter sido fechada.[691] Após a restauração do serviço, o WhatsApp foi novamente bloqueado, pois as velocidades de conexão diminuíram em **19 de setembro de 2017**. As restrições de acesso à Internet vieram em meio à intensificação de protestos contra o governo no país. [nota692]
- Em **12 de maio de 2017**, a Comissão Nacional de Radiodifusão e Telecomunicações (NBTC) da **Tailândia** ameaçou bloquear o Facebook a menos que a empresa sediada nos EUA removesse 130 postagens 'ilegais'.[693] A demanda veio após a Associação de Prestadores de Serviços de Internet da Tailândia (TISPA), que representa 95% do tráfego de Internet no país, supostamente ter solicitado que o Facebook Tailândia restringisse o acesso a conteúdo com críticas à monarquia.[694]
- Em **5 de maio de 2017**, um tribunal turco em Ancara rejeitou um recurso da Wikimedia Foundation contra um bloqueio da Wikipédia em sua jurisdição.[695] Em **29 de abril**, a autoridade turca de telecomunicações, BTK, anunciou que a Wikipédia seria bloqueada através de uma medida administrativa citando a lei n.º 5651, que regula o conteúdo on-line na Turquia. Após o bloqueio, o Ministério das Comunicações Turco afirmou que a Wikipédia tinha sido parte de uma campanha difamatória contra a Turquia na arena internacional. Na sua decisão, os juízes do tribunal de Ancara foram citados como tendo dito que, embora a liberdade de expressão seja um direito fundamental, ela pode ser limitada nos casos em que há uma "necessidade de regulação".[696] Após esta decisão judicial, a Wikipédia anunciou em **9 de maio** que havia peticionado ao tribunal constitucional turco após sua apelação ter sido rejeitada.[697] A proibição continuou e, em maio de 2019, a Wikimedia peticionou ao Tribunal Europeu dos Direitos do Homem para anular a proibição de 2 anos.[698]

Em algumas ocasiões, as razões para bloquear uma plataforma em um determinado momento não são totalmente transparentes. Por exemplo, em 25 de novembro de 2017, o Twitter afirmou que o governo paquistanês havia tomado medidas para bloquear seu serviço, bem como outros serviços de mídia social.[699] Os motivos por trás do bloqueio não eram claros, embora alguns veículos de notícias o tenham vinculado aos protestos islâmicos em Islamabad.[700] Da mesma forma, em 25 de setembro de 2017, mensagens de texto enviadas através do WhatsApp foram bloqueadas na China, após bloqueios parciais de imagens e vídeos em julho de 2017.[701] Embora as razões para o bloqueio não fossem claras, os noticiários observaram que a decisão veio antes do 19º Congresso Nacional do Partido Comunista Chinês, um grande evento político que começou em 18 de outubro de 2017.[702] Há também variações nas etapas processuais necessárias para que um serviço possa ser bloqueado ou encerrado. Por exemplo, em 14 de junho de 2018, a Assembleia Nacional da Bielorrússia alterou a lei de mídia do país, introduzindo um requisito para que os autores de todos os posts e comentários on-line se identifiquem e se registrem. O governo poderá bloquear plataformas de mídia social sem a necessidade de uma ordem judicial. As plataformas de mídia também devem se registrar no Registro de Informações; os meios de comunicação não registrados não desfrutarão das proteções concedidas à imprensa.

4.2.6. Desligamentos da Internet

Em alguns casos extremos, os governos optaram por encerrar o acesso à Internet inteiramente dentro de países específicos. Mesmo que sejam temporários, tais desligamentos de Internet são fundamentalmente opostos à ideia de uma Internet global. Afinal de contas, os desligamentos da Internet afetam não só as pessoas no país onde ocorre o desligamento, mas também qualquer pessoa de fora que tente se comunicar com pessoas ou instalações nesse país. Além disso, se uma empresa estrangeira investiu no mercado em questão, um desligamento da Internet pode ter efeitos devastadores. Isto é especialmente verdadeiro se a empresa estrangeira tiver decidido localizar seus dados nesse país, voluntária ou involuntariamente. Neste contexto, os desligamentos da Internet constituem um obstáculo óbvio à atração de empresas e investimentos estrangeiros.

Exemplos de desligamentos da Internet são abundantes. Em janeiro de 2019, a Internet foi temporariamente desligada no Zimbábue,[703] tendo sido restaurada após uma ordem judicial declarando que o governo do Zimbábue excedeu seu mandato ao ordenar um apagão na Internet durante os protestos civis.[704] Da mesma forma, após as eleições gerais de 30 de dezembro de 2018, foi relatado que o acesso à Internet fora restrito na República Democrática do Congo (RDC).[705] Um porta-voz da Presidência da RDC indicou que o acesso à Internet, bem como os serviços SMS, haviam sido interrompidos depois que "resultados fictícios" começaram a aparecer.[706]

Em 12 de dezembro de 2017, o governo etíope bloqueou parcialmente o acesso à Internet à medida que os protestos estudantis se tornaram violentos na região de Oromia.[707] A Etiópia restringiu repetidamente o acesso à Internet nos últimos anos, e apenas um ISP, que é propriedade do Estado, opera atualmente no país.[708] O final de 2017 também viu um longo período de restrições ao acesso à Internet nas regiões anglófonas dos Camarões.[709] O bloqueio foi promulgado em 1º de outubro de 2017, com protestos nas regiões anglófonas sobre uma percepção de falha na defesa dos direitos da minoria de língua inglesa. Um bloqueio anterior no mesmo ano foi levantado após mais de três meses, tendo durado de janeiro a abril de 2017. [710] Outros exemplos recentes em 2019 de paralisações da Internet como forma de reprimir os protestos e impedir a disseminação de informações incluem o desligamento do acesso à Internet por parte do governo indiano na Caxemira, [711] o bloqueio do acesso pelo governo argelino[712] e também pelos militares do Sudão no poder em resposta a protestos pacíficos.[713] Benim também sofreu um desligamento da Internet em 28 de abril de 2019, no dia de eleições legislativas.[714]

Apesar da prevalência de desligamentos da Internet, há um reconhecimento generalizado de que as paradas da Internet têm um sério impacto negativo. Por exemplo, em 2 de junho de 2017, as Organizações Africanas para a Governança da Internet (AF*), que inclui a AFRINIC e outras organizações africanas da Internet, divulgaram um comunicado criticando o número crescente de desligamentos da Internet ordenados por Governo na África e chamando a atenção para os seus efeitos negativos.[715] A declaração também criticou uma política, proposta

pela AFRINIC em abril, para restringir o acesso a novos endereços IP para os governos que se envolvem em desligamentos da Internet, que a AFRINIC formalmente retratou durante a 5ª Cúpula da Internet Africana.[716]

Da mesma forma, o Conselho de Direitos Humanos das Nações Unidas salientou repetidamente que:

Condena medidas inequívocas para prevenir ou interromper intencionalmente o acesso ou a divulgação de informações on-line em violação ao direito internacional dos direitos humanos e apela a todos os Estados para que se abstenham e cessem tais medidas.[717]

Os entrevistados destacaram iniciativas que buscam informar melhor os impactos dos desligamentos da Internet, incluindo a Ferramenta Custo de Desligamento desenvolvida pela Internet Society e Netblocks, que é uma ferramenta on-line de acesso livre para medir o custo econômico dos desligamentos da Internet.[718] A Access Now também publicou seu Relatório *#keepiton* em 2018, que mostra tendências recentes de desligamentos da Internet e destaca que eles estão em ascensão.[719]

4.2.7. Localização obrigatória dos dados

Tal como se vê no capítulo que descreve as principais tendências atuais (Capítulo 3), os requisitos de localização forçada de dados estão se tornando uma abordagem amplamente adotada — e, segundo se alega, uma solução — para alguns dos desafios jurídicos transfronteiriços na Internet. Esta questão é distinta da localização dos dados enquanto fator de conexão jurisdicional. No entanto, pode ser interessante observar como mais Estados atribuem significado à localização de dados por razões práticas de execução da lei, enquanto o seu significado como um fator de conexão jurisdicional é quase erradicado.

Os exemplos de leis que obrigam a localização de dados são abundantes. Por exemplo, em 10 de setembro de 2018, foi noticiado[720] que o Google tinha concordado em cumprir os requisitos de localização de dados estabelecidos pelo Reserve Bank of India (RBI), o banco central do país. O RBI estabeleceu a data de 15 de outubro de 2018 para que todos os operadores do sistema de pagamento armazenem os dados financeiros dos indianos no território do país.[721] Embora alterações recentes tenham flexibilizado os requisitos, a proposta de lei de proteção de dados pessoais da Índia também incorporou requi-

sitos obrigatórios de localização de dados.[722] Este é apenas um exemplo de uma tendência clara. Um dos exemplos mais conhecidos é encontrado na Lei de Segurança Cibernética da China, que estipula que os dados confidenciais devem ser armazenados internamente.[723] Outro exemplo de requisito de localização de dados é o Regulamento do Governo da Indonésia nº 82 de 2012 sobre a Implementação de Sistemas e Transações Eletrônicas ("GR 82") e, apesar de um período de transição de 5 anos, os operadores têm procurado leniência e mais esclarecimentos do governo sobre os requisitos. O governo está trabalhando em um projeto de emenda à lei.[724]

LOCALIZAÇÃO DE DADOS — PARTE DO PROBLEMA OU PARTE DA SOLUÇÃO?

Quando perguntado se o número crescente de leis que exigem a localização de dados é parte do problema ou parte da solução, 47% dos especialistas pesquisados indicaram que essa tendência é parte do problema. 31% afirmaram que é simultaneamente parte do problema e parte da solução, enquanto 9,5% consideraram que esta tendência não faz parte do problema nem da solução. Apenas 12,5% viram a tendência como parte da solução.

Houve claras diferenças setoriais e regionais entre as atitudes dos especialistas consultados em relação às leis de localização de dados. Embora a amostra regional seja, reconhecidamente, demasiado pequena para constituir a base das conclusões, existem, por si só, evidências qualitativas — incluindo discussões em conferências recentes — que apoiam a conclusão de que a localização dos dados é mais facilmente vista como uma solução entre os países asiáticos do que em outros países.

Talvez não seja surpreendente que países — incluindo países da Ásia — que se sintam sujeitos a uma forma de colonização digital pelos países nos quais estão baseadas as principais empresas de Internet, tenderiam a ter uma visão mais favorável à localização de dados. De outra forma, os países que são principalmente receptores de serviços de Internet podem — correta ou incorretamente — perceber a localização dos dados como uma ferramenta para a equalização de forças.

Em seus comentários, vários especialistas pesquisados expressaram a opinião de que os requisitos de localização de dados representam uma abordagem contundente, datada e inadequada para o problema e que eles refletem uma falha na resolução de questões legais. Um entrevistado apontou para as leis de localização de dados como um sinal de desconfiança em outros sistemas jurídicos; outro enfatizou que tais leis devem ser parcialmente entendidas como uma resposta ao estado atual das coisas, já que a capacidade dos Estados para fazer cumprir suas leis está sendo prejudicada. Um especialista entrevistado apontou preocupações sobre como os dados armazenados fora da jurisdição de um Estado afetarão a soberania desse Estado.

> **Os países que são principalmente receptores de serviços de Internet podem [...] perceber a localização dos dados como uma ferramenta para a equalização de forças.**

Outros levantaram preocupações de que a localização forçada de dados não possui escalabilidade como abordagem e observaram que os requisitos de localização de dados não alteram quem é responsável pelos dados.

Como os especialistas que responderam à pesquisa, os especialistas entrevistados apontaram para várias fraquezas e riscos associados à localização forçada dos dados. Quando imposta amplamente, a localização forçada dos dados é muito dispendiosa para as empresas cumprirem. Isso, observaram os especialistas entrevistados, corre o risco de consolidar a posição e o poder do pequeno número de empresas já estabelecidas que podem pagar e têm o conhecimento jurídico e técnico necessário para cumprir múltiplos requisitos de localização forçada de dados. Isso, acrescentaram, vai sufocar a inovação. Outro especialista entrevistado observou outro aspecto do fator de custo: o grau em que as empresas fora do país decidirão cumprir os requisitos de localização de dados dependerá de seu desejo de se envolver economicamente naquele país.

Um especialista entrevistado observou que os requisitos de localização de dados podem fornecer alguns aumentos de desempenho. Mas o mesmo especialista também apontou para o risco de que, quando impostos por pequenos países, tais requisitos possam simplesmente resultar em que as empresas optem por não

se envolver em seus mercados, resultando em uma falta de acesso a opções de serviço e uma potencial redução do desempenho.

Especialistas entrevistados também observaram que os requisitos de localização forçada de dados por regimes opressivos podem representar riscos para os direitos. Por exemplo, em uma entrevista publicada em 18 de abril de 2018, o chefe da agência reguladora de comunicações russa, *Roskomnadzor,* afirmou que o Facebook poderia ser bloqueado se a plataforma não mostrar conformidade com os requisitos de localização de dados da Rússia.[725] A *Roskomnadzor* já avisara a plataforma de que seria bloqueada, a menos que cumprisse suas regras de localização de dados em setembro de 2017.[726] Em novembro de 2016, o LinkedIn foi bloqueado por se recusar a cumprir as regras. [727] Em abril de 2019, um tribunal russo multou o Facebook e Twitter por não fornecer informações em conformidade com os requisitos de localização de dados.[728]

Finalmente, apesar de toda a atenção direcionada aos requisitos de localização forçada de dados, vale a pena notar que a localização dos dados também ocorre de forma voluntária. Na verdade, uma vez que os dados sempre precisam ser armazenados em algum local físico, escolhas voluntárias de localização de dados são extremamente comuns e são afetadas por uma ampla gama de fatores.

4.2.8. Inteligência Artificial

Inteligência artificial (IA), embora não seja um fenômeno novo, recentemente capturou a atenção de todos os grupos de atores da Rede de Políticas Internet & Jurisdição. Com efeito, é possível argumentar que nenhum outro tópico discutido nesta seção do Relatório transcende, e até unifica, as três áreas de expressão, economia e segurança, como a IA. Consequentemente, o impacto da IA e dos desenvolvimentos técnicos a ela relacionados, como a aprendizagem de máquinas, a tomada de decisões algorítmicas e outras formas de processamento automatizado de dados, são relevantes para várias partes do presente Relatório.

Qualquer discussão sobre a crescente responsabilidade conferida à operação privada (através de leis que tornam as plataformas de Internet os guardiões de conteúdo) devem levar em conta o potencial da IA como moderadora de conteúdo — que

pode ser implementada em vários níveis e por vários atores.[729] Vários especialistas entrevistados previram que os legisladores vão apelar às plataformas para implementar IA para detectar e remover conteúdo ilegal, pelo menos em relação a algumas categorias de ilegalidade. Como isso acontece, questões como vieses algorítmicos, bloqueio excessivo, falta de transparência, falta de direito a recursos e preocupações de responsabilidade já surgiram e só aumentarão em intensidade.[730]

A IA irá transformar a maioria — se não todos — dos aspectos da sociedade. Ela desempenha um papel cada vez mais importante na operação de nossos telefones celulares e sistemas de computador doméstico e na forma como as informações são acessadas e compartilhadas; a IA afeta os tipos de empregos disponíveis e a maneira como os funcionários irão trabalhar nos empregos que forem mantidos; melhora o diagnóstico de saúde; e traz enormes implicações econômicas:

> *A PwC estimou que a IA poderá contribuir com até 15,7 trilhões de dólares para a economia global em 2030, mais do que a produção atual da China e da Índia combinadas. Assim sendo, US$6,6 trilhões provavelmente virão do aumento da produtividade devido à automação de tarefas e funções e 9,1 trilhões de dólares provavelmente virão de melhorias de produtos que estimulam a demanda do consumidor.*[731]

A Inteligência Artificial também pode transformar a arena de segurança nacional. Como foi observado recentemente: "Três dos maiores atores do mundo, EUA, Rússia e China, estão entrincheirados na batalha não cinética para superar o outro no desenvolvimento e implementação de IA."[732]

A IA também apresenta riscos em relação à criação e distribuição de conteúdo on-line indesejável, como discurso de ódio, bullying e *deep fakes*. Há preocupações de que a Inteligência Artificial pode vir a contribuir para a "junkificação da Internet" de uma forma que comprometa o valor da Internet.

Tendo em conta o acima exposto, não restam dúvidas de que a IA terá impacto em muitas, se não na maior parte, das questões discutidas no presente Relatório, devendo ser cuidadosamente acompanhada nos próximos anos.

> **É possível argumentar que nenhum outro tópico discutido nesta seção do Relatório transcende, e até unifica, as três áreas de expressão, economia e segurança, como a IA.**

Alguns dos principais avanços e publicações recentes sobre IA são:

Em **setembro de 2019**, o **Fórum Econômico Mundial** publicou seu Livro Branco intitulado AI Government Guidelines.[733]

Na Reunião Ministerial do **G20** sobre Comércio e Economia Digital, realizada em **junho de 2019**, em Tsubuka, Japão, os Ministros do Comércio e da Economia Digital do G20 aprovaram os Princípios da IA do G20, com foco numa abordagem de IA centrada no ser humano.[734]

A OCDE adotou seus Princípios sobre Inteligência Artificial em **maio de 2019**.[735]

Em **janeiro de 2019**, a Comissão de Proteção de Dados Pessoais de **Singapura** publicou seu Modelo para um Quadro de Governança de IA.[736] A Consulta ocorreu durante o primeiro semestre de 2019.[737] E em **novembro de 2018**, a Autoridade Monetária de Singapura (MAS) lançou um conjunto de princípios para promover a equidade, ética, *accountability* e transparência (FEAT) no uso de inteligência artificial (IA) e análise de dados em finanças.[738]

Em **2018**, 32 organismos/agências da **ONU** e a **UIT** publicaram um relatório intitulado Atividades das Nações Unidas sobre Inteligência Artificial (IA), descrevendo como várias agências da ONU usam tecnologias de IA para alcançar seus objetivos.[739]

Em **dezembro de 2018**, o Grupo de especialistas de Alto Nível em Inteligência Artificial da **Comissão Europeia** publicou seu Projeto de Orientações Éticas para uma IA Confiável.[740] Na sequência de novas consultas, as Orientações revistas foram publicadas em 2019.[741] Em 2019, a UE lançou também a Aliança de IA Europeia, uma plataforma de discussão aberta.[742]

Em **dezembro de 2018**, o **Conselho da Europa** adotou um texto que estabelece os princípios éticos relativos à utilização da inteligência artificial nos sistemas judiciários.[743] O **Conselho da Europa** também criou — em 11 de setembro de 2019 — um Comitê Ad Hoc para a Inteligência Artificial[744] e publicou numerosos relatórios e declarações nos últimos anos, tais como:

- Tirando a IA da caixa: 10 passos para proteger os Direitos Humanos,[745] de **maio de 2019**.
- Declaração do Comitê de Ministros sobre as capacidades manipulativas dos processos algorítmicos[746], de **fevereiro de 2019**.
- Projeto de Declaração do Comitê de Ministros sobre as capacidades manipulativas dos processos algorítmicos[747], de **novembro de 2018**.
- Projeto de Recomendação do Comitê de Ministros aos Estados-Membros sobre o impacto dos sistemas algorítmicos nos direitos humanos,[748] de **novembro de 2018**.
- Um estudo das implicações das tecnologias digitais avançadas (incluindo sistemas de IA) para o conceito de responsabilidade dentro de um quadro de direitos humanos,[749] de **novembro de 2018**.

- Algoritmos e Direitos Humanos: Estudo sobre as dimensões de direitos humanos nas técnicas automatizadas de processamento de dados e possíveis implicações regulatórias,[750] de **dezembro de 2017**.

A **UNESCO** organizou eventos como o Fórum de Inteligência Artificial na África em **dezembro de 2018**.[751]

Em **novembro de 2018**, foi publicada a estratégia de Inteligência Artificial (IA) do Governo Federal **Alemão**.[752]

Fazendo referência específica a agricultura, saúde, serviços públicos e serviços financeiros, um livro branco de **novembro de 2018** da Access Partnership e da Universidade de Pretória fez a seguinte observação: "O conjunto de tecnologias de inteligência artificial (IA) em rápido desenvolvimento tem o potencial de resolver alguns dos desafios mais urgentes que impactam a **África subsaariana** e impulsionam o crescimento e o desenvolvimento em setores centrais".[753] No entanto, em seu relatório de **novembro de 2018** "Coming to Life: Artificial Intelligence in Africa",[754] o Conselho Atlântico observou que:

"Infelizmente, exceto em alguns países — notadamente, **Quênia, África do Sul, Nigéria, Gana e Etiópia** — a aplicação da IA é uma quimera, não uma realidade. Os fatores críticos necessários para que a tecnologia se consolide estão lamentavelmente ausentes na maior parte do continente e muitos países africanos continuam incapazes de realizar as reformas necessárias nas áreas de coleta de dados e privacidade de dados, infraestruturas, educação e governança. Sem essas reformas, há poucas chances de que a maioria das nações africanas seja capaz de explorar tecnologias de IA para promover o desenvolvimento sustentável e o crescimento inclusivo. O espectro da automação ameaça deixar esses países para trás."[755]

Em **novembro de 2018**, a **Access Now** publicou seu relatório sobre Direitos Humanos na Era da Inteligência Artificial.[756]

Em **setembro de 2018**, a World Wide Web Foundation publicou seu relatório intitulado Algoritmos e Inteligência Artificial na **América Latina**.[757]

Em **setembro de 2018**, o Subcomitê de Tecnologia da Informação do Comitê de Supervisão e Reforma do Governo da Câmara dos Representantes dos **EUA** emitiu um livro branco intitulado Rise of the Machines: Artificial Intelligence and its Growing Impact on U.S. Policy (Ascensão das Máquinas: Inteligência Artificial e seu crescente impacto na política dos EUA).[758]

Em **junho de 2018**, a National Institution for Transforming **India** (NITI Aayog) lançou um livro branco sobre o desenvolvimento de uma estratégia nacional abrangente.[759]

A Anistia Internacional e a Access Now lançaram a Declaração de Toronto: Protegendo os Direitos à Igualdade e Não Discriminação em Sistemas de Aprendizagem de Máquina na RightsCon em Toronto, **Canadá** em **maio 2018**.[760]

Em **abril de 2018**, a **ARTICLE 19** e a **Privacy International** publicaram um relatório intitulado Privacidade e Liberdade de Expressão na Era da Inteligência Artificial.[761] A ARTICLE 19 publicou um novo relatório em **abril de 2019** intitulado Governança com Dentes: Como os Direitos Humanos Podem Fortalecer as Iniciativas de FAT e Ética na Inteligência Artificial.[762]

Observou-se que "a **China** tem a capacidade e a oportunidade de liderar a colaboração internacional no desenvolvimento e governança da IA, garantindo que esta tecnologia inovadora contribua positivamente para o bem-estar geral de toda a humanidade".[763] Em **janeiro de 2018**, o Instituto de Padronização Eletrônica da China

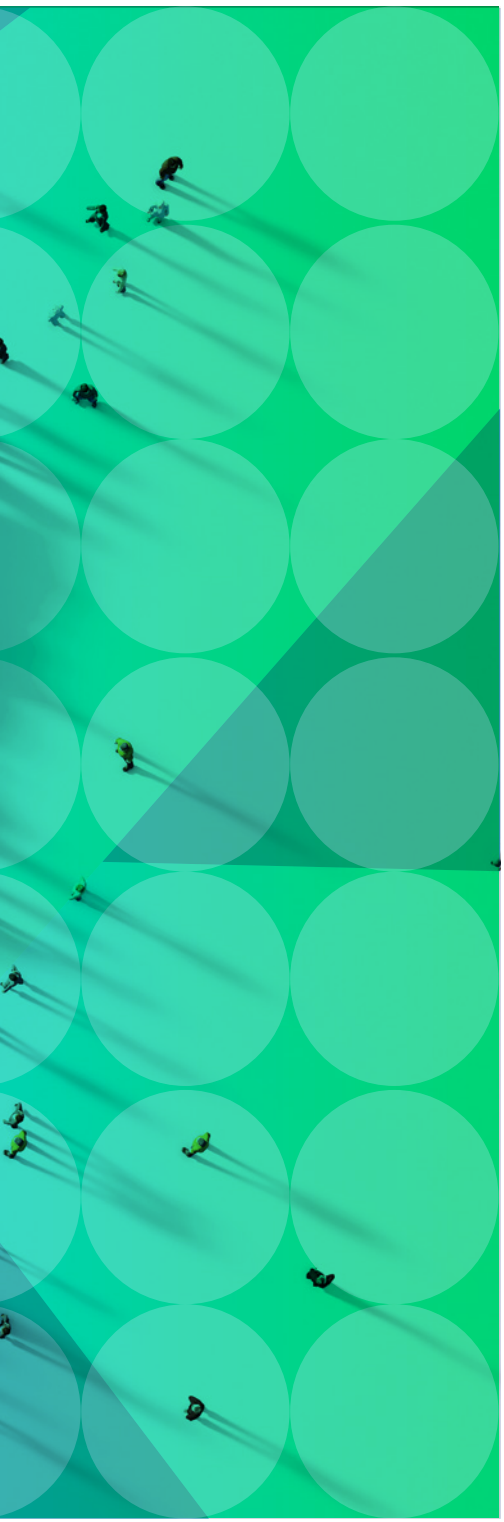
publicou seu livro branco de padronização de Inteligência artificial, "que resume os progressos atuais na tecnologia de IA, processos de padronização em outros países, estrutura de padronização IA na China e plano da China para desenvolver recursos de IA no futuro."[764]

Em **2017**, o Grupo dos Sete (G7) — composto pelo **Canadá, França, Alemanha, Itália, Japão, Reino Unido e EUA** — emitiu sua Declaração dos Ministros da Inovação sobre Inteligência Artificial.[765]

Um relatório do McKinsey Global Institute de **2017** observou que: "A **China** e os **Estados Unidos** são atualmente os líderes mundiais no desenvolvimento de IA. Só em 2015, eles responderam por quase 10.000 artigos sobre IA publicados em revistas acadêmicas, enquanto o **Reino Unido, Índia, Alemanha e Japão** se uniram para produzir apenas cerca de metade dos artigos de pesquisa acadêmica". [766]

Em **outubro de 2017**, os **Emirados Árabes Unidos** lançaram uma estratégia de IA.[767]

Um tema que, até agora, tem merecido pouca atenção é até que ponto a Inteligência Artificial pode ajudar a superar alguns dos desafios que o presente Relatório aborda. No entanto, este tópico tem o potencial de se tornar cada vez mais importante. Na verdade, a IA pode potencialmente ajudar em diferentes áreas, desde ajudar indivíduos e empresas a navegar no complexo cenário regulatório on-line, até ser utilizada por tribunais para informar o tribunal, ou mesmo para direta ou indiretamente decidir disputas.[768]



05.
Grupos de conceitos relevantes

- Expressão
- Segurança
- Economia

Tal como foi mencionado (Capítulo 1.5) e observado pelos especialistas entrevistados e consultados, os progressos nos desafios jurídicos transfronteiriços enfrentados na Internet foram prejudicados, em parte, pela insuficiência do marco e dos conceitos que utilizamos para abordar estes desafios. Todo o campo sofre de um pronunciado "desafio regulamentar artificial".

A atual complexidade conceitual no campo dos desafios jurídicos transfronteiriços enfrentados na Internet impede a participação informada de diversos atores, e frequentemente resulta em mal-entendidos, falta de comunicação e discordância evitável.

Existem inúmeros conceitos que devem ser compreendidos e acordados a fim de promover uma discussão produtiva sobre o tema. O que complica ainda mais a questão é o fato de que esses conceitos muitas vezes só são devidamente compreendidos quando examinados em relação a outros conceitos correlatos.

Este Capítulo destaca a variedade de 'grupos de conceitos' relevantes, com o objetivo de discutir uma seleção de conceitos e ilustrar como eles se relacionam entre si. Alguns conceitos-chave — como o conceito de "jurisdição" — devem ser vistos em relação a vários outros conceitos e, portanto, são discutidos como parte de vários grupos.

5.1. Direito internacional público, direito internacional privado (ou conflito de leis)

A disciplina do **direito internacional público** é tradicionalmente descrita como um ordenamento jurídico que estrutura as interações entre os Estados. Há um reconhecimento recente, no entanto, que a disciplina também engloba outros sujeitos do direito internacional e relações entre indivíduos e Estados.

Por outro lado, **o direito internacional privado** (ou conflito de leis, como a disciplina é frequentemente referida em países de Direito Consuetudinário *Common Law*),[769] é a parte do direito nacional que governa as relações (sobre diferentes jurisdições jurídicas) entre pessoas, empresas, corporações e outras entidades jurídicas.

Esta distinção, embora ainda prevalecente, foi objeto de críticas durante muito tempo e está, sem dúvida, tornando-se mais difícil de manter:

> *De um ponto de vista funcional, a distinção entre direito internacional público e privado pareceria ser, na melhor das hipóteses, artificial, uma vez que tanto o direito internacional público como privado lidam, em última análise, com o mito e a prática de responder às reivindicações para a alocação do que é bom e do que é indesejável nos processos sociais mundiais. [...] o direito internacional público e privado são, na realidade, componentes complementares e indispensáveis de uma concepção maior e mais inclusiva da ordem pública mundial.*[770]

Uma área como o direito de privacidade de dados, por exemplo, parece se encaixar parcialmente no direito público internacional e, em parte, em direito internacional privado. Além disso, os desafios jurídicos transfronteiriços enfrentados na Internet são praticamente os mesmos, quer surjam no âmbito do direito internacional público (tal como tradicionalmente definido) ou do direito internacional privado; tanto o direito internacional público quanto o direito internacional privado visam a "alocar entre os Estados do mundo a competência para fazer e aplicar a lei aos acontecimentos transnacionais que os afetam."[771]

Finalmente, deve-se notar que, se um recurso concedido ao abrigo do direito privado for ignorado, o direito público pode impor sanções. Portanto, questões do direito privado que inicialmente levantam questões jurisdicionais ao abrigo do direito internacional privado poderão também suscitar questões jurisdicionais ao abrigo do direito internacional público.

Neste contexto, é frutífero abordar a jurisdição da Internet como um campo de estudo homogêneo.

5.2. Soberania, jurisdição, território e direitos humanos

O termo **jurisdição** tem mais de um significado.[772] Aqui, ele é usado para significar o poder de analisar uma questão, por exemplo, quando um tribunal tem jurisdição sobre uma determinada disputa.

O conceito de **soberania**[773] é tipicamente descrito como envolvendo autoridade suprema dentro de um território. Existe, por-

tanto, uma ligação clara entre soberania, jurisdição e **território**, embora esta ligação seja muitas vezes mal compreendida.

Embora tradicionalmente a territorialidade desempenhe um papel importante em relação à jurisdição, o conceito de soberania nem sempre exige que a jurisdição se assente apenas na territorialidade, sozinha. Para ver que isso é verdade, basta considerar conceitos de direito internacional estabelecidos, como o princípio da nacionalidade que autoriza reivindicações jurisdicionais baseadas na nacionalidade da pessoa em questão.

Além disso, enquanto o direito internacional pode exigir que haja apenas um soberano sobre um determinado território, é claro que um indivíduo ou matéria pode estar sujeito a mais de um poder soberano. A soberania não deve necessariamente ser entendida como significando exclusividade em todos os contextos; a exclusividade baseada na soberania, em relação a pessoas e assuntos, é uma adequação ruim ao mundo interconectado.[774]

Há um debate em curso sobre como o conceito de soberania se aplica on-line. Este debate chega ao cerne do conceito de soberania; alguns têm levantado questões sobre se a soberania é, em si mesma, uma regra vinculativa do direito internacional, ou antes, um princípio do direito internacional que orienta as interações entre Estados, mas não dita resultados sob o direito internacional.[775] Isto tem implicações de longo alcance em geral, mas também para reivindicações da chamada "soberania de dados" e "soberania da informação" - termos frequentemente usados sem que haja qualquer consenso claro sobre seus significados precisos.

Isto leva-nos à tensão de longa data entre a soberania, por um lado, e os direitos humanos, por outro. A relação, ou mesmo a hierarquia, entre soberania e direitos humanos é de importância crucial. A visão tradicionalmente ocidental de que os direitos humanos se sobrepõem sobre a soberania impõe necessariamente limitações ao que os Estados podem fazer. No entanto, por exemplo, sob a antiga doutrina do direito internacional soviético, a soberania tinha prioridade sobre os direitos humanos[776] e, segundo o conceito soviético de "soberania da informação", "o Estado tem o direito de controlar a disseminação da informação dentro de seu território".[777] Tais sentimentos são cada vez mais comuns em relação à Internet, e a tensão entre soberania e direitos humanos permanece de importância central.

5.3. Reivindicações jurisdicionais territoriais e extraterritoriais

Muitas vezes é feita uma distinção entre reivindicações jurisdicionais territoriais e extraterritoriais. Infelizmente, as implicações das reivindicações jurisdicionais extraterritoriais são muitas vezes exageradas no que diz respeito ao direito internacional. Na verdade, a **dicotomia territorial/extraterritorial** é, por vezes, mal utilizada como abreviação para distinguir entre reivindicações legítimas e ilegítimas de jurisdição. No entanto, assim como pode haver reivindicações extraterritoriais de jurisdição perfeitamente legítimas ao abrigo do direito internacional, também pode haver reivindicações de jurisdição baseadas na territorialidade questionáveis.

Além disso, ao abrigo do direito internacional, não existe um consenso claro sobre como definir uma reivindicação jurisdicional como extraterritorial. Conforme ilustrado no Caso *Microsoft Warrant*, de 2018,[778] por exemplo, até mesmo os sistemas legais que incluem uma presunção expressa contra a extraterritorialidade carecem de uma definição clara de extraterritorialidade no contexto on-line. Esta situação compromete ainda mais a utilidade da dicotomia territorial/extraterritorial como instrumento para fazer face aos desafios jurídicos transfronteiriços na Internet.

5.4. Devida diligência, dever de não intervenção e cortesia

O conceito de cortesia é encontrado tanto no direito internacional quanto nas leis de vários Estados. Falta-lhe uma definição uniforme e pode não ter necessariamente o mesmo significado na arena internacional que tem nas leis internas de um Estado. No entanto, **a ideia geral de cortesia** é que um Estado deve considerar os direitos e interesses de outros Estados.[779] Assim, no contexto dos desafios jurídicos transfronteiriços enfrentados na Internet, o conceito de cortesia é um lembrete importante de que, mesmo que um Estado que faz uma reivindicação de jurisdição tenha uma forte conexão com, e interesse na matéria em questão, ele deve também considerar os direitos e interesses de outros Estados antes de decidir reivindicar jurisdição.

O **dever de não intervenção** (ou "princípio da não interferência") é uma consequência direta da soberania; os Estados gozam de soberania e outros Estados devem tomar medidas para evitar interferir nessa soberania.[780] Portanto, tal como o

conceito de cortesia, o dever de não intervenção ressalta a necessidade de contabilização dos direitos e interesses de outros Estados ao fazer reivindicações jurisdicionais.

Enquanto as discussões sobre jurisdição da Internet geralmente se concentram em restrições de jurisdição, tais como as impostas pelo conceito de cortesia e pelo dever de não intervenção, o direito internacional pode igualmente impor pedidos de jurisdição em determinadas circunstâncias. De acordo com o **princípio** da **diligência devida** (e da sobreposição do princípio da "inexistência de danos"), um Estado é essencialmente obrigado a garantir que os direitos e interesses de outros Estados não sejam violados sob a sua jurisdição.[781]

Em conjunto, estes três conceitos impõem a obrigação de os Estados terem em conta os interesses de outros Estados na decisão de reivindicar jurisdição sobre uma matéria ou pessoa específica.

5.5. Jurisdição legislativa, jurisdição adjudicativa, jurisdição de investigação e jurisdição de execução

No direito internacional público, reivindicações jurisdicionais tradicionalmente se localizam nas categorias:

1. **Jurisdição legislativa (ou prescritiva)**— isto é, o poder de fazer sua lei aplicável às atividades, empresas ou pessoas;
2. **Jurisdição adjudicatória (ou competência judicial)** — ou seja, o poder de sujeitar pessoas ou coisas ao processo de seus tribunais judiciais ou administrativos; ou
3. **Jurisdição executória (de execução/cumprimento da lei)** - ou seja, o poder de induzir ou obrigar o cumprimento ou punir o não cumprimento de suas leis ou regulamentos.

Uma quarta categoria —**jurisdição investigativa**— é cada vez mais reconhecida.[782] Enquanto medidas de investigação têm sido tradicionalmente tratadas como um aspecto da jurisdição de cumprimento da lei [executória], tais medidas diferem radicalmente de outras categorias de conduta (tais como detenções em solo estrangeiro) que também são classificados como reivindicações da jurisdição de execução. Por conseguinte, há pouco mérito em agrupar questões tão distintas numa só rubrica.

A categorização clara delineada acima é uma espécie de ilusão. Como ilustrado pela discussão em torno do caso seminal

Lotus,[783] nem sempre existe acordo sobre a categoria a que pertence uma determinada reivindicação jurisdicional. Além disso, presume-se frequentemente que os impactos das reivindicações de execução são necessariamente mais graves do que as consequências das requisições de jurisdições legislativas ou adjudicatórias. No entanto, trata-se de uma super simplificação. Em última análise, o impacto de cada reivindicação jurisdicional deve ser avaliado independentemente da categoria; e quanto maior o potencial de uma reivindicação jurisdicional tem de interferir na soberania de outro Estado, maior será a razão para limitar o exercício da jurisdição.

5.6. Competência [jurisdição adjudicatória], escolha da lei aplicável, recusa de jurisdição, reconhecimento e execução

O direito internacional privado aborda quatro tipos de questões.[784] A primeira é a questão da **competência** — o poder do tribunal para analisar o litígio. A segunda é a questão da **escolha da lei**. A escolha da lei é uma questão importante porque, uma vez que um tribunal decide reclamar a competência, pode, por uma série de razões, decidir aplicar a lei material estrangeira, e a lei aplicável determinará o resultado de qualquer litígio.

Um tribunal que determinou que pode reivindicar jurisdição adjudicatória sobre uma determinada disputa poderá, no entanto, decidir não exercer essa jurisdição. Isto é conhecido como **o poder do tribunal para se recusar a exercer jurisdição**. Os motivos pelos quais o tribunal pode chegar a tal conclusão variam consideravelmente consoante os países. Em geral, os tribunais da tradição do Direito Consuetudinário (*Common Law*) têm um poder discricionário mais amplo (nomeadamente por meio da doutrina do *forum non conveniens*[785]) em comparação com o seu equivalente do Direito Civil, que normalmente só pode recusar jurisdição se uma ação já estiver pendente em outro tribunal (*lis alibi pendens*[786]). Por último, se um tribunal de um país tiver decidido um litígio material, a decisão resultante poderá ter de ser **reconhecida e executada** em outro país.

Estes quatro componentes estão entrelaçados e melhor vistos como um sistema no qual mudanças nas regras de um podem afetar as regras dos outros.

5.7. Jurisdição pessoal, jurisdição temática e alcance da 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.

5.8. Neutralidade tecnológica, equivalência funcional, resistência ao tempo

Dada a velocidade com que a tecnologia se desenvolve, as leis adotadas hoje correm o risco de serem desatualizadas mesmo antes de entrarem em vigor. Como resultado, as leis podem falhar em: (1) regular os comportamentos a que devem se aplicar; e/ou (2) regular os comportamentos a que não devem se aplicar.

Para resolver estas preocupações, os legisladores têm procurado há muito tempo desenvolver **leis tecnologicamente neutras**. Tais leis não estão ancoradas em terminologia e conceitos que são específicos da tecnologia e, portanto, são suscetíveis de ficarem rapidamente datadas. Por conseguinte, as leis tecnologicamente neutras estão melhor equipadas para fazer face ao primeiro dos dois riscos acima identificados. Mas pode-se argumentar que, em comparação com as leis específicas da tecnologia, as leis tecnologicamente neutras correm maior risco de regularem condutas às quais não devem ser aplicadas.

A ideia relacionada de **leis funcionalmente equivalentes** visa a garantir que as leis regulam a conduta da Internet da mesma forma que regulam a conduta equivalente off-line.

Leis que resistem ao tempo (*future proofing laws*) é um conceito mais amplo que, essencialmente, chama a atenção para: (1) a forma como os potenciais avanços futuros podem afetar a aplicação da lei em causa e (2) a forma como a lei em questão pode afetar potenciais desenvolvimentos futuros.

5.9. Tipos de dados

Várias classificações de dados surgiram em diferentes configurações e, infelizmente, com pouca coordenação. No estabelecimento da privacidade dos dados, é normalmente feita uma distinção entre dados que correspondem a "dados pessoais" e dados que não correspondem. Esta distinção é crucial, uma vez que as leis de privacidade de dados normalmente regulam apenas os dados pessoais. Dos dados que se qualificam como dados pessoais, alguns tipos são vistos como dados confidenciais e podem ser amparados pela proteção de salvaguardas adicionais.

A classificação de dados também surgiu nos casos em que a execução da lei procura acessar dados privados.[787] Aqui, muitas vezes é feita uma distinção entre metadados e dados de conteúdo. Os metadados são, por vezes, divididos em subcategorias: mais comumente, "informações do assinante" e "dados de tráfego". Mas, por vezes, estão divididos em três subcategorias — "dados dos assinantes", "dados de acesso" e "dados transacionais" — como é o caso das recentes propostas da UE sobre este tema.[788]

5.10. Excluir da lista, desindexar, desreferenciar, excluir, bloquear, remover, retirar, manter removido

A terminologia das ordens judiciais destinadas a lidar com conteúdo ilegal expandiu-se muito nos últimos anos. Vários termos são usados de forma intercambiável; ordens para **excluir, remover** ou **retirar** conteúdo, por exemplo, ordenam que uma parte não deixe o conteúdo em questão disponível on-line. Em contrapartida, as ordens para **excluir da lista**, **desindexar**, **desreferenciar** ou **bloquear** conteúdos destinam-se a forçar uma parte - normalmente um intermediário, como um motor de busca ou uma plataforma Internet - a tornar o conteúdo relevante indisponível na plataforma em questão.

Finalmente, vale a pena notar a diferença entre ***takedown*** (retirar) e ***staydown*** **(manter removido).** O primeiro já foi explicado. Este último vai mais longe, exigindo que a parte em questão tome medidas para impedir o reaparecimento do conteúdo.[789]

5.11. Registro, registrador, gTLD e ccTLD

A governança do sistema de nomes de domínio (DNS) é estruturada em camadas. Uma organização que gerencia nomes de domínio de topo é conhecida como um **registro** de nome de domínio. A função de um registro inclui criar extensões de nome de domínio, definir as regras para os nomes de domínio sob esse domínio de topo e trabalhar com empresas de registro de domínio para vender nomes de domínio para o público. Um **registrador** é uma organização — credenciada por um registro de nome de domínio — que vende nomes de domínio para o público.

Também é importante distinguir entre **domínios de topo genéricos** (gTLDs) e **domínios de topo de código de país** (ccTLDs). Como alguns especialistas entrevistados enfatizaram, gTLDs são globais por natureza, e os registradores de gTLD são vinculados a uma estrutura contratual com a ICANN. Em contraste, ccTLDs são regulados pelas leis e procedimentos nacionais.

O mesmo especialista entrevistado observou que, embora aproximadamente 45% dos nomes de domínio no mundo sejam domínios de topo de código de países (ccTLDs), a maioria das discussões parece focada em gTLDs.

5.12. Internet, World Wide Web

Enquanto às vezes se vê os termos Internet e World Wide Web (WWW) sendo usados como sinônimos, esse uso intercambiável é incorreto. A Internet é a infraestrutura técnica que conecta computadores ao redor do mundo e é muitas vezes descrita como uma rede de redes. É, portanto, possível, em teoria, imaginar uma Internet sem conteúdo. Mas, a maioria das referências à Internet parece implicitamente incorporar o conteúdo disponível na Internet. Assim, o termo "Internet", como mais comumente usado, tem simultaneamente uma dimensão física (a infraestrutura técnica) e uma dimensão digital (o conteúdo). Ambas as dimensões criam potenciais pontos de conexão jurisdicional.

As comunicações na Internet são controladas por vários protocolos. **WWW** usa o protocolo de transferência de hipertexto (HTTP, sigla do termo em inglês Hypertext Transfer Protocol). Os usuários podem operar softwares chamados navegadores da web para acessar páginas da Web que podem ser conectadas através dos chamados hiperlinks. A WWW é apenas uma das várias formas de comunicação que são construídas na Internet. Outras incluem e-mail (baseado em SMTP, do inglês Simple Mail Transfer Protocol) e o FTP (sigla do inglês File Transfer Protocol), comumente usado para transmissão de arquivos através da Internet.

5.13. B2B, B2C e C2C

As transações entre duas empresas são geralmente designadas por **transações entre empresas** (B2B, sigla do termo em inglês *business-to-business*). Se, por exemplo, uma loja de departamentos comprar um sistema de computador sofisticado de um fabricante, as duas empresas se envolvem em uma transação B2B. Se, por outro lado, um indivíduo compra um livro numa livraria on-line (fora da sua capacidade profissional), realiza-se uma transação entre **empresas e consumidores** (B2C, sigla do termo em inglês *business-to-consumer*).

Ambas as transações B2B e B2C ocorrem on-line por um período de tempo relativamente longo. A terceira categoria, **transações entre consumidores** (C2C, sigla do termo em inglês *consumer-to-consumer*), são comparativamente mais recentes. Numa transação C2C, nenhuma das partes atua na sua qualidade profissional. Um exemplo típico de tal transação envolve um indivíduo comprando um objeto de outro indivíduo através de uma plataforma de negociação on-line.

5.14. Inteligência artificial forte, moderada e fraca

Existem inúmeras definições de inteligência artificial e uma variedade de maneiras como conceituar diferentes tipos de IA.

O Conselho da Europa, por exemplo, define IA como "um conjunto de ciências, teorias e técnicas cujo objetivo é reproduzir por máquina as habilidades cognitivas de um ser humano. Os progressos atuais visam, por exemplo, confiar a uma máquina tarefas complexas anteriormente delegadas a um ser humano."[790]

O Conselho registra igualmente a distinção entre aquilo que foi denominado IA "forte", com a capacidade de "contextualizar pro-

blemas especializados muito diferentes de forma completamente independente", e IA 'fraca' a 'moderada', com a capacidade de "executar extremamente bem em seu campo de treinamento."[791] A IA forte geralmente está além do alcance das tecnologias atuais.

Isto - esta classificação da IA como sendo forte, moderada ou fraca - é, naturalmente, apenas uma forma de categorizar a IA. Outra abordagem comum é distinguir entre diferentes tecnologias de IA, como aprendizado de máquina e processamento de linguagem natural (PLN, do inglês *natural language processing*). Simplificando, o aprendizado de máquina envolve algoritmos de aprendizagem expostos a dados de treinamento resultando em software com a capacidade de fazer previsões ou decisões sem ser explicitamente programado para executar a tarefa.[792] A PLN está "preocupada com as interações entre computadores e linguagens humanas (naturais), em particular como programar computadores para processar e analisar grandes quantidades de dados de linguagem natural."[793]

Finalmente, deve-se notar que a IA muitas vezes é discutida no contexto de uma variedade de outras 'palavras da moda', como automação e mineração de dados. Tanto a automação quanto a mineração de dados[794] podem, mas não precisam, ser baseadas em IA.

Notas

Notas do sumário executivo

1 Infográfico 4, página 28.

2 Infográfico 6, página 33.

3 Infográfico 8, página 35.

4. Internet & Jurisdiction Policy Network. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect>.

Notas do capítulo 01
Por que um relatório de status global, e o que está em jogo?

1.1

5. Um especialista consultado referiu-se especificamente a este recurso: Fórum Global para o Desenvolvimento de Mídia. Internet Governance. Disponível em: <https://gfmd.info/internet-governance/>.

6. Free Access to Law Movement. Disponível em: <http://www.falm.info/members/current/> .

1.5

7. Webach, K. (1997). Digital Tornado: The Internet and Telecommunications Policy (Working paper of the Federal Communications Commission). Disponível em: <https://www.fcc.gov/reports-research/working-papers/digital-tornado-internet-and-telecommunications-policy>.

8. Google Inc. contra Equustek Solutions Inc 2017 SCC 34. Disponível em: <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do>.

9 American Libraries Association contra Pataki 1997 SDNY 969 F Supp 160, 170 (por Preska J).

10 Ou "conflito de leis", como "direito internacional privado" é frequentemente referido nos países de direito consuetudinário.

11. Introductory Comment to the Harvard Draft Convention on Jurisdiction with Respect to Crime 1935. (1935). Supplement American Journal of International Law, 29, 443, p. 445.

12. (2017). Sovereignty, cyberspace and Tallinn manual 2.0. American Journal of International Law Unbound, 111. Disponível em: <https://www.cambridge.org/core/journals/american-journal-of-international-law/ajil-unbound-by-symposium/sovereignty-cyberspace-and-tallinn-manual-2-0>.

13. Ver capítulo 5 "Grupos de conceitos relevantes 101" para as definições destes conceitos.

14. United Nations Special Rapporteur on the Right to Privacy Task Force on Health Data.. (2019). Draft recommendation on the protection and use of health related data. Disponível em: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf>.

15. Internet Society. (2018, setembro). The Internet and Extra-Territorial Effects of Laws. Disponível em: <https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf>. p. 1.

16. Kuner, C. (2017, 1 de fevereiro). The Internet and the global reach of EU Law. Law Society Economy Working Papers No. 4/2017. Disponível em SSRN: <https://ssrn.com/abstract=2890930> ou <http://dx.doi.org/10.2139/ssrn.2890930>, p. 7.

17. PwC. (2018). Revitalizing privacy and trust in a data-driven world. Disponível em: <https://www.pwc.com/us/en/cybersecurity/assets/revitalizing-privacy-trust-in-data-driven-world.pdf> <privacy-trust-in-data-driven-world.pdf>.

18. Fórum Econômico Mundial. (2016). Internet fragmentation: An overview. Disponível em: <https://www.weforum.org/reports/internet-fragmentation-an-overview>, p. 3.

19. Song, S. Internet drift: How the Internet is likely to splinter and fracture. Digital Freedom Fund. Disponível em: <https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/>.

20. Song, S. Internet drift: How the Internet is likely to splinter and fracture. Digital Freedom Fund. Disponível em: <https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/>.

21. Song, S. Internet drift: How the Internet is likely to splinter and fracture. Digital Freedom Fund. Disponível em: <https://digitalfreedomfund.org/internet-drift-how-the-internet-is-likely-to-splinter-and-fracture/>.

22. Internet & Jurisdiction Policy Network. (2017, dezembro). . Russia reportedly moves ahead with plan to create independent DNS backup for BRICScountries.. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6626_2017-12>.

23. RT. (20 de fevereiro de 2018). Russia to launch 'independent Internet' for BRICS nations report. Disponível em: <https://www.rt.com/politics/411156-russia-to-launch-independent-internet/>.

24. Cimpanu, C. (11 de fevereiro de 2019). Russia to disconnect from the Internet as part of a planned test. ZD Net. Disponível em: <https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/>.

25. Internet & Jurisdiction Policy Network. (2019, maio). Russia's Internet Sovereignty law is signed into law. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJ0byI6IjIwMTktMDUifQ==>.

26. NETmundial. Os princípios NETmundial. Disponível em: <https://www.cgi.br/media/docs/publicacoes/4/Documento_NETmundial_pt.pdf>. Acesso em: 20 de setembro de 2020.

27. Diretiva 2000/31/CE do Parlamento Europeu e do Conselho, de 8 de Junho de 2000, relativa a certos aspectos jurídicos dos serviços da sociedade da informação, em especial do comércio eletrônico, no mercado interno, Artigo 4(1). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32000L0031&qid=1600640178099&from=PT>. Acesso em: 20 de setembro de 2020.

1.10

28. Ver, por exemplo: UNESCO. (2017). What if we all governed the Internet? Advancing multi-stakeholder participation in Internet governance. Disponível em: <https://en.unesco.org/sites/default/files/what_if_we_all_governed_internet_en.pdf>.

29. Para obter um exemplo de 2019, consulte: GSMA. Digital Declaration. Disponível em: <https://www.gsma.com/betterfuture/digitaldeclaration>.

30. Para uma discussão detalhada sobre a estrutura da ICANN, consulte, por exemplo: Mahler, T. (2019). Generic toplevel domains – A study of transnational private regulation. Cheltenham, United Kingdom: Edward Elgar Publishing; Bygrave, L.A. (2015). Internet governance by contract. Oxford, United Kingdom: Oxford University Press, capítulo 4.

31. Por exemplo, a African Regional At-Large Organization, a Asian, Australasian and Pacific Islands Regional At-Large Organization, a European Regional At-Large Organization, a Latin American and Caribbean Islands Regional At-Large Organization e a North American Regional At-Large Organization.

32. World Wide Web Consortium. Disponível em: <http://www.w3.org/Consortium/>.

33. Por exemplo, o IGF da América Latina e Caribe, o IGF da África Oriental, o IGF da África Central, o IGF do Norte da África, o IGF da África Ocidental, o IGF da Ásia Central, o IGF da Ásia Pacífico e o IGF árabe.

1.11

34. Wikipédia. Microsoft Corp. contra United States. Disponível em: <https://en.wikipedia.org/wiki/Microsoft_Corp._contra_United_States>.

35. Considere, por exemplo, a abordagem da Suprema Corte do Canadá para pareceres de *amicus* no caso Google Inc. contra Equustek Solutions Inc. 2017 SCC 34. Disponível em: <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do>.

Notas do capítulo 02
Tendências dominantes

2.1

36. Lessig, L. (1999). The law of the horse: What cyberlaw might teach. Harvard Law Review, 113, 506. Disponível em: <https://cyber.harvard.edu/publications/1999/The_Law_of_the_Horse>.

37. Ver mais em: Millard, C. (Ed.). (2013). Cloud Computing Law. Oxford, United Kingdom: Oxford University Press.

38. McGillivray, K. (2019). Government cloud procurement: Contracts, data Protection, and the quest for compliance (Tese de doutorado). Universidade de Oslo, Oslo, Noruega, p. 55-56.

2.2

39. Em re Search Warrants Nos 16960M01 e 161061M para Google, para 7.

40. Em re Search Warrants n.os 16960M01 e 161061M para Google, para 25.

41. Australian government. (2018). Australia's tech future. Disponível em: <https://www.industry.gov.au/sites/default/files/2018-12/australias-tech-future.pdf>.

42. Software One. Managing and understanding on premises and cloud spend. Disponível em: <https://www.softwareone.com/en/learn-and-inform/ebooks-and-whitepapers/survey-on-premises-and-cloud-spend>.

43. Ver, por exemplo, Comissão Europeia. Digital single market: Cloud computing. Disponível em: <https://ec.europa.eu/digitalsinglemarket/en/cloud>.

44. Johnson, D.R. & Post, D.G. (1996). Law and borders: The rise of law in cyberspace. Stanford Law Review, 48, 1367; Reidenberg, J.R. (1998). Lex Informatica. Texas Law Review, 76(3), 553; Geist, M. (2001). Is there a there there? Towards greater certainty for Internet jurisdiction. Berkeley Technology Law Journal, 16, 1345; Menthe, D.C. (1998). Jurisdiction in cyberspace: A theory of international spaces. Michigan Technology Law Review, 4(1), 69; and Goldsmith, J.L. (1998). Against cyberanarchy. University of Chicago Law Review, 65(4), 1250.

45. Barlow, J.P. (1996). A declaration of the independence of cyberspace. Electronic Frontier Foundation. Disponível em: <https://www.eff.org/cyberspace-independence>.

46. Ost. F, & van de Kerchove. M. (2002). De la pyramide au réseau? Pour une théorie dialectique du droit, Facultés universitaires SaintLouis Bruxelles.

47. Weitzenboeck. E, (2014). Hybrid net: the regulatory framework of ICANN and the DNS. International Journal of Law and Information Technology, 22(1), 49.

48. Weitzenboeck. E, (2014). Hybrid net: the regulatory framework of ICANN and the DNS. International Journal of Law and Information Technology, 22(1) 49, 68.

49. Weitzenboeck. E, (2014). Hybrid net: the regulatory framework of ICANN and the DNS. International Journal of Law and Information Technology, 22(1), 49.

50. Ver também: Weber, R. H. (2012). Overcoming the hard law/soft law dichotomy in times of (financial) crisis. Journal of Governance and Regulation, 1(1) , 814.

51. Ver mais em: Svantesson, D. (2017). Solving the Internet jurisdiction puzzle. Oxford, United Kingdom: Oxford University Press, 91-112.

52. Ver, por exemplo, Internet & Jurisdiction Policy Network. (2019, março). Facebook calls for increased regulation pertaining to harmful content, elections, privacy and data portability. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/%0Aretrospect#eyJ0byI6IjIwMTktMDMifQ==>.

53. Internet & Jurisdiction Policy Network. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect>.

54. Zippo Manufacturing Company contra Zippo Dot Com, Inc 952 F.Supp 1119 (WD Pa 1997).

55. Dow Jones & Company Inc. contra Gutnick (2002) 210 CLR 575. Para uma discussão recente sobre a doutrina do fórum *non conveniens* em relação à Internet, ver: Haaretz.com contra Goldhar, 2018 SCC 28, 2018 2 S.C.R. 3.

56. Ver, no entanto, o apelo do advogado-geral Szpunar para que os tribunais adotem uma abordagem de "autolimitação" (Parecer no processo C18/18, n.o 100), bem como a ênfase dada pelo TJUE na diversidade das legislações (processo C-507/17).

57. Este estudo baseia-se em uma pesquisa de texto de artigos de periódicos contendo pelo menos uma frase com o termo "Internet" e o termo "jurisdição", ou pelo menos uma frase com o termo "ciberespaço" e o termo "jurisdição" (ou seja, (Ciberespaço /s jurisdição) OU (Internet /s jurisdição)). As buscas foram realizadas no dia 7 de janeiro de 2019 na Law Journal Library da HeinOnline. A pesquisa limitou-se às seguintes categorias: "Artigos", "Comentários", "Notas" e "Editoriais", incluindo "artigos externos (artigos fora da HeinOnline)", bem como "resultados periódicos de outras Coleções HeinOnline". Esta abordagem tem, sem dúvida, as suas limitações. No entanto, o resultado é indicativo da evolução de artigos, comentários, notas e editoriais em revistas de direito que abordam o tema da jurisdição da Internet.

58. Resultado produzido através da seguinte pesquisa: (Ciberespaço OU Internet). As buscas foram realizadas no dia 7 de janeiro de 2019 na Law Journal Library da HeinOnline. A pesquisa limitou-se às seguintes categorias: "Artigos", "Comentários", "Notas" e "Editoriais", incluindo "artigos externos (artigos fora da HeinOnline)", bem como "resultados periódicos de outras Coleções HeinOnline".

2.3

59. Ver mais em: Ryngaert, C. (2015). Jurisdiction in International Law 2nd edn. Oxford, United Kingdom: Oxford University Press, p. 8.

60. Caso S.S. "Lotus" (França contra Turquia), PCIJ Série A, nº 10, p. 21.

61. Caso S.S. "Lotus" (França contra Turquia), PCIJ Série A, nº 10, p. 21.

62. Internet & Jurisdiction Policy Network. Data & Jurisdiction program: Operational Approaches. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Operational-Approaches.pdf>.

63. Estes "outros interesses" podem incluir os interesses dos indivíduos, ver, por exemplo, o trabalho da Irland-Piper sobre se a doutrina do "abuso de direitos" pode ser útil para procurar manter um equilíbrio adequado entre os direitos dos Estados e dos indivíduos (Irland-Piper, D. (2017). Accountability in extraterritoriality. Cheltenham, Inglaterra: Edward Elgar).

64. Ver mais em: United Nations Special Rapporteur on the Right to Privacy Task Force on Health Data. (2019). Draft recommendation on the protection and use of healthrelated data. Disponível em: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/DraftRecommendationProtectionUseHealthRelatedData.pdf>, and Svantesson, D. (2017). Solving the internet jurisdiction puzzle. Oxford, United Kingdom: Oxford University Press, pp. 57-90

65. Para exemplos de tentativas de construção de tais ferramentas, ver por exemplo, Svantesson, D. (2013). A "layered approach" to the extraterriotoriality of data privacy laws. International Data Privacy Law, 3(4), 278-286; e Svantesson, D. (2017). Solving the Internet jurisdiction puzzle. Oxford, United Kingdom: Oxford University Press, p. 171-189, que descreve um quadro para o "alcance da jurisdição".

66. Ver mais em: Svantesson, D. (2016). Private international law and the Internet (3rd ed.). Alphen aan den Rijn, The Netherlands: Lei Kluwer International, pp. 11-12.

2.4

67. COM (2018) 226 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0226&from=PT>. Acesso em: 04 de outubro de 2020. .

68. COM (2018) 225 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>. Acesso em: 20 de setembro de 2020.

69. Weber, R. H. (2012). Overcoming the hard law/soft law dichotomy in times of (financial) crisis. Journal of Governance and Regulation.1(1), 8-14, 12.

70. Ver, por exemplo: Lessig, L. (1999). The law of the horse: What cyberlaw might teach. Harvard Law Review, 113, 506. Disponível em: <https://cyber.harvard.edu/publications/1999/The_Law_of_the_Horse>.

71. Annual report of the United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression to the General Assembly. (2012). A/67/357, para.2. Disponível em: <https://undocs.org/en/A/67/357>.

72. United Nations, Human Rights Committee. (12 de setembro de 2011). General comment No. 34 Article 19: Freedoms of opinion and expression. CCPR/C/GC/34, n.o 11. Disponível em: <https://undocs.org/en/CCPR/C/GC/34>.

73. Esta categoria é ampla e abrange, por exemplo, conteúdo ofensivo, bem como desinformação e conteúdo que pode aumentar o risco de que seu público irá tolerar ou cometer violência contra outros.

2.5

74. Stanford Center for Internet and Society. (2018). World intermediary liability map. Disponível em: <https://wilmap.law.stanford.edu/>.

75. Internet & Jurisdiction Policy Network. (2018, dezembro). Facebook announces ban of over 400 pages and 100 accounts relating to Myanmar conflict. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7741_2018-12>.

76. Wagner. K. (2018, 18 de dezembro). Facebook removed hundreds more accounts linked to the Myanmar military for posting hate speech and attacks against ethnic minorities. Recode. Extraído de removed-drohingya-genocide.

77. Internet & Jurisdiction Policy Network. (2019, julho). US court rules that Facebook is well within its limits to remove pages linked to misinformation campaign. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiZmVkZXJhbCBhZ2VuY3kgb2YgbmV3cyIsImZyb20iOiIyMDEyLTAyIiwidG8iOiIyMDE5LTA5In0=>.

78. Christchurch Call. (2019). Disponível em: <https://www.christchurchcall.com/>.

79. Directiva 2000/31/CE do Parlamento Europeu e do Conselho de 8 de Junho de 2000 relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno («Directiva sobre o comércio electrónico») [2000] JO L 178/ 1 de 369. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32000L0031&qid=1600648496607&from=PT>. Acesso em: 20 de setembro de 2020.

80. Privacy Act 1988 (Cth), para 6A(4).

81. PwC. (2018). Top policy trends of 2018. Disponível em: <https://www.pwc.com/us/en/services/consulting/risk-regulatory/top-policy-trends-2018.html>.

82. Internet & Jurisdiction Policy Network. (2018, outubro). Facebook announces it has removed 8.7 million child abuse images in past three months thanks to previously undisclosed software. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7567_2018-10>.

83. Internet & Jurisdiction Policy Network. (2018, dezembro). Uganda: ISPs start implementing regulator's order to remove access to websites with adult content. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7736_2018-12>.

84. Sartor, G. (2013). Provider's liability and the right to be forgotten. Em Svantesson, D. & Greenstein, S. (Eds). Nordic yearbook of law and informatics 2010– 2012: Internationalisation of law in the digital information society. Copenhagen: Ex Tuto Publishing.101-37, 111.

85. Equustek Solutions Inc. contra Jack, 2014 BCSC 1063, para 156. Além disso, a afirmação do Juiz Fenlon de que não existe outra forma prática de cessar as vendas no sítio Web do requerido parece equivocada, uma vez que, por exemplo, os canais de pagamento do requerido em causa poderiam ter sido visados.

86. United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom and Expression. (2018) 2018 Thematic Report to the Human Rights Council. A/HRC/38/35. Disponível em: <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35>, p. 8.

87. Hern, A. (26 de setembro de 2019). TikTok's local moderation guidelines ban pro-LGBT content. The Guardian. Disponível em: <https://www.theguardian.com/technology/2019/sep/26/tiktoks-local-moderation-guidelines-ban-pro-lgbt-content>.

88. Internet Governance Forum. Dynamic Coalition on Platform Responsibility. Disponível em: <https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-platform-responsibility-dcpr>. Ver também iniciativas como: Internet Policy Observatory. The Santa Clara Principles on Transparency and Content Moderation. Disponível em: <https://santaclaraprinciples.org> e Princípios de Manila sobre Responsabilidade Intermediária. Disponível em: <https://www.manilaprinciples.org/pt-br>. Acesso em: 20 de setembro de 2020.

89. United Nations Special Rapporteur on the Promotion and Protection of the Right to Freedom and Expression. (2018) 2018 Thematic Report to the Human Rights Council. A/HRC/38/35. Disponível em: <http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/35>.

90. Ver também o trabalho de: Ranking Digital Rights. Disponível em <https://rankingdigitalrights.org/>.

91. Institute for Accountability in the Digital Age. Disponível em <https://i4ada.org/>.

92. Institute for Accountability in the Digital Age. (2018). The Hague Global Principles for Accountability in the Digital Age. Disponível em: <https://i4ada.org/wp-content/uploads/2018/06/TheHaguePrinciples_public_consultation-v0.1.pdf>.

Notas do capítulo 03
Tendências atuais

93. Office of the Director of National Intelligence. (2017). Global trends: Paradox of progress. Disponível em:<https://www.dni.gov/index.php/global-trends/near-future>.

94. Internet & Jurisdiction Policy Network. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect> .

95. Existem algumas tendências jurisdicionais importantes deixadas de fora nesta seção que provavelmente ganharão muito mais atenção em um futuro previsível. Por exemplo, um especialista consultado chamou a atenção para a dimensão jurisdicional dos custos ambientais em que o crescimento tecnológico incorre (por exemplo, ver capítulo 3.3.5). E, como apontado por um especialista entrevistado, outro tipo de assunto encontrado é uma crescente preocupação sobre questões trabalhistas digitais. Por exemplo, as pessoas empregadas para avaliar o pedido de retirada estão se tornando parte integrante da infraestrutura da Internet, fazendo tarefas servis que impactam grandemente a liberdade de expressão. Surgem questões transfronteiriças quando essas tarefas são atribuídas a trabalhadores estrangeiros e surgiram questões quanto ao grau de apoio concedido a esses trabalhadores, que muitas vezes estão expostos a conteúdos altamente perturbadores e ofensivos. Questões como esta são importantes, mas não foram incluídas no relatório deste ano.

3.1

96. U.S. Const. Amend. I. Disponível em: <https://constitutioncenter.org/interactive-constitution/amendments/amendment-i>.

97. Ver, por exemplo: United Nations, General Assembly. Human Rights Council: Draft Resolution: The promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20 (27 de junho de 2016). Disponível em: <https://digitallibrary.un.org/record/845728> Acesso em 21 de outubro de 2020.

98. United Nations, General Assembly. Human Rights Council: Draft Resolution: The promotion, protection and enjoyment of human rights on the Internet, A/HRC/32/L.20 (27 de junho de 2016). Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G16/131/89/PDF/G1613189.pdf>. Acesso em 21 de setembro de 2020. p.3.

99. Conselho da Europa. (2014). Guia de direitos humanos para os utilizadores da Internet. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a0532>. Acesso em 21 de setembro de 2020.

100. Ver mais em: Oster, J. (2017). Which limits on freedom of expression are legitimate? Divergence of free speech values in Europe and the United States. Em: Kohl, U. (Ed.). The net and the nation state. Cambridge, Reino Unido: Cambridge University Press, 39-47.

101. International League Against Racism & Anti Semitism (LICRA) contra Yahoo! Inc and Yahoo! França [2000] Tribunal de Grande Instance de Paris (Tribunal do Condado de Paris).

102. Dawn. (25 de outubro de 2017). Body to block blasphemous content on Internet. Disponível em: <https://www.dawn.com/news/1366064/body-to-block-blasphemous-content-on-internet>.

103. McDonell, S. (17 de julho de 2017). Why China censors banned Winnie the Pooh. Disponível em: <https://www.bbc.com/news/blogs-china-blog-40627855>.

104. Freedom House. (2018). Freedom in the world 2018. Disponível em: <https://freedomhouse.org/report/freedom-world/freedom-world-2018>.

105. Khashoggi, J. (17 de outubro de 2018). What he Arab world needs most is freedom of expression. The Washington Post. Disponível em: <https://www.washingtonpost.com/opinions/global-opinions/jamal-khashoggi-what-the-arab-world-needs-most-is-free-expression/2018/10/17/adfc8c44-d21d-11e8-8c22-fa2ef74bd6d6_story.html?noredirect=on&utm_term=.4d5fab2ea101>.

106. De fato, o Art.1(2)(g), do Regulamento Roma II (Regulamento (CE) n. 864/2007 do Parlamento Europeu e do Conselho, de 11 de julho de 2007, relativo à lei aplicável às obrigações extracontratuais), que determina a lei aplicável às obrigações extracontratuais, exclui obrigações "que decorram da violação da vida privada e de direitos relacionados com a personalidade, incluindo a difamação" do referido Regulamento. Esta exclusão resulta diretamente das diferenças consideráveis que existem no equilíbrio entre a liberdade de expressão e o direito à reputação entre os Estados-Membros da União Europeia.

107. Electronic Frontier Foundation. (1 de outubro de 2018). California's net neutrality law: What's happened, What's next. Disponível em: <https://www.eff.org/deeplinks/2018/10/californias-net-neutrality-law-whats-happened-whats-next>.

108. International League Against Racism & Anti Semitism (LICRA) contra Yahoo! Inc and Yahoo! França [2000] Tribunal de Grande Instance de Paris (Tribunal do Condado de Paris).

109. Yahoo! Inc. contra La Ligue Contre le Racisme et L'Antisemitisme [2001] NDCal 169 F Supp 2d 1181. Veja, também, Yahoo! Inc. contra La Ligue Contre le Racisme et L'Antisemitisme [2006] 9ª Cir 433 F3D 1199.

110. Gold, H. (2 de julho de 2019). Germany fines Facebook for underreporting illegal content. CNN Business. Disponível em: <https://edition.cnn.com/2019/07/02/tech/facebook-germany-illegal-content/index.html>.

111. Internet & Jurisdiction Policy Network. (2019, julho). France passes a new law requiring platforms to remove hate speech within 24 hours. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiZnJhbmNlIiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDcifQ==>.

112. Chutel, L. (7 de julho de 2018). Zambia is the latest African state trying to muzzle social media with arbitrary laws. Quartz Africa. Disponível em: <https://qz.com/africa/1322814/zambia-considers-social-media-clampdown-through-new-laws-or-tighter-regulation/>.

113. Internet & Jurisdiction Policy Network. (julho de 2018). Zambia: Government announces regulation of social media to fight against hate speech, identity theft and pornographic content. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7192_2018-07>.

114. Attorney General for Australia. (4 de abril de 2019). Tough new laws to protect Australians from live streaming of violent crimes. [Press Release], Australia. Disponível em: <https://www.attorneygeneral.gov.au/Media/Pages/Tough-New-Laws-to-protect-Australians-from-Live-Streaming-of-Violent-Crimes.aspx>.

115. Para a Lei Australiana, ver, por exemplo, s.474.37 (1) (d) da Lei do Código Penal de 1995, que prevê o acesso a esse material para fins de pesquisa.

116. Blum, R. (6 de fevereiro de 2017). Israeli Justice Minister: Efforts to remove terrorismincitement from social media platforms bearing fruit. The Algemeiner. Disponível em: <https://www.algemeiner.com/2017/02/06/israeli-justice-minister-at-international-cyber-conference-efforts-of-our-task-force-to-remove-terrorism-incitement-from-social-media-platforms-bearing-fruit/>.

117. Internet & Jurisdiction Policy Network. (2017, fevereiro). Israeli minister highlights successful content removals, proposes fines against platforms. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-5622_2017-02>.

118. CounterTerrorism and Border Security Act 2019 (UK) c.3. Disponível em: <http://www.legislation.gov.uk/ukpga/2019/3/contents>.

119. Comissão Europeia. (12 de setembro de 2018). Estado da União 2018: Comissão propõe novas regras para remover conteúdos terroristas da Internet. [Comunicado de Imprensa]. Estrasburgo. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/pt/IP_18_5561>. Acesso em: 21 de setembro de 2020.

120. Comissão Europeia. (12 de setembro de 2018). Estado da União 2018: Comissão propõe novas regras para remover conteúdos terroristas da Internet. [Comunicado de Imprensa]. Estrasburgo. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/pt/IP_18_5561>. Acesso em: 21 de setembro de 2020.

121. Conselho da União Europeia. (6 de dezembro de 2018). Conteúdos terroristas em linha [N.E.: online]: Conselho aprova posição de negociação sobre novas regras destinadas a evitar a sua difusão. [Comunicado de Imprensa]. Estrasburgo. Disponível em:<https://www.consilium.europa.eu/pt/press/press-releases/2018/12/06/terrorist-content-online-council-adopts-negotiating-position-on-new-rules-to-prevent-dissemination/>. Acesso em: 21 de setembro de 2020.

122. Internet & Jurisdiction Policy Network. (6 de dezembro de 2018). EU Council adopts negotiating position on regulation against online terrorista contente, endorsing one-hour takedown upon notice and proactive measures against contente reappearance. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article7726_201812>.

123. United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression; the Special Rapporteur on the right to privacy and the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism. (7 de dezembro de 2018). Joint Report on the European Union's proposal for a Regulation on preventing the dissemination of terrorist content online to complement Directive 2017/541 on combating terrorism. OL OTH 71/2018. Disponível em: <https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234>.

124. Internet & Jurisdiction Policy Network. (2018, dezembro). EU Council adopts negotiating position on regulation against online terrorista contente, endorsing one-hour takedown upon notice and proactive measures against content reappearance. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7726_2018-12>.

125. Parlamento Europeu. (17 de Abril de 2019). Terrorist content online should be removed within one hour, says EP. [Press Release]. Disponível em: <https://www.europarl.europa.eu/news/en/press-room/20190410IPR37571/terrorist-content-online-should-be-removed-within-one-hour-says-ep>.

126. Nações Unidas, Assembleia Geral. (1966). Pacto Internacional sobre os Direitos Civis e Políticos. Treaty Series, 999, 171, Artigo 20(2). Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/D0592.htm>. Acesso em: 21 de setembro de 2020. No entanto, na ratificação do PIDCP, alguns Estados (incluindo os EUA) anexaram ressalvas ao artigo 20.

127. Nações Unidas. (1966). Convenção Internacional sobre a Eliminação de Todas as Formas de Discriminação Racial. Treaty Series, 660, 195, Artigo 4. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/1950-1969/D65810.html>. Acesso em: 21 de setembro de 2020.

128. Por exemplo, em setembro de 2019, o Programa da Universidade George Washington sobre Extremismo lançou três novos trabalhos sobre Extremismo Violento On-line. Disponível em: <https://www.hsdl.org/c/three-new-papers-online-violent-extremism/>.

129. Nações Unidas. (23 de setembro de 2019). Joint open letter on concerns about the global increase in hate speech. Disponível em: <https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25036&LangID=E>.

130. US Senate Committee on Commerce, Science and Transportation. (18 de setembro de 2019). Mass violence, extremism, and digital responsibility. Disponível em: <https://www.commerce.senate.gov/2019/9/mass-violence-extremism-and-digital-responsibility>.

131. Sky News. (26 de agosto de 2019). OECD join push to tackle online extremism. Disponível em: <https://www.skynews.com.au/details/_6076962754001> .

132. Christchurch call to eliminate terrorist and violent extremist content online. Disponível em: <https://www.christchurchcall.com/call.html> .

133. C, Knaus. (19 de março de 2019). Australian telcos block dozens of websites hosting Christchurch terror video. The Guardian. Disponível em: <https://www.theguardian.com/technology/2019/mar/19/australian-telcos-block-dozens-of-websites-hosting-christchurch-terror-video>.

134. Kelly, M. (19 de junho de 2019). Twitch sues to unmask trolls that posted violent and pornographic streams. The Verge. Disponível em: <https://www.theverge.com/2019/6/17/18682395/twitch-amazon-sues-anonymous-trolls-porn--christchurch>.

135. G20. (2019). Declaração de Osaka dos Líderes do G20 para a Prevenção da Exploração da Internet para o Terrorismo e o Extremismo Violento Conducente ao Terrorismo (EVCT). Disponível em: <http://www.itamaraty.gov.br/pt-BR/notas-a-imprensa/20563-declaracao-de-osaka-dos-lideres--do-g20-para-a-prevencao-da-exploracao-da-internet-para-o-terrorismo-e-o-extremismo-violento-conducente-ao-terrorismo-evct>. Acesso em: 21 de setembro de 2020.

136. Dangerous Speech Project. Disponível em: <https://dangerousspeech.org/guide/>.

137. United States Department of Justice. Hate crimes. Disponível em: <https://www.justice.gov/hatecrimes>.

138. Gadde, V. & Harvey, D. (25 de setembro de 2018). Creating new policies together. Twitter. Disponível em: <https://blog.twitter.com/official/en_us/topics/company/2018/Creating-new-policies-together.html>.

139. Global Counterterrorism Forum. (2018, Setembro). Policy toolkit on the Zurich-London recommendations on preventing and countering violent extremism and terrorism online. Disponível em: <https://www.thegctf.org/Tools-and-Manuals/Policy-Toolkit-on-the-Zurich-London-Recommendations-on-Preventing-and-Countering-Violent-Extremism-and-Terrorism-Online>.

140. European Court of Human Rights. (2018, junho). Factsheet - Hate speech. Disponível em: <https://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf>.

141. The Straits Times. (3 de janeiro de 2018). Indonesia launches cyber agency to tackle extremism, fake news. Disponível em: <http://www.straitstimes.com/asia/se-asia/indonesia-launches-cyber-agency-to-tackle-extremism-fake-news>.

142. Internet & Jurisdiction Policy Network. (2018, janeiro). Indonesia. New cyber agency launches automated system to detect and block extremist content and adult websites. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6695_2018-01>.

143. French-British Action Plan: Internet security. (13 de junho de 2017). Paris. Disponível em: <https://www.gov.uk/government/publications/french-british-action-plan-internet-security>.

144. Five Country Ministerial Statement on Countering the Illicit Use of Online Spaces. (28-29 de agosto de 2018). Gold Coast. Disponível em: <https://archive.homeaffairs.gov.au/about/national-security/five-country-ministerial-2018/countering-illicit-use-online-spaces>.

145. G7 Security Minister's Commitment Statement. (2018). Charlevoix. Disponível em: <https://www.international.gc.ca/world-monde/international_relations-relations_internationales/g7/documents/2018-06-09-defending_democracy-defense_democratie.aspx?lang=eng>. Acesso em: 21 de setembro de 2020.

146. G7 Outcomes Document on Combating the Use of the Internet for Violent and Extremist Purposes. (2019, Abril). Paris. Disponível em: <https://www.elysee.fr/admin/upload/default/0001/04/287b5bb9a30155452ff7762a9131301284ff6417.pdf>.

147. Google. (4 de dezembro de 2017). Update on the Global Internet Forum to Counter Terrorism. Disponível em: <https://www.blog.google/around-the-globe/google-europe/update-global-internet-forum-counter-terrorism/>.

148. Shanghai Cooperation Organisation. (2017, junho). Statement by the heads of the member states of the Shanghai Cooperation Organisation on joint counteraction to international terrorism. Disponível em: <http://eng.sectsco.org/load/295671/>.

149. Shanghai Cooperation Organisation. (15 de junho de 2001). Shanghai convention on combating terrorism, separatism and extremism. Disponível em: <https://www.refworld.org/docid/49f5d9f92.html>.

150. European Commission. (2019). Disponível em: <https://ec.europa.eu/info/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en>.

151. UNESCO. (2015). Countering online hate speech. Disponível em: <http://unesdoc.unesco.org/images/0023/002332/233231e.pdf>.

152. ARTICLE19. (2015). 'Hate speech' explained: A toolkit. Disponível em: <https://www.article19.org/data/files/medialibrary/38231/'Hate-Speech'-Explained---A-Toolkit-%282015-Edition%29.pdf>.

153. ARTICLE19. (2018). Responding to 'hate speech' with positive measures: A case study from six EU countries. Disponível em: <https://www.article19.org/wp-content/uploads/2018/06/Responding-to-'hate-speech'-with-positive-measures-A-case-study-from-six-EU-countries-.pdf>.

154. Jordan Times. (26 de fevereiro de 2019). King participates in tech-focused Aqaba meetings hosted by US. Disponível em: <http://www.jordantimes.com/news/local/king-participates-tech-focused-aqaba-meetings-hosted-us>.

155. Australian Human Rights Commission. (2013). Background paper: Human rights in cyberspace. Disponível em: <https://www.humanrights.gov.au/our-work/rights-and-freedoms/publications/background-paper-human-rights-cyberspace>.

156. Report of the Australian Taskforce to combat terrorist and extreme violent material online. (30 de junho de 2019). Disponível em: <https://www.pmc.gov.au/resource-centre/national-security/report-australian-taskforce-combat-terrorist-and-extreme-violent-material-online>.

157. The Rabat Plan of Action on the prohibition of advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence, A/HRC/22/17/Add.4, Appendix, adotado em 5 de outubro de 2012.

158. Council of the European Union (2000). General policy recommendation on combating the dissemination of racist, xenophobic and antisemitic material via the Internet. Disponível em: <https://rm.coe.int/ecri-general-policy-recommendation-no-6-on-combating-the-dissemination/16808b5a8d>.

159. Conselho da Europa. (28 de janeiro de 2003). Protocolo adicional à Convenção sobre o Cibercrime relativo à incriminação de actos de natureza racista e xenófoba praticados através de sistemas informáticos. Disponível em: <https://rm.coe.int/16802ed8cd>. Acesso em: 22 de setembro de 2020.

160. United Nations, Counter-Terrorism Committee Executive Directorate. Tech against terrorism. Disponível em: <https://www.techagainstterrorism.org>.

161. United Nations. Plan of action to prevent violent extremism. Disponível em: <https://www.un.org/counterterrorism/ctitf/en/plan-action-prevent-violent-extremism>.

162. Southern Poverty Law Centre. Disponível em: <https://www.splcenter.org>.

163. United Nations, Counter=Terrorism Committee Executive Directorate. (14 de setembro de 2018). Public-private efforts to address terrorist content online: A year of progress – what's next?. Disponível em: <https://www.un.org/sc/ctc/news/event/public-private-efforts-address-terrorist-content-online-year-progress-whats-next>. UN Security Resolution 2129, S/RES/2129 (2013), Un Security Council Resolution 2354, S/RES/2354 (2017), UN Security Council Resolution 2395, S/RES/2395 (2017) and UN Security Council Resolution 2396, S/RES/2396 (2017).

164. Dow Jones and Company Inc contra Gutnick [2002] HCA 56.

165. No entanto, ainda há casos proeminentes em litígio nos mais altos níveis. Ver, por exemplo: Haaretz.com contra Goldhar, 2018 SCC 28, [2018] 2 S.C.R.3.

166. Riquelme, R. & Galindo, J. S. (Dezembro 6 de 2017). La Suprema Corte confirma sentencia contra Google en México. El Economista. Disponível em: <https://www.eleconomista.com.mx/empresas/Companias-extranjeras-pueden-ser-juzgadas-en-Mexico-SCJN-20171206-0075.html>.

167. Disponível em alguns sistemas jurídicos de língua espanhola, um recurso de amparo é um remédio para a proteção dos direitos constitucionais. Ver: Wikipédia. Recurso de Amparo. Disponível em: <https://en.wikipedia.org/wiki/Recurso_de_amparo>.

168. Internet & Jurisdiction Policy Network. (2017, dezembro). 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#article-6609_2017-12>.

169. Garcia, D. (15 de junho de 2017). Demandan a Google por fraude en México. El Universal. Disponível em: <http://www.eluniversal.com.mx/articulo/nacion/sociedad/2017/06/15/demandan-google-por-fraude>.

170. Reyes, J. P. (6 de dezembro de 2017). Google se desiste de amparo la Suprema corte. Excelsior. Disponível em: <http://www.excelsior.com.mx/nacional/2017/12/06/1206075>. Ver também uma situação um pouco semelhante na Colômbia, disponível em: <http://www.corteconstitucional.gov.co/relatoria/autos/2018/a285-18.htm>.

171. Ver, por exemplo, o artigo 19, n.o 3 do ICCPR.

172. Hornyak. T. (16 de abril de 2013). Google loses autocomplete defamation suit in Japan. CNet. Disponível em: <https://www.cnet.com/news/google-loses-autocomplete-defamation-suit-in-japan/>.

173. Swinson, J, Lai, P. & English, J. (13 de junho de 2018). Google this: The High Court allows Google to be sued for defamation. King and Wood Mallesons. Disponível em: <https://www.kwm.com/en/au/knowledge/insights/trkulja-v-google-high-court-australia-appeal-20180613> e Google Inc contra Duffy [2017] SASCFC 130.

174. Lau, S. (6 de agosto de 2014). Hong Kong tycoon can sue Google over 'autocomplete' search suggestions, court rules. South China Morning Post. Disponível em: <https://www.scmp.com/news/hong-kong/article/1567521/hong-kong-court-rules-tycoon-can-sue-google-over-autocomplete-search>.

175. Ver, por exemplo: Case of former German First Lady: Niggemeier, S. (20 de setembro de 2012). Autocompleting Bettina Wulff: Can a Google function be libelous? Spiegel Online. Disponível em: <http://www.spiegel.de/international/zeitgeist/google-autocomplete-former-german-first-lady-defamation-case-a-856820.html>.

176. Global Freedom of Expression, Columbia University. Delfi AS contra Estônia. Disponível em: <https://globalfreedomofexpression.columbia.edu/cases/delfi-as-v-estonia/>.

177. Institute of International Law. (2019, agosto). Resolution concerning injuries to rights of personality through the use of the Internet: Jurisdiction, applicable law and recognition of foreign judgments. Disponível em: <http://www.idi-iil.org/app/uploads/2019/09/8-RES-EN.pdf>.

178. Institute of International Law. (2019, agosto). Resolution concerning injuries to rights of personality through the use of the Internet: Jurisdiction, applicable law and recognition of foreign judgments. Disponível em: <http://www.idi-iil.org/app/uploads/2019/09/8-RES-EN.pdf>.

179. Council of Attorneys-General. (2019, fevereiro). Review of model defamation provisions. Disponível em: <https://www.justice.nsw.gov.au/justicepolicy/Documents/review-model-defamation-provisions/Final-CAG-Defamation-Discussion-Paper-Feb-2019.pdf>.

180. Office of the Privacy Commissioner of Canada. (2018). Draft OPC Position on online reputation. Disponível em: <https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-online-reputation/pos_or_201801/>.

181. Ungku, F. (20 de novembro de 2018). Singapore lawmaker blasts Facebook over refusal to take down 'false' post. Reuters. Disponível em: <www.reuters.com/article/us-singapore-politics-facebook/singapore-lawmaker-blasts-facebook-over-refusal-to-take-down-false-post-idUSKCN1NP0KZ?feedType=RSS&feedName=technologyNews>.

182. Internet & Jurisdiction Policy Network. (2018, novembro). Singapore threatens antimisinformation regulation following Facebook refusal to take down post critical of government. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7682_2018-11>.

183. Council of Europe. (19 de outubro de 2018). Draft study on forms of liability and jurisdictional issues in the application of civil and administrative defamation laws in Council of Europe member states. MSIAUT (2018) 04. Disponível em: <https://rm.coe.int/draft-study-on-forms-of-liability-and-jurisdictional-issues-in-the-app/16808ef307>.

184. Law Commission of Ontario. Defamation in the Internet age. Disponível em: <https://www.lco-cdo.org/en/our-current-projects/defamation-law-in-the-internet-age/>.

185. Law Commission of Ontario. Defamation in the Internet age: Consultation paper. Disponível em: <http://www.lco-cdo.org/wp-content/uploads/2017/12/Defamation-Consultation-Paper-Eng.pdf> , pp. 6973.

186. Council of Europe. (4 de julho de 2012). Declaration by the Committee of Ministers on the Desirability of International Standards dealing with Forum Shopping in respect of Defamation. Disponível em: <https://www.coe.int/en/web/freedom-expression/committee-of-ministers-adopted-texts/-/asset_publisher/C10Tb8ZfKDoJ/content/declaration-of-the-committee-of-ministers-on-the-desirability-of-international-standards-dealing-with-forum-shopping-in-respect-of-defamation-libel-to?inheritRedirect=false>.

187. Por exemplo, esta questão foi especificamente levantada, nas perguntas suplementares de junho de 2019 aos atores, pelo Conselho de Advogados-Geral da Austrália na Revisão do Modelo das Provisões de Difamação.

188. Ver, por exemplo: Processos C-509/09 e-Date Advertising GmbH e o./X e Société MGN Limited e C-161/10 Martinez e Martinez.

189. Ver, por exemplo: Processo C-68/93, Fiona Shevill, Ixora Trading Inc., Chequepoint SARL e Chequepoint International Ltd/Presse Alliance SA.

190. Processo C194/16 Bolagsupplysningen OÜ Ingrid Ilsjan contra Svensk Handel AB.

191. Processo C-194/16 Bolagsupplysningen OÜ Ingrid Ilsjan/Svensk Handel AB, para. 50. Ver mais em: Van Calster. G. Close, but no sigar. The CJEU on libel, Internet and centre of interests in Bolagsupplysningen. Disponível em: <:https://gavclaw.com/2017/11/15/close-but-no-sigar-the-cjeu-on-libel-internet-and-centre-of-interests-in-bolagsupplysningen/>.

192. Processo C18/18 GlawischnigPiesczek.

193. Parecer do Advogado-Geral Szpunar no caso Glawischnig-Piesczek (Processo C18/18). O parecer é analisado detalhadamente em Keller. D. Dolphins in the net: Internet content filters and the Advocate General's Glawischnig-Piesczek contra Facebook Ireland Opinion. Disponível em: <https://cyberlaw.stanford.edu/files/Dolphins-in-the-Net-A-G-Analysis.pdf>, van Calster. G,.The Internet's not written in pencil, it's written in ink. Szpunar AG in Eva Glawischnig-Piesczek contra Facebook, re i.a. jurisdiction and removal of hate speech. (As well as confirming my reading of his Opinion in Google). Disponível em: <https://gavclaw.com/2019/06/07/the-internets-not-written-in-pencil-its-written-in-ink-szpunar-ag-in-eva-glawischnig-piesczek-v-facebook-re-i-a-jurisdiction-and-removal-of-hate-speech-as-well-as-confirming-my/> e em Svantesson. D. Grading AG Szpunar's Opinion in Case C18/18 – A caution against worldwide content blocking as default. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3404385>.

194. Conclusões do Advogado-Geral Szpunar no caso Glawischnig-Piesczek (Processo C18/18). Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=PT&mode=lst&dir=&occ=-first&part=1&cid=174621>. Acesso em: 23 de setembro de 2020. , para. 109.

195. Processo C18/18 GlawischnigPiesczek. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218621&pageIndex=0&doclang=PT&mode=req&dir=&occ=-first&part=1&cid=1956673>. Acesso em: 23 de setembro de 2020. Acesso em: 23 de setembro de 2020. > , para 52. Ver mais em: Smith, G. (2019, outubro). Bird & Bird. Disponível em: <https://www.twobirds.com/en/news/articles/2019/global/notice-and-stay-down-orders-and-impact-on-online-platforms#__prclt=pzS67trR>. \, e van Calster, G. (10 de outubro de 2019). Steady now. Eva Glawischnig-Piesczek contra Facebook. The CJEU on jurisdiction and removal of hate speech. GAVC Law. Disponível em: <https://gavclaw.com/tag/c-18-18>.

196. Conclusões do Advogado-Geral Szpunar no caso Glawischnig-Piesczek (Processo C18/18). Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=214686&pageIndex=0&doclang=PT&mode=lst&dir=&occ=-first&part=1&cid=174621>. Acesso em: 23 de setembro de 2020, para 100.

197. Swami Ramdev & Anr. contra Facebook, Inc. & Ors. em 23 de outubro de 2019, High Court of Delhi em New Delhi CS (OS) 27/2019. Disponível em: <http://lobis.nic.in/ddir/dhc/PMS/judgement/23-10-2019/>.

198. Deery, S. (26 de março de 2019) . Victorian DPP wants reporters and jailed for coverage of George Pell case. Herald Sun. Disponível em: <https://www.heraldsun.com.au/news/law-order/victorian-dpp-wants-reporters-and-media-jailed-for-coverage-of-george-pell-case/news-story/86e42945bcdc22158738128f235b8ded>.

199. Durkin, P. (20 de junho de 2017). Outdated contempt laws need overhaul says leading law expert. Australian Financial Review. Disponível em: <https://www.afr.com/companies/professional-services/outdated-contempt-laws-need-overhaul-says-leading-law-expert-20170620-gwup7p>.

200. Victorian Law Reform Commission. Contempt of Court Consultation Paper. Disponível em: <https://www.lawreform.vic.gov.au/projects/contempt-court-judicial-proceedings-reports-act-1958-and-enforcement-processes/contempt>, nas páginas 163-164.

201. Para uma visão sobre a experiência da Colômbia com o cyberbullying, por exemplo, consulte: <http://www.corteconstitucional.gov.co/relatoria/2016/T-281A-16.htm> e <http://www.corteconstitucional.gov.co/relatoria/2014/T-365-14.htm >. Os últimos desenvolvimentos em Hong Kong são articulados em: Privacy Commissioner for Personal Data. (8 de outubro de 2019). PCPD's Updates on Doxxing and Cyberbullying. [Press Release]. Hong Kong. Disponível em: <https://www.pcpd.org.hk/english/news_events/media_statements/press_20191008.html>.

202. Por exemplo, um especialista pesquisado referiu-se ao artigo 71 bis do Código de Contravenções da Cidade de Buenos Aires, Argentina, que se refere especialmente à difusão não autorizada de fotos e vídeos íntimos na Internet ("qualquer tipo de meio de comunicação eletrônica"), bem como ao artigo 493 do Projeto de lei do Código Penal da Argentina. Disponível em: <http://www.pensamientopenal.com.ar/system/files/2018/06/legislacion46694.pdf>.

203. Ver, por exemplo: Davis, A. (5 de abril de 2017). Using technology to protect intimate images and help build a safe community. Facebook newsroom. Disponível em: <https://newsroom.fb.com/news/2017/04/using-technology-to-protect-intimate-images-and-help-build-a-safe-community/>.

204. Timebase. (13 de setembro de 2018). Criminalising the nonconsensual online sharing of intimate images. Disponível em: <https://www.timebase.com.au/news/2018/AT04790-article.html>.

205. Australian eSafety Commissioner. Disponível em: <https://www.esafety.gov.au/>.

206. Child Dignity Alliance. (2018, novembro). Child Dignity Alliance Technical Working Group Report. Disponível em: <https://www.childdignity.com/technical-working-group-report>.

207. Internet Watch Foundation. Disponível em: <https://www.iwf.org.uk>.

208. 5Rights Foundation. Disponível em: <https://5rightsfoundation.com>.

209. Freedom House. (2017). Freedom on the net 2017: Manipulating social media to undermine democracy. Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2017>.

210. Freedom House. (2018). Freedom on the net 2018: The rise of digital authoritarianism. Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2018/rise-digital-authoritarianism>.

211. Reuters Institute for the Study of Journalism. (2018). Reuters Institute Digital News Report 2018. Disponível em: <http://media.digitalnews-report.org/wp-content/uploads/2018/06/digital-news-report-2018.pdf?x89475>, p. 9.

212. Twitter Safety. (19 de agosto de 2019). Information operations directed at Hong Kong. Disponível em: <https://blog.twitter.com/en_us/topics/company/2019/information_operations_directed_at_Hong_Kong.html>.

213. Human Rights Watch. (25 de julho de 2019). Philippines: Reject sweeping 'Fake News' Bill. Disponível em: <https://www.hrw.org/news/2019/07/25/philippines-reject-sweeping-fake-news-bill>.

214. Russell, J. (9 de maio de 2019). Singapore passes controversial 'fake news' law which critics fear will stifle free speech. Tech Crunch. Disponível em: <https://techcrunch.com/2019/05/09/singapore-fake-news-law/>.

215. UK Digital, Culture, Media and Sport Select Committee. (2019, fevereiro). Disinformation and fake news: final report. Disponível em: <https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/1791.pdf>.

216. UK Digital, Culture, Media and Sport Select Committee. (2019, abril). Online Harms White Paper. Disponível em: https://assets.publishing.service. gov.uk/goverment/uploads/system/uploads/attachment_data/file/793360/on-line_harms_white_paper.pdf. Para uma discussão, consulte por exemplo: Smith, D. (5 de maio de 2019). The rule of law and the Online Harms White Paper. Cyberleagle. Disponível em: <https://www.cyberleagle.com/2019/05/the-rule-of-law-and-online-harms-white.html>.

217. Phartiyal, S. (7 de dezembro de 2018). India government meets with WhatsApp over tracing of fake news: source. Reuters. Disponível em: <https://www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/declaration-internet-17-19/>.

218. Internet & Jurisdiction Policy Network. (2018, dezembro). Indian government officials meet with WhatsApp representatives over traceability of misinformation leading to violence. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7734_2018-12>.

220. Internet & Jurisdiction Policy Network. (2018, outubro). Facebook announces removal of pages and accounts for breaking rules against coordinated inauthentic behaviour, including some linked to Iran. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7558_2018-10>.

221. Gleicher, N. (26 de outubro de 2018). Taking down coordinated inauthentic behavior from Iran. Facebook Newsroom. Disponível em: <https://newsroom.fb.com/news/2018/10/coordinated-inauthentic-behavior-takedown/>.

222. Sipalan, J. (12 de setembro de 2018). Malaysia opposition blocks repeal of 'fake news' law in challenge to Mahathir. Reuters. Disponível em: <www.reuters.com/article/us-malaysia-politics-fakenews/malaysia-opposition-blocks-repeal-of-fake-news-law-in-challenge-to-mahathir-idUSKCN1LS0WO>.

223. Pigman, L. (22 de julho de 2018). Russia, Accused of faking news, unfurls its own 'fake news' Bill. The New York Times. Disponível em: <https://www.nytimes.com/2018/07/22/world/europe/russia-fake-news-law.html>.

224. Internet & Jurisdiction Policy Network. (julho de 2018). Russia: Proposed Bill would require platforms to remove 'factually inaccurate posts'. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7180_2018-07>.

225. Baker, S. (2019, março). Vladimir Putin signed a restrictive new law that makes it illegal to insult government officials. Business Insider. Disponível em: <https://www.businessinsider.com/vladimir-putin-law-illegal-insult-him-government-2019-3?IR=T>.

226. Committee to Protect Journalists. (10 de maio de 2018). Gambia declares criminal defamation unconstitutional, keeps some laws on sedition, fake news. Disponível em: <https://cpj.org/2018/05/gambia-declares-criminal-defamation-unconstitution.php>.

227. Internet & Jurisdiction Policy Network. (2018, maio). Gambia Supreme Court upholds prohibition of spreading misinformation online, in spite of recent ECOWAS Court ruling. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7044_2018-05>.

228. International Federation of Library Associations and Institutions. (2018). IFLA statement on fake news. Disponível em: <https://www.ifla.org/publicações/node/67341> .

229. Freedom House. (2018). Internet freedom: Election monitor. Disponível em: <https://freedomhouse.org/report/special-reports/internet-freedom-election-monitor>.

230. Cederberg, G. (7 de setembro de 2018). Catching Swedish phish: How Sweden is protecting its 2018 elections. Belfer Centre for Science and International Affairs. Disponível em: <https://www.belfercenter.org/publication/catching-swedish-phish-how-sweden-protecting-its-2018-elections>.

231. União Europeia (26 de setembro de 2018). Código de Conduta sobre Desinformação. Disponível em: <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59123>. Acesso em: 23 de setembro de 2020.

232. União Europeia (26 de setembro de 2018). Código de Conduta sobre Desinformação. Disponível em: <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59123>. Acesso em: 23 de setembro de 2020, p.4.

233. European Commission. (28 de fevereiro de 2019). First monthly intermediate results of the EU Code of Practice against disinformation. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/first-monthly-intermediate-results-eu-code-practice-against-disinformation>.

234. European Commission. (2019, maio). Code of Practice against disinformation: Commission recognises platforms' efforts ahead of the European elections. Disponível em: <https://europa.eu/rapid/pressrelease_MEX192613_en.htm> .

235. European Commission. (12 de março de 2018). Final Report of the High Level Expert Group on Fake News and Online Disinformation. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation>.

236. Internet Society. (2018, setembro). The Internet and extraterritorial application of laws. Disponível em: <https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf>, p.24.

237. Internet Society. (2018, setembro). The Internet and extraterritorial application of laws. Disponível em: <https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf>, p.24.

238. Government of Canada. Online disinformation. Disponível em: <https://www.canada.ca/en/canadian-heritage/services/online-disinformation.html>.>. Notar também: Iniciativa de Diversidade de Conteúdo do Governo do Canadá, ver: Government of Canada. Diversity of content in the digital age. Disponível em: <https://www.canada.ca/en/canadianheritage/services/diversity-contentdigital-age.html>. Um dos atores entrevistados enfatizou o impacto da desinformação sobre os cidadãos e sobre a coesão social.

239. Oxford Internet Institute. The Computational Propaganda Project. Disponível em: <https://comprop.oii.ox.ac.uk/about-the-project/>.

240. Ver mais em: Pfefferkorn. R, (2019, setembro). Too good to be true? "Deep fakes" pose a new challenge for trial courts. NWLawyer. Disponível em: <http://nwlawyer.wsba.org/nwlawyer/sept_2019/MobilePagedReplica.action?pm=2&folio=22> ; Browne, R. (7 de dezembro de 2018). Antielection meddling group makes A.I. powered Trump impersonator to warn about 'deep fakes'. CNBC. Disponível em: <https://www.cnbc.com/2018/12/07/deepfake-ai-trump-impersonator-highlights-election-fake-news-threat.html>; Bloomberg. (11 de setembro de 2018). How faking videos became easy: and why that's so scary. Fortune. Disponível em: <http://fortune.com/2018/09/11/deep-fakes-obama-video/>; Alliance of Democracies. The Campaign for Democracy. Disponível em: <http://www.allianceofdemocracies.org/initiatives/the-campaign/>; e Council on Foreign Relations. (16 de outubro de 2018). Disinformation on Steroids. Disponível em: <https://www.cfr.org/report/deep-fake-disinformation-steroids>.

241. Mas também outros, como a Austrália: Packham, C. (16 de setembro de 2019). Exclusive: Australia concluded China was behind hack on parliament, political parties – sources. Reuters. Disponível em: <https://www.reuters.com/article/us-australia-china-cyber-exclusive-idUSKBN1W00VF>. Em caráter mais geral, ver: Bisen, A. (24 de abril de 2019). Disinformation is drowning democracy. Foreign Policy. Disponível em: <https://foreignpolicy.com/2019/04/24/disinformation-is-drowning-democracy/>.

242. Um especialista consultado apontou para tais convites na Alemanha, França, Bélgica, Países Baixos, Paraguai, Argentina e Peru.

243. United States of America contra Netyksho et al (Case 1:18cr00215ABJ). Disponível em: <https://www.justice.gov/file/1080281/download>.

244. New Knowledge. The tactics and tropes of the Internet Research Agency. Disponível em: <https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf>, p.3.

245. New Knowledge. The tactics and tropes of the Internet Research Agency. Disponível em: <https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf>, p. 7.

246. New Knowledge. The tactics and tropes of the Internet Research Agency. Disponível em: <https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf> , p. 8.

247. New Knowledge. The tactics and tropes of the Internet Research Agency. Disponível em <https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf>, p. 9.

248. New Knowledge. The tactics and tropes of the Internet Research Agency. Disponível em: <https://disinformationreport.blob.core.windows.net/disinformation-report/NewKnowledge-Disinformation-Report-Whitepaper.pdf>, p.100-101.

249. Oxford Internet Institute. Computational Propaganda Research Project. The IRA, social media and political polarization in the United States, 2012-2018. Disponível em: <https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/12/IRA-Report-2018.pdf>.

250. Mueller, R.S. (2019). Report on the Investigation into Russian Interference in the 2016 Presidential Election. Disponível em: <https://www.justice.gov/storage/report.pdf>.

251. Spring, J. & Brito, R. (20 de outubro de 2018). Brazil election battle rages over Facebook's WhatsApp. Reuters. Disponível em: <https://www.reuters.com/article/us-brazil-election-facebook/brazil-election-battle-rages-over-facebooks-whatsapp-idUSKCN1MT2WP?feedType=RSS&feedName=technologyNews>.

252. Internet & Jurisdiction Policy Network. (2018, outubro). WhatsApp announced legal action against companies spreading misinformation ahead of Brazilian elections. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7550_2018-10>.

253. Ver, por exemplo: Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2019, junho). Research paper 1/2019: Freedom of expression and elections in the digital age. Disponível em: <https://www.ohchr.org/Documents/Issues/Opinion/ElectionsReportDigitalAge.pdf> .

254. Internetstiftelsen i Sverige. (2018). Svenskarna och Internet valspecial 2018. Disponível em: <https://www.iis.se/docs/Svenskarna_och_internet-_valspecial_2018>, p. 9.

255. Criminal Code (R.S.C., 1985, c. C46), section 181.

256. R contra Zundel [1992] 2 S.C.R. 731.

257. Lima, C. & Briz, A. (7 de outubro de 2018). Is this true? A fake news database. Politico. Disponível em: <https://www.politico.com/interactives/2018/is-this-true/about>.

258. União Europeia. Regulamento (UE) 2016/679 do Parlamento e do Conselho Europeu, de 27 de abril de 2016, relativo à proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, e que revoga a Diretiva 95/46/CE. Disponível em: <https://op.europa.eu/pt/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1>. Acesso em: 24 de setembro de 2020.

259. Ranking Digital Rights. (2019).2019 Ranking Digital Rights Corporate Accountability Index. Disponível em: <https://rankingdigitalrights.org/index2019/>.

260. Greenleaf, G. (31 de janeiro de 2017). Global tables of data privacy laws and bills (5th Ed 2017). Privacy Laws & Business International Report 145, 14-26. Disponível em: <https://ssrn.com/abstract=2992986>. Ver também: United Nations Conference on Trade and Development. Data Protection and Privacy Legislation Worldwide. Disponível em: <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx>.

261. Sabiiti, D. (3 de julho de 2019). Rwanda working on a Personal Data Protection Law. KT Press. Disponível em: <https://ktpress.rw/2019/07/rwanda-working-on-a-personal-data-protection-law/>.

262. UK Information Commissioner. (20 de junho de 2019). Update Report into AdTech and Real Time Bidding. Disponível em: <https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906.pdf>.

263. Personal Data Protection Commission Singapore. (fevereiro de 2019). Discussion paper: Data portability. Disponível em: <https://www.pdpc.gov.sg/help-and-resources/2019/02/data-portability-discussion-paper>.

264. Internet & Jurisdiction Policy Network. (fevereiro de 2019). Nigerian agency releases draft Data Protection Regulation. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoibmlnZXJpYSIsImZyb20iOiIyMDE5LTAxIiwidG8iOiIyMDE5LTA4In0=>.

265. Innovation, Science and Economic Development Canada. (2019). Canada's Digital Charter: Trust in a digital world. Disponível em: <https:www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html>.

266. Blaszcyk, W.N. (3 de janeiro de 2019). Finland: Data Protection Act enters into force after being "significantly delayed". Data Guidance. Disponível em: <https://www.dataguidance.com/finland-new-data-protection-act-enters-into-force-after-being-significantly-delayed/>.

267. Internet & Jurisdiction Policy Network. (2018, setembro). Argentina's draft Data Protection Bill introduced in parliament. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7465_2018-09>.

268. Internet & Jurisdiction Policy Network. (2018, agosto). Brazil: President signs Data Protection Bill into law. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7465_2018-09>.

269. Internet & Jurisdiction Policy Network. (julho de 2018). Kenya: Data Protection Bill introduced in Parliament. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7190_2018-07>.

270. Hunton Andrews Kurth. (2018, 28 de junho). Protection of personal data now a constitutional right in Chile. Privacy and Information Security Law Blog. Disponível em: <https://www.huntonprivacyblog.com/2018/06/28/protection-personal-data-now-constitutional-right-chile/>.

271. Internet & Jurisdiction Policy Network. (junho de 2018). Chile passes amendment making data protection a constitutional right. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7071_2018-06>.

272. California Consumer Privacy Act of 2018, 1798.140. C(1)(a).

273. Internet Association. Policy position: Privacy. Disponível em: <https://internetassociation.org/positions/privacy/>.

274. Ver também: Tsukayama, H. (4 de setembro de 2019). Lawmakers Must Not Listen to the Internet Association and Weaken the California Consumer Privacy Act. Electronic Frontier Foundation. Disponível em: <https://www.eff.org/deeplinks/2019/09/lawmakers-must-not-let-internet-association-weaken-california-consumer-privacy-act>.

275. Internet & Jurisdiction Policy Network. (2019, agosto). Australia passes Consumer Data Rights Bill. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiY29uc3VtZXIgZGF0YSIsImZyb20iOiIyMDEyLTAyIiwidG8iOiIyMDE5LTA4In0=>.

276. Justice K. S. Puttaswamy (Retd.) e Anr. contra Union Of India And Or, Writ Petition (Civil) No.494 de 2012 (Sup. Ct. India. ago 24, 2017).

277. PRS Legislative Research. Draft Personal Data Protection Bill, 2018. Disponível em: <https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018>.

278. United Nations Conference on Trade and Development. (2016). Data protection regulations and international data flows: Implications for trade and development. Disponível em: <https://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf>.

279. European Commission. Proposal for an ePrivacy regulation. Disponível em: <https://ec.europa.eu/digital-single-market/en/proposal-eprivacy-regulation>. Uma discussão sobre a relação entre o GDPR e a atual Diretiva ePrivacidade pode ser encontrada aqui: European Data Protection Board. (12 de março de 2019). Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities. Disponível em: <https://edpb.europa.eu/our-work-tools/our-documents/noukogu-arvamus-artikkel-64/opinion-52019-interplay-between-eprivacy_en>.

280. Ver, por exemplo: United Nations Special Rapporteur on the Right to Privacy. (2019). Report of the Special Rapporteur on the Right to Privacy to Human Rights Council. A/HRC/40/63. Disponível em: <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/A_HRC_40_63.DOCX>; United Nations Special Rapporteur on the Right to Privacy Task Force on Health Data. (2019). Draft recommendation on the protection and use of healthrelated data. Disponível em: <https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc>.

281. Office of the United Nations High Commissioner for Human Rights. (2014). Report of the High Commissioner for Human Rights on the right to privacy in the digital age. A/HRC/27/37. Disponível em: <https://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc>.

282. Global Network Initiative. The GNI Principles. Disponível em: <https://globalnetworkinitiative.org/gni-principles/>.

283. Global Network Initiative. (20 de março de 2017). GNI publishes updates to the core commitments of our membership. Disponível em: <https://globalnetworkinitiative.org/gni-publishes-updates-to-the-core-commitments-of-our-membership/>.

284. International Federation of Library Associations and Institutions. IFLA Statement on Privacy in the Library Environment. Disponível em: <https://www.ifla.org/publications/node/10056>.

285. Center for Democracy and Technology. (13 de dezembro de 2018). CDT's Federal Baseline Privacy Legislation. Disponível em: <https://cdt.org/insight/cdts-federal-baseline-privacy-legislation-discussion-draft>.

286. International Conference on Data Protection and Privacy Commissioners. Disponível em: <https://icdppc.org>.

287. Asia Pacific Privacy Authorities. Disponível em: <http://www.appaforum.org>.

288. Rede Iberoamericana de Proteção de Dados. Disponível em: <https://www.redipd.org/pt-pt>. Acesso em: 24 de setembro de 2020.

289. Rede latino-americana de estudos sobre vigilância, tecnologia e sociedade. Disponível em: <http://lavits.org/?lang=pt>. Acesso em: 12 de outubro de 2020.

290. Comité Europeu para a Proteção de Dados. Disponível em: <https://edpb.europa.eu/about-edpb/about-edpb_pt>. Acesso em: 12 de outubro de 2020.

291. African Network of Data Protection Authorities. Disponível em: <https://apdp.bj/>.

292. Central and Eastern Europe Data Protection Authorities. Disponível em: <http://www.ceecprivacy.org/main.php?s=2>.

293. Ver mais em: Diretrizes 3/2018 sobre o âmbito de aplicação territorial do RGPD (artigo 3.º) (adotadas em 16 de novembro de 2018). Disponível em: <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_pt.pdf>. Acesso em: 12 de outubro de 2020, Taylor, M. (2018). Transatlantic jurisdictional conflicts in data protection law: How the fundamental right to data protection conditions the European Union's exercise of extraterritorial jurisdiction. (Dissertation). Utrecht University. Disponível em: <https://dspace.library.uu.nl/handle/1874/367936>, e Kuner, C., Bygrave, L.A. & Docksey, C. (Eds.). (2019). Commentary on the EU General Data Protection Regulation. - Owford. Oxford University Press.

294. Data Verified Joseph. Websites not available in the European Union after GDPR. Disponível em: <https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr>.

295. Thailand's Personal Data Protection Bill 2018.

296. Charter of Fundamental Rights of the European Union. (2000/C 364/01), Article 8.

297. Processo C131/12 Google Spain SL e Google Inc. contra Agencia Española de Protección de Datos (AEPD) e Mario Costeja González. Disponível em: <http://curia.europa.eu/juris/fiche.jsf?id=C%3B131%3B12%3BRP%3B1%3BP%3B1%3BC2012%2F0131%2FJ&oqp=&for=&mat=or&lgrec=pt&jge=&td=%3BALL&jur=C%2CT%2CF&num=131%252F12&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791#section_titre>. Acesso em: 12 de outubro de 2020. Ver mais: van Alsenoy, B., Kuczerawy, A. & Ausloos, J. (2013), Search engines after 'Google Spain': Internet @Liberty ou Privacy @Peril? ICRI Research Paper 15 TPRC 41. The 41st Research Conference on Communication, Information and Internet Policy. Disponível emSSRN: <https://ssrn.com/abstract=2321494> ou <http://dx.doi.org/10.2139/ssrn.2321494>, e Lindsay, D. (2014). The "Right to be Forgotten" by search engines under data privacy law: A legal analysis of the Costeja ruling. Journal of Media Law, 6(2), 159; e Lynskey, O. (2015). Control over personal data in a digital age: Google Spain contra AEPD and Mario Costeja Gonzalez. The Modern Law Review, 78(3), 522.

298. Masnick, M. (16 de outubro de 2018). Canadian Privacy Commissioner goes to court to determine if Canada can force Google to delete history. Tech Dirt. Disponível em: <https://www.techdirt.com/articles/20181013/23132640833/canadian-privacy-commissioner-goes-to-court-to-determine-if-canada-can-force-google-to-delete-history.shtml>.

299. Ver, por exemplo: Kohl, U & Rowland, D. (2017). Censorship and Cyberborders through EU Data Protection Law. Em: Kohl, U. (Ed.). The net and the nation state. - Cambridge. Cambridge University Press, 93-109.

300. Datainspektionen överklagar Googledom. (30 de maio de 2018). DataInspektionen. Disponível em: <https://www.datainspektionen.se/nyheter/datainspektionen-overklagar-google-dom/>.

301. Tribunal de Justiça da União Europeia. (10 de janeiro de 2019). O advogado-geral M. Szpunar propõe ao Tribunal de Justiça que limite à escala da União Europeia a supressão de hiperligações a que os operadores de motores de busca são obrigados a proceder. [Comunicado de imprensa]. Luxemburgo. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002pt.pdf >. Acesso em: 25 de setembro de 2020.

302. Tribunal de Justiça da União Europeia. (10 de janeiro de 2019). O advogado-geral M. Szpunar propõe ao Tribunal de Justiça que limite à escala da União Europeia a supressão de hiperligações a que os operadores de motores de busca são obrigados a procede. [Comunicado de imprensa]. Luxemburgo. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002pt.pdf >. Acesso em: 25 de setembro de 2020.

303. Processo C507/17 Google LLC, sucessor processual de Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL), para 74. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020. Ver mais: van Calster, G. (2019). Court of Justice in Google sees no objection in principle to EU 'Right to be forgotten' leading to worldwide delisting orders. Holds that as EU law stands, however, it is limited to EUwide application, leaves the door open to national authorities holding otherwise. GAVC Law. Disponível em: <https://gavclaw.com/2019/09/25/court-of-justice-sees-no-objection-in-principle-to-eu-right-to-be-forgotten-leading-to-worldwide-delisting-orders-holds-that-as-eu-law-stands-however-it-is-limited-to-eu-wide-application-leave/>; e Svantesson, D.(2019, 24 de setembro). The Court of Justice of the European Union steers away from global removal orders. LinkedIn. Disponível em: <https://www.linkedin.com/pulse/court-justice-european-union-steers-away-from-global-svantesson/>.

304. Processo C507/17 Google LLC, sucessor processual de Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL), para 59.Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020.

305. Processo C507/17 Google LLC, sucessor processual de Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL), para 60. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020.

306. Processo C507/17 Google LLC, sucessor processual de Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL), para 60. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020.

307. Processo C507/17 Google LLC, sucessor processual de Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL), para 61. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020.

308. Processo C507/17 Google LLC, sucessor processual de Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL), para 62. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020.

309. Processo C507/17 Google LLC, sucessor processual de Google Inc. contra Commission nationale de l'informatique et des libertés (CNIL), para 72. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=507%252F17&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020. Esta abordagem diferenciada foi inicialmente analisada em detalhes em: Svantesson, D. J. B. (2015). The Google Spain case: Part of a harmful trend of jurisdictional overreach. EUI Working Paper RSCAS 2015/45. Disponível em <https://cadmus.eui.eu/bitstream/handle/1814/36317/RSCAS_2015_45.pdf?sequence=1>.

310. Bentzen, H. B. et al., (2019). Are requirements to deposit data in research repositories compatible with the European Union's General Data Protection Regulation?, Annals of Internal Medicine, 170(5), 332334

311. OECD Guidelines on the protection of privacy and transborder flows of personal data. Disponível em: <http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm>.

312. Ver, por exemplo: Toy, A. & Gunasekara, G. (2019). Is there a better option than the data transfer model to protect data privacy? University of New South Wales Law Journal, 42(2), 719746.

313. Processo C362/14 Maximillian Schrems contra Data Protection Commissioner. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=pt&jge=&td=%3BALL&jur=C%2CT%2CF&num=362%252F14&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Acesso em: 12 de outubro de 2020.

314. Processo C311/18 Data Protection Commissioner contra Facebook Ireland Limited e Maximillian Schrems. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=pt&jge=&td=%3BALL&jur=C%2CT%2CF&num=311%252F18&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7920791>. Disponível em: 12 de outubro de 2020.

315. Asia-Pacific Economic Cooperation. APEC Cross Border Privacy Enforcement Arrangement. Disponível em: <https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx>.

316. Cross Border Privacy Rules System. Disponível em: <http://cbprs.org>.

317. Caiyu, L. (13 de junho de 2019). China sets cross-border data flow rules. Global Times. Disponível em: <http://www.globaltimes.cn/content/1154091.shtml>.

318. NelsonDaley, R. (27 de julho de 2017). Colombia: Amended draft transfers regulation seeks to 'address main concern' regarding adequate jurisdictions. DataGuidance. Disponível em: <http://www.dataguidance.com/colombia-amended-draft-data--transfers-regulation-addresses-main-concerns--regarding-list-adequate-jurisdictions/>.

319. Sanlate, G., Gordon, P., Méndez, S.M &, Varela, J. C. (29 de julho de 2013). Colombia adopts regulations to implement its data protection laws. Littler. Disponível em: <https://www.littler.com/publication-press/publication/colombia-adopts-regulations-implement-its-data-protection-laws>.

320. Internet & Jurisdiction Policy Network. (2017, julho). Colombia establishes list of countries with adequate data protection for cross-border transfers. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6188_2017-07>.

321. Sugiyama, S. (2019). Abe heralds launch of 'Osaka Track' framework for free cross-border data flow at G20. Japan Times. Disponível em: <https://www.japantimes.co.jp/news/2019/06/28/national/abe-heralds-launch-osaka-track-framework-free-cross-border-data-flow-g20/#.XY73EGXA5lI>.

3.2

322. World Economic Forum. (2018). The Global Risks Report 2018. (13th ed.). Disponível em: <http://reports.weforum.org/global-risks-2018/>.

323. Para uma discussão interessante, ver: Hataja, S. (2019). Cyber attacks and international law on the use of force: The turn to information ethics. New York: Taylor & Francis Ltd.

324. Council to Secure the Digital Economy. Disponível em: <https://securingdigitaleconomy.org>.

325. Cyber Threat Alliance. Disponível em: <https://www.cyberthreatalliance.org>.

326. Cybersecurity Tech Accord. Disponível em: <https://cybertechaccord.org/accord/>.

327. Forum of Incident Response and Security Teams. Disponível em: <https://www.first.org>.

328. AntiPhishing Working Group. Disponível em: <https://apwg.org>.

329. Messaging, Malware and Mobile AntiAbuse Working Group. Disponível em: <https://www.m3aawg.org>.

330. Mann, M., Warren, I. & Kennedy, S. (2018). The legal geographies of transnational cyber-prosecutions: extradition, human rights and forum shifting. Global Crime, 19(2), 107124. Disponível em: <https://www.tandfonline.com/doi/full/10.1080/17440572.2018.1448272>.

331. Ver: United Nations Conference on Trade and Development. Cybercrime legislation worldwide. Disponível em: <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx>. Ver mais, por exemplo, em: Walden, I. (2016). Computer crimes and digital investigations. (2nd ed.). New York: Oxford University Press.

332. Interpol. Cybercrime. Disponível em: <https://www.interpol.int/Crimes/Cybercrime>.

333. Interpol. ICT Law Projects. Disponível em: <https://www.interpol.int/Who-we-are/Legal-framework/Information-communications-and-technology-ICT-law-projects>.

334. The European Union's Judicial Cooperation Unit. Disponível em: <http://www.eurojust.europa.eu/Pages/home.aspx>.

335. Europol. European Cybercrime Centre EC3. Disponível em: <https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3>.

336. Europol. Joint Cybercrime Action Taskforce (JCAT). Disponível em: <https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce>.

337. Ver mais em: Council of Europe. Action against cybercrime. Disponível em: <https://www.coe.int/en/web/cybercrime/home>.

338. Council of Europe. Budapest Convention and related standards. Disponível em: <https://www.coe.int/en/web/cybercrime/the-budapest-convention>.

339. Council of Europe. Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime. Disponível em:<https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=9zMAKGj4>.

340. Ver mais em: Brown, C.S.D. (2015). Investigating and prosecuting cyber crime: Forensics dependencies and barriers to justice. International Journal of Cyber Criminology, 9:55–119.

341. World Economic Forum. (2018). Centre for Cybersecurity. Disponível em: <https://www.weforum.org/centre-for-cybersecurity>.

342. European Union Agency for Network and Information Security. About ENISA. Disponível em <https://www.enisa.europa.eu/about-enisa>.

343. Kleijssen, J. & Perri, P. (2016). Cybercrime, evidence and territoriality: Issues and options. Netherlands Yearbook of International Law, 47, pp.153-154.

344. Ver, por exemplo: Kleijssen, J. & e Perri, P. (2016). Cybercrime, evidence and territoriality: Issues and options. Netherlands Yearbook of International Law, 47, p.154.

345. Processo C-618/15 Concurrence Sàrl contra Samsung Electronics France SAS e Amazon Services Europe Sàrl, para 2.

346. Europol. (2018). Internet Organised Crime Threat Assessment 2018. Disponível em: <https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf> , p. 7.

347. Wikipédia. Silk Road (marketplace). Disponível em: <https://en.wikipedia.org/wiki/Silk_Road_(marketplace)>. Ver mais em: Mann, M. & Warren, I. (2018). The digital and legal divide: Silk Road, transnational online policing and Southern criminology. In Carrington, K., Hogg, R., Scott, J. & Sozzo, M. (Eds.), The Palgrave handbook of criminology and the global south (pp.245-260). Cham, Suíça: Palgrave Macmillan. Disponível em: <http://dro.deakin.edu.au/view/DU:30105929>. >.

348. Europol. (2018). Internet Organised Crime Threat Assessment 2018. Disponível em: <https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf>, p. 7.

349. Europol. (2018). Internet Organised Crime Threat Assessment 2018. Disponível em: <https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf>, p. 8.

350. Por exemplo, em 2017, a American Library Association publicou suas Suggested Guidelines: How to respond to law enforcement requests for library records and user information. Disponível em: <http://www.ala.org/advocacy/privacy/lawenforcement/guidelines>.

351. Ver mais em: Kent, G. (14 de fevereiro de 2014). Sharing investigation specific data with law enforcement - An international approach. Stanford Public Law Working Paper. Disponível em: <http://dx.doi.org/10.2139/ssrn.2472413>; e Osula, M. (2017). Remote search and seizure of extraterritorial data. - Tartu. University of Tartu Press.

352. Council of Europe, Cybercrime Convention Committee. (16 de setembro de 2016). Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the TCY. TCY (2016) 5, p. 9. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e>.

353. Council of Europe. MLA Council of Europe Standards. Disponível em: <https://www.coe.int/en/web/transnational-criminal-justice-pcoc/MLA-council-of-europe-standards>.

354. Interpol. (12 de novembro de 2018). Interpol's eMLA initiative focus of EU expert meeting. Disponível em: <https://www.interpol.int/News-and-Events/News/2018/INTERPOL-s-e-MLA-initiative-focus-of-EU-expert-meeting>.

355. Em re: Grand Jury Subpoena, No.183071 (D.C. Cir.2019). Disponível em: <https://www.cadc.uscourts.gov/internet/judgments.nsf/DA9F6932C876287F852583680053B08B/$file/18-3071-1764819.pdf>.

356. Osula, AM. & Zoetekouw, M. (2017). The notification requirement in transborder remote search and seizure: Domestic and international law perspectives. Masaryk University Journal of Law and Technology, 11(1), 103–128.

357. Para os últimos desenvolvimentos sobre a redação, ver: Council of Europe, Cybercrime Convention Committee. (8 de julho de 2019). Preparation of the 2nd Additional Protocol to the Budapest Convention on Cybercrime – State of Play. Disponível em: <https://rm.coe.int/t-cy-2019-19-protocol-tor-extension-chair-note-v3/16809577ff>.

358. Council of Europe, Cybercrime Convention Committee. TCY Guidance Note #10 Production orders for subscriber information (Article 18 Budapest Convention). Disponível em: <https://rm.coe.int/16806f943e>.

359. Council of Europe, Cybercrime Convention Committee. (16 de setembro 2016). Criminal justice access to electronic evidence in the cloud: Recommendations for consideration by the TCY. TCY (2016) 5, p. 9. Disponível em: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495>.

360. Council of Europe. (29 de abril de 2019). Use of a 'disconnection clause' in the second additional protocol to the Budapest Convention on Cybercrime. Disponível em: <https://www.coe.int/en/web/dlapil/-/use-of-a-disconnection-clause-in-the-second-additional-protocol-to-the-budapest-convention-on-cybercri-1>.

361. United Nations Office on Drugs and Crime. (1 de fevereiro de 2019). UNODC and partners release Practical Guide for Requesting Electronic Evidence Across Borders. Disponível em: <https://www.unodc.org/unodc/en/frontpage/2019/January/unodc-and-partners-release-practical-guide-for-requesting-electronic-evidence-across-boarders.htm>.

362. Comissão Europeia. (17 de abril de 2018). Proposta de Diretiva do Parlamento e do Conselho Europeu que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal . COM (2018) 226 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0226&from=PT >. Acesso em 27 de setembro de 2020.

363. Comissão Europeia. (17 de abril de 2018). Proposta de Regulamento do Parlamento Europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal. COM (2018) 225 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>. Acesso em: 27 de setembro de 2020.

364. Conselho da União Europeia. (7 de dezembro de 2018). Regulamento relativo ao acesso transfronteiras a provas eletrônicas: Conselho define a sua posição. [Comunicado de Imprensa]. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/>. Acesso em: 27 de setembro de 2020.

365. Conselho Europeu. (8 de março de 2019). Pacote legislativo em matéria de provas eletrônicas: Conselho define a sua posição sobre as normas para designar representantes legais para efeitos de recolha de provas. [Comunicado de Imprensa]. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2019/03/08/e-evidence-package-council-agrees-its-position-on-rules-to-appoint-legal-representatives-for-the-gathering-of-evidence/>. Acesso em: 27 de setembro de 2020.

366. Wikipédia. Microsoft Corp. contra United States. Disponível em: <https://en.wikipedia.org/wiki/Microsoft_Corp._contra_United_States.>

367. Ver mais em: Daskal, J. (31 de janeiro de 2019). Unpacking the CLOUD Act. Disponível em: <https://eucrim.eu/articles/unpackingcloudact/>.

368. British Columbia (Attorney General) v. Brecknell 2018 BCCA 5. Disponível em: <https://www.canlii.org/en/bc/bcca/doc/2018/2018bcca5/2018bcca5.html?resultIndex=1>.

369. Internet & Jurisdiction Policy Network. (2018, janeiro). Canadian provincial Court of Appeal rules courts can demand data from non-Canadian companies if they have 'presence' in the country. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6681_2018-01>.

370. Internet & Jurisdiction Policy Network. Data and Jurisdiction. Disponível em: <https://www.internetjurisdiction.net/work/data-jurisdiction>.

371. Além disso, existem outras iniciativas parcialmente sobrepostas, como: Evidence2e-CODEX. Disponível em: <https://evidence2e-codex.eu>. e Cross-Border Data Forum. Disponível em: <https://www.crossborderdataforum.org/>.

372. Council of Europe Convention on Cybercrime (ETS No.185). Aberto para assinatura em 23 de novembro de 2001 (entrada em vigor em 01 de julho de 2004).

373. Para as propostas concretas, ver: Internet & Jurisdiction Policy Network. Data & Jurisdiction Program Operational Approaches. Disponível em: <http://internetjurisdiction.net/Data-Jurisdiction-Program-Operational-Approaches>. Para o último plano de trabalho, ver 3rd Global Conference of the Internet & Jurisdiction Policy Network. (3 - 5 de junho de 2019). Berlin Roadmap. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/Berlin-Roadmap-and-Secretariat-Summary-3rd-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf>.

374. 2nd Global Conference of the Internet & Jurisdiction Policy Network. (26-28 fevereiro de 2018). Ottawa Roadmap. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/ Secretariat-Summary-and-Ottawa-Roadmap-second-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf> , p. 6-7.

375. Clarifying Lawful Overseas Use of Data Act. S.2383. Disponível em: <https://www.congress.gov/bill/115th-congress/senate-bill/2383/text>.

376. Comissão Europeia. (17 de abril de 2018). Proposta de Regulamento do Parlamento europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal. COM (2018) 225 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>. Acesso em: 27 de setembro de 2020.

377. Comisão Europeia. (17 de abril de 2018). Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal . COM (2018) 226 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0226&from=PT>. Acesso em: 27 de setembro de 2020.

378. Comissão Europeia. (17 de abril de 2018). Proposta de Regulamento do Parlamento europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal. COM (2018) 225 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>. Acesso em: 27 de setembro de 2020, Recital 47.

379. Comissão Europeia. (17 de abril de 2018). Proposta de Regulamento do Parlamento europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrónicas em matéria penal. COM (2018) 225 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>. Acesso em: 27 de setembro de 2020, Recital 52.

380. Wikipédia. PRISM (surveillance program). Disponível em: <https://en.wikipedia.org/wiki/PRISM_(surveillance_program)>.

381. Internet & Jurisdiction Policy Network. (2018, dezembro). India: Government issues order allowing agencies to intercept, monitor and decrypt user data. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7725_2018-12>.

382. Ver, por exemplo: United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. (2019). Report of the Special Rapporteur to the Human Rights Council on surveillance and human rights. A/HRC/41/35. Disponível em: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/148/76/PDF/G1914876.pdf?OpenElement>.

383. Walsh, D. (10 de junho de 2017). Dilemma for Uber and Rival: Egypt's demand for data on riders. The New York Times. Disponível em: <https://www.nytimes.com/2017/06/10/world/middleeast/egypt-uber-sisi-surveillance-repression-careem.html>.

384. Internet & Jurisdiction Policy Network. (2017, junho). Egyptian draft bill would introduce data localization rules for ridesharing services. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6103_2017-06>.

385. Matsakis, L. (29 de julho de 2019). How the West got China's social credit system wrong. Wired. Disponível em: <https://www.wired.com/story/china-social-credit-score-system/>.

386. Carney, M. (18 de setembro de 2018). Leave no dark corner. ABC News. Disponível em: <https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278>.

387. Carney, M. (18 de setembro de 2018). Leave no dark corner. ABC News. Disponível em: <https://www.abc.net.au/news/2018-09-18/china-social-credit-a-model-citizen-in-a-digital-dictatorship/10200278>.

388. Hatton, C. (26 de outubro de 2015). China 'social credit': Beijing sets up huge system. BBC News. Disponível em: <https://www.bbc.com/news/world-asia-china-34592186>.

389. Liu, J. (6 de dezembro de 2018). Is China's social credit system really the dystopian sifi scenario that many fear? Science Nordic. Disponível em: <http://sciencenordic.com/china's-social-credit-system-really-dystopian-si-fi-scenario-many-fear>.

390. Cheng, E. (3 de setembro de 2019). China is building a 'comprehensive system' for tracking companies' activities, report says. CNBC. Disponível em: <https://www.cnbc.com/2019/09/04/china-plans-for-corporate-social-credit-system-eu-sinolytics-report.html>.

391. Processos conjuntos C293/12 e C594/12 Digital Rights Ireland Ltd contra Minister for Communications, Marine and Natural Resources e outros e Kärntner Landesregierung e outros. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&jge=&td=%3BALL&jur=C%2CT%2CF&num=293%252F12&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7953006>. Acesso em: 12 de outubro de 2020.

392. Processos conjuntos C203/15 e C698/15 Tele2 Sverige AB contra Post och telestyrelsen e Secretary of State for the Home Department contra Tom Watson e outros, para 122. Disponível em: <http://curia.europa.eu/juris/liste.jsf?oqp=&for=&mat=or&lgrec=pt&jge=&td=%3BALL&jur=C%2CT%2CF&num=203%252F15&page=1&dates=&pcs=Oor&lg=&pro=&nat=or&cit=none%252CC%252CCJ%252CR%252C2008E%252C%252C%252C%252C%252C%252C%252C%252C%252C%252Ctrue%252Cfalse%252Cfalse&language=pt&avg=&cid=7953006>. Acesso em: 12 de outubro de 2020.

393. Tribunal de Justiça da União Europeia. (2 de outubro de 2018). As infrações penais que não são particularmente graves podem justificar um acesso aos dados pessoais conservados porfornecedores de serviços de comunicações eletrônicas desde que esse acesso não constitua uma ofensa-grave à vida privada. [Comunicado de Imprensa]. Luxemburgo. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2018-10/cp180141pt.pdf>. Acesso em: 27 de setembro de 2020.

394. Internet & Jurisdiction Policy Network. (2018, outubro). ECJ rules law enforcement can access personal data held by telecommunication operators if it does not seriously infringe on privacy. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7552_2018-10>.

395. Ver: Processo C520/18. Para a posição da UE, ver também: Conselho da União Europeia. (6 de junho de 2019). Conservação de dados para lutar contra a criminalidade: Conselho adota conclusões. [Comunicado de Imprensa]. Disponível em: <https://www.consilium.europa.eu/pt/press/press-releases/2019/06/06/data-retention-to-fight-crime-council-adopts-conclusions/>.

396. Internet & Jurisdiction Policy Network. (julho de 2018). Russian law requiring platform and telecommunication operators to retain user correspondence enters into force. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7186_2018-07>.

397. Levine, D. & Menn, J. (18 de agosto de 2018). Exclusive: U.S. government seeks Facebook help to wiretap Messenger sources. Reuters. Disponível em: <https://www.reuters.com/article/us-facebook-encryption-exclusive/exclusive-u-s-government-seeks-facebook-help-to-wiretap-messenger-sources-idUSKBN1L226D>.

398. Internet & Jurisdiction Policy Network. (2018, agosto). US DOJ reportedly asks Facebook to break Messenger's encryption in criminal investigation. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7040_2018-05>.

399. Internet & Jurisdiction Policy Network. (2018, maio). Iran blocks encrypted messaging service Telegram. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7040_2018-05>.

400. Para uma dessas iniciativas, ver: The Carnegie Endowment for International Peace. Encryption Working Group. Disponível em: <https://carnegieendowment.org/programs/technology/cyber/encryption>.

401. Access Now. (6 de dezembro de 2018). Australia joins Russia and China in undermining users' security and threatening human rights. Disponível em: <https://www.accessnow.org/australia-joins-russia-and-china-in-undermining-users-security-and-threatening-human-rights/>.

402. Koen Geens Ministre de la Justice. (4 de outubro de 2017). Quadripartite Maroc / Espagne / France / Belgique. Disponível em: <https://www.koengeens.be/fr/news/2017/10/04/quadripartite-maroc-espagne-france-belgique-1>.

403. Hosenball, M. & Holden, M. (30 de julho de 2019). 'Five Eyes' security alliance calls for access to encrypted material. Reuters. Disponível em: <https://www.reuters.com/article/us-security-fiveeyes-britain/five-eyes-security-alliance-calls-for-access-to-encrypted-material-idUSKCN1UP199>.

404. Ver mais em: Kettemann, M. (2019) "This is not a drill": International law and protection of cybersecurity, in Wagner/Kettemann/Vieth (eds.), Research Handbook of Human Rights and Digital Technology. Cheltenham, Edward Elgar.

405. Thomas, J. (3 de agosto de 2019). Intensifying ASEAN's cybersecurity efforts. The ASEAN Post. Disponível em: <https://theaseanpost.com/article/intensifying-aseans-cybersecurity-efforts>; ASEAN. (2017, 1 de dezembro). ASEAN Telecommunications and Information Technology Ministers. [Joint Media Statement]. Siem Reap, Camboja. Disponível em: <https://asean.org/wp-content/uploads/2012/05/14-TELMIN-17-JMS_adopted.pdf>; ASEAN-United States leaders' statement on cybersecurity cooperation. (2018). Disponível em: <https://asean.org/storage/2018/11/ASEAN-US-Leaders-Statement-on-Cybersecurity-Cooperation-Final.pdf>; Baharudin, H. (20 de setembro de 2018). ASEAN framework on cyber security in the works. Straits Times. Disponível em: <https://www.straitstimes.com/singapore/asean-framework-on-cyber-security-in-the-works>.

406. European Commission. (11 de dezembro de 2018). EU negotiators agree on strengthening Europe's cybersecurity. Disponível em: <https://ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_pt>.

407. Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e das comunicações e que revoga o Regulamento (UE) n.o 526/2013 (Regulamento Cibersegurança).

408. European Commission. (2019). The Directive on security of network and information systems (NIS Directive). Disponível em: <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.

409. Mutually Agreed Norms for Routing Security. Disponível em: <https://www.manrs.org/>.

410. Schnidrig, D. & Kaspar, L. (27 de junho de 2018). Multi-stakeholder approaches to national cybersecurity development. Global Partners Digital. Disponível em: <https://www.gp-digital.org/publication/multistakeholder-approaches-to-national-cybersecurity-strategy-development/>.

411. Paris call for trust and security in cyberspace. (12 de novembro de 2018). Disponível em: <https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf>.

412. Ver, por exemplo: Roigas, H. & Minarik, T. (2015). UN GGE Report:: Major players recommending norms of behavior, highlighting aspects of international law. NATO Cooperative Cyber Defence Centre of Excellence. Disponível em: <https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/>; e Grigsby, A. (15 de novembro de 2018). The United Nations doubles its workload on cyber norms, and not everyone is pleased. Council of Foreign Relations. Disponível em: <https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms--and-not-everyone-pleased>.

413. Global Commission on the Stability of Cyberspace. (2018). Disponível em: <https://cyberstability.org/about/>.

414. Shanghai Cooperation Organisation. (16 de maio de 2019). SCO participation at the 4th Central Asian Internet Governance Forum: Internet for Increasing capacities in central Asia. Disponível em: <http://eng.sectsco.org/news/20190516/540999.html>.

415. Organization for Security and Cooperation in Europe. (19 de junho de 2019). Officials, practitioners and experts gather in Bratislava for OSCEwide conference on the future of cybersecurity. [Press Release]. Bratislava. Disponível em: <https://www.osce.org/chairmanship/423365>.

416. Ver, por exemplo, Organization for Security and Cooperation in Europe. (10 de março de 2016). Decision No, 1202 OSCE confidence-building measures to reduce the risks of conflict stemming from the use of information and communication technologies. PC. DEC/1202. Disponível em: <https://www.osce.org/pc/227281?download=true>.

417. New America. Cybersecurity initiative. Disponível em: <https://www.newamerica.org/cybersecurity-initiative/about/>.

418. Ver, por exemplo: Carnegie Endowment for International Peace. Cyber strategy. Disponível em: <https://carnegieendowment.org/programs/technology/cyber/cyberstrategy> ; Carnegie Endowment for International Peace. Cybersecurity and the financial system. Disponível em: <https://carnegieendowment.org/specialprojects/fincyber>; Carnegie Endowment for International Peace. U.S.-China cyber stability. Disponível em: <https://carnegieendowment.org/programs/technology/cyber/uschinacyberstability>; Carnegie Endowment for International Peace. International cybersecurity norms. Disponível em: <https://carnegieendowment.org/specialprojects/cybernorms/?lang=en>.

419. The National Law Review. (9 de janeiro de 2018). Top data governance issues from 2017 and what to watch in 2018. Disponível em: <https://www.natlawreview.com/article/top-data-governance-issues-2017-and-what-to-watch-2018>.

420. Tech Crunch. (28 de fevereiro de 2019). Thailand passes controversial cybersecurity law that could enable government surveillance. Disponível em: <https://techcrunch.com/2019/02/28/thailand-passes-controversial-cybersecurity-law/>.

421. LeesAnguansuk, S. Tortermvasana, K. & Banchongduang, S. (22 de outubro de 2018). The cybersecurity balancing act. Bangkok Post. Disponível em: <https://www.bangkokpost.com/thailand/politics/1562230/the-cybersecurity-balancing--act>.

422. Eristavi, M. (13 de dezembro de 2018). Interpol keeps despots' dissidents close. Politico. Disponível em: <https://www.politico.eu/article/interpol-russian-abuse-keeps-despots-dissidents--close/>.

423. Internet & Jurisdiction Policy Network. (2018, novembro). Vietnamese government releases draft decree on implementation of cybersecurity law requiring service providers to establish local offices, store data within the country. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7691_2018-11>.

424. Nellis, S. & Cadell, C. (24 de fevereiro de 2018). Apple moves to store iCloud keys in China, raising human rights fears. Reuters. Disponível em: <https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060>.

425. Internet & Jurisdiction Policy Network. (2018, fevereiro). Apple stores Chinese iCloud accounts and encryption keys in China to comply with data localization requirements. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7691_2018-11>.

426. European Commission NIS Cooperation Group. (2019). Report: EU coordinated risk assessment of the cybersecurity of 5G networks. Disponível em: <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=62132>.

427. Schuetze, A. (2018, 20 de dezembro). Amazon error allowed Alexa user to eavesdrop on another home. Reuters. Disponível em: <https://www.reuters.com/article/us-amazon-data-security-idUSKCN1OJ15J>.

428. United States of America contra Zhang et al 13CR3132H, Indictment. Disponível em: <https://www.justice.gov/opa/press-release/file/1106491/download> , para 1.

429. Australian Cyber Security Centre. (2017). Australian Cyber Security Centre 2017 Threat Report. Disponível em: <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf>, p.51.

430. Australian Cyber Security Centre. (2017). Australian Cyber Security Centre 2017 Threat Report. Disponível em: <https://www.acsc.gov.au/publications/ACSC_Threat_Report_2017.pdf>, p.55.

3.3

431. E-Estonia. E-governance. Disponível em: <https://e-estonia.com/solutions/e-governance/>.

432. Digital Luxembourg. Data Embassy. Disponível em: <https://digital-luxembourg.public.lu/initiatives/data-embassy>.

433. LeeMakiyama. (10 de julho de 2017). The digital trade oversight. International Trade Forum. Disponível em: <http://www.tradeforum.org/article/The-digital-trade-oversight/>.

434. Cann, O. (22 de janeiro de 2016). $100 trillion by 2025: The digital dividend for society and business. World Economic Forum. Disponível em: <https://www.weforum.org/press/2016/01/100-trillion-by-2025-the-digital-dividend-for-society-and-business/>.

435. Baur, C. & Wee, D. (2015, junho). Manufacturing's next act. McKinsey & Company. Disponível em: <https://www.mckinsey.com/business-functions/operations/our-insights/manufacturings-next-act>.

436. Hague Conference on Private International Law. (2 de julho de 2019). Convention of 2 July 2019 on the Recognition and Enforcement of Foreign Judgments in Civil or Commercial Matters. Disponível em: <https://www.hcch.net/en/instruments/conventions/full-text/?cid=137>.

437. Hague Conference on Private International Law. (19 de março de 2015). Principles on choice of law in international commercial contracts. Disponível em: <https://www.hcch.net/en/instruments/conventions/full-text/?cid=135>.

438. Hague Conference on Private International Law. Hague Convention of 30 June 2005 on choice of court agreements. Disponível em: <https://www.hcch.net/en/instruments/conventions/specialised-sections/choice-of-court>.

439. Asia-Pacific Economic Cooperation. APEC workshop on harnessing digital trade for SMEs. Disponível em: <https://aimp2.apec.org/sites/PDB/Lists/Proposals/DispForm.aspx?ID=2252>.

440. Asia-Pacific Economic Cooperation. APEC workshop on harnessing digital trade for SMEs. Disponível em: <https://www.apec.org/-/media/APEC/Publications/2019/6/APEC-Workshop-on-Harnessing-Digital-Trade-for-SMEs/219_SME_APEC-Workshop-on-Harnessing-Digital-Trade-for-SMEs.pdf>.

441. United Nations. (2018). Secretary-General's High-level Panel on Digital Cooperation. Disponível em: <http://www.un.org/en/digital-cooperation-panel/>.

442. United Nations Conference on Trade and Development. E-transactions legislation worldwide. Disponível em: <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Transactions-Laws.aspx>.

443. World Economic Forum. (2018, maio). Digital Transformation Initiative. Disponível em: <http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-executive-summary-20180510.pdf>.

444. World Economic Forum. Digital Trade. Disponível em: <https://www.weforum.org/projects/digital-trade-policy>.

445. World Economic Forum. (2017, outubro). White paper: Making deals in cyberspace: What's the problem? Disponível em: <http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf>.

446. World Economic Forum. (2017, outubro). White paper: Making deals in cyberspace: What's the problem? Disponível em: <http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf>, p. 11.

447. G20 Digital Economy Ministerial Declaration: Shaping digitalisation for an interconnected world. (7 de abril de 2017), Dusseldorf. Disponível em: <http://www.g20.utoronto.ca/2017/170407-digitalization.htm>.

448. OECD. (2017). OECD Digital Economy Outlook 2017. Paris: OECD Publishing. Disponível em: <https://read.oecd-ilibrary.org/science-and-technology/oecd-digital-economy-outlook-2017_9789264276284-en#page1>.

449. Ahmad, N. & Ribarsky, J. (2018, setembro). Towards a framework for measuring the digital economy, OECD. Paper prepared for the 16th Conference of the International Association of Official Statisticians, France. Disponível em: <http://www.oecd.org/iaos2018/programme/IAOS-OECD2018_Ahmad-Ribarsky.pdf>.

450. World Economic Forum. (11 de dezembro de 2017). WTO, World Economic Forum and e-WTP launch joint public-private dialogue to open up e-commerce for small business. Disponível em: <https://www.weforum.org/press/2017/12/trade-press-release/>.

451. Global Forum on Cyber Expertise. (2019). Disponível em: <https://www.thegfce.com>.

452. International Telecommunications Union. (2018). Developing skills for the digital economy and society. Disponível em: <https://www.itu.int/en/itunews/Documents/2018/2018-ITUNewsPlus-CBS/2017_ITUNewsPlus-CBS.pdf>.

453. World Trade Organization. (25 de maio de 1998). The Geneva Ministerial Declaration on global electronic commerce. Disponível em: <https://www.wto.org/english/tratop_e/ecom_e/mindec1_e.htm>.

454. World Trade Organization. Electronic commerce. Disponível em: <https://www.wto.org/english/tratop_e/ecom_e/ecom_e.htm>.

455. World Trade Organization. The Doha Declaration explained. Disponível em: <https://www.wto.org/english/tratop_e/dda_e/dohaexplained_e.htm#electroniccommerce>.

456. Reidenberg, J.R., Debelak, J., Kovnot, J., Bright, M., Russell, N.C. Alvarado, D., Seiderman, E. & Rosen, A. (30 de junho de 2013). Internet jurisdiction: A survey of legal scholarship published in English and United States case law. Fordham Law Legal Studies Research Paper No.2309526. Disponível em SSRN: <http://ssrn.com/abstract=2309526> ou <http://dx.doi.org/10.2139/ssrn.2309526>, pp. 56-57 (notas de rodapé omitidas).

457. Zippo Manufacturing Company contra Zippo Dot Com, Inc. 952 F.Supp.1119 (W.D.Pa 1997).

458. Google Inc. contra Equustek Solutions Inc 2017 SCC 34.

459. Google Inc. contra Equustek Solutions Inc 2017 SCC 34. Disponível em: <https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do>.

460. Geist, M. (3 de novembro de 2017). U.S. Judge Rules Canadian court order 'threatens free speech on the global Internet'. Disponível em: <http://www.michaelgeist.ca/2017/11/googleequustekinjunction/>.

461. Internet & Jurisdiction Policy Network. (2018, abril). Canada: Regional court upholds Equustek decision requiring Google to globally delist search results in spite of US court decision. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6957_2018-04>.

462. Internet & Jurisdiction Policy Network. (2018, setembro). Highest German court refers case on YouTube liability over copyrightinfringing videos to ECJ. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7454_2018-09>. Ver mais em: Processo C682/18 LF contra Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=211267&pageIndex=0&doclang=PT&mode=req&dir=&occ=first&part=1&cid=1142050>. Acesso em: 27 de setembro de 2020.

463. Geigner, T. (6 de março de 2019). Swiss Supreme Court refuses to order ISPs to block 'pirate' sites. Tech Dirt. Disponível em: <https://www.techdirt.com/articles/20190228/11582441695/swiss-supreme-court-refuses-to-order-isps-to-block-pirate-sites.shtml>.

464. Torrent Freak. (13 de março de 2019). YouTube is not liable for copyright infringing videos, Appeal Court rules. Disponível em: <https://torrentfreak.com/youtube-is-not-liable-for-copyright-infringing-videos-appeal-court-rules-190312/>.

465. Internet & Jurisdiction Policy Network. (2019, julho). Italian court holds video sharing platform liable for content uploaded by users. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaXRhbGlhbiIsImZyb20iOiIyMDEyLTAyIiwidG8iOiIyMDE5LTA4In0=> ; Internet & Jurisdiction Policy Network. (2019, junho). Australian court rules media organizations liable for content posted by users on their pages. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiYXVzdHJhbGlhIiwiZnJvbSI6IjIwMTItMDliLCJ0byI6IjIwMTktMDgifQ==>.

466. CS (COMM) 344/2018.

467. AZB & Partners. (19 de janeiro de 2019). Changing landscape of intermediary liability. Disponível em: <https://www.azbpartners.com/bank/changing-landscape-of-intermediary-liability/>.

468. Torrent Freak. (15 de março de 2019). Russia plans to block pirate sites without trial & de-anonymize their operators. Disponível em: <https://torrentfreak.com/russia-plans-to-block-pirate-sites-without-trial-de-anonymize-operators-190315/>.

469. Ubertazzi, B. (2012). Exclusive jurisdiction in intellectual property. Tubingen: Mohr Siebeck, 139 (notas de rodapé omitidas).

470. Ubertazzi, B. (2012). Exclusive jurisdiction in intellectual property. Tubingen: Mohr Siebeck, 139 (notas de rodapé omitidas).

471. Proposta de Diretiva do Parlamento Europeu e do Conselho relativa aos direitos de autor no mercado único digital. COM/2016/0593 final 2016/0280 (COD). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:52016PC0593&from=PT>. Acesso em: 27 de setembro de 2020.

472. Kayali, L. (26 de março de 2019). European Parliament approves overhaul of online copyright rules. Politico. Disponível em: <https://www.politico.eu/article/european-parliament-approves-copyright-reform-in-final-vote/?utm_source=RSS_Feed&utm_medium=RSS&utm_campaign=RSS_Syndication>.

473. União Europeia. Rectificação à Directiva 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de Abril de 2004, relativa ao respeito dos direitos de propriedade intelectual. OJL 157, 30.4.2004. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32004L0048R(01)&from=EN>. Acesso em: 27 de setembro de 2020.

474. Comissão Europeia. (29 de novembro de 2017). Orientações relativas a certos aspetos da Diretiva 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de abril de 2004, relativa ao respeito dos direitos de propriedade intelectual. COM (2017) 431. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/?qid=1601247376398&uri=CELEX:52017DC0708>.

475. United Kingdom Intellectual Property Office. Protecting creativity, supporting innovation: IP enforcement 2020. Disponível em: <https://www.gov.uk/government/publications/protecting-creativity-supporting-innovation-ip-enforcement-2020>.

476. Center for International Intellectual Property Studies. Disponível em: <http://www.ceipi.edu/en>.

477. ICANN. Domain name dispute resolution policies. Disponível em: <https://www.icann.org/resources/pages/dndr-2012-02-25-en>.

478. The White House: Office of the Press Secretary. (25 de setembro de 2015). Fact Sheet: President Xi Jinping's state visit to the United States. [Press Release]. Disponível em: <https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states>.

479. Ver, por exemplo: United States of America contra Zhang et al 13CR3132H, Indictment. Disponível em: <https://www.justice.gov/opa/press-release/file/1106491/download>.

480. Office of the United States Trade Representative. (22 de março de 2018). Findings of the investigation into China's acts, policies and practices related to technology transfer, intellectual property, and innovation under section 301 of the Trade Act of 1974. Disponível em: <https://ustr.gov/sites/default/files/Section%20301%20FINAL.PDF>, p. 19.

481. Ver, por exemplo: Cerulus, L. (20 de dezembro de 2018). West accuses Beijing of 'extensive' cyber espionage. Politico. Disponível em: <https://www.politico.eu/article/china-cyber-espionage-uk-us-accuses-beijing/>, Fitzpatrick, M. (15 de abril de 2013). Did China steal Japan's high-speed train. Fortune. Disponível em: <http://fortune.com/2013/04/15/did-china-steal-japans-high-speed-train/> , e Laskai, L. (28 de março de 2018). Why does everyone hate Made in China 2025? Council on Foreign Relations. Disponível em: <https://www.cfr.org/blog/why-does-everyone-hate-made-china-2025>.

482. Internet & Jurisdiction Policy Network. (2018, setembro). Japanese government presents draft report to implement website blocking to fight against copyright infringement. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7470_2018-09>.

483. Torrent Freak. (13 de março de 2019). Japan Abandons Tough AntiDownloading Copyright Law. Disponível em: <https://torrentfreak.com/japan-abandons-tough-anti-downloading-copyright-law-190313/>.

484. Garcia contra Google Inc 786 f.3d 733. Disponível em: <http://cdn.ca9.uscourts.gov/datastore/general/2014/02/28/12-57302_opinion.pdf>.

485. Canadian Radio-television and Telecommunications Commission. (2 de outubro de 2018). CRTC denies FairPlay Canada's application on piracy websites on jurisdictional grounds. [Press Release]. Canada.

486. Ver, por exemplo: Regulamento (UE) n.o 1215/2012 do Parlamento europeu e do Conselho de 12 de dezembro de 2012 relativo à competência judiciária, ao reconhecimento e à execução de decisões em matéria civil e comercial (Bruxelas i bis), artigo 18, como exemplificado nos processos conjuntos c 585/ 08 peter pammer contra Reederei Karl Schlüter GmbH & Co KG e C 144/09 Hotel Alpenhof GESmbH contra Oliver Heller.

487. United Nations Conference on Trade and Development. Online consumer protection legislation worldwide. Disponível em: <https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Consumer-Protection-Laws.aspx>.

488. International Consumer Protection and Enforcement Network. (29 de junho de 2018). Joint open letter to businesses in the digital economy on the importance of standard terms and conditions for consumers. Disponível em https: <https://www.icpen.org/news/902>.

489. Morrison, S. (4 de dezembro de 2017). Letter to ACCC Chairman Rod Sims requiring ACCC inquiry into digital platforms. Disponível em: <https://www.accc.gov.au/system/files/ministeria%20direction.pdf>. O relatório final pode ser encontrado em: Australian Competition and Consumer Commission. (26 de julho de 2019) Digital platforms inquiry final report. Disponível em: <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>.

490. Internet Governance Forum. Dynamic Coalition on Platform Responsibility. Disponível em: <https://www.intgovforum.org/multilingual/content/dynamic-coalition-on-platform-responsibility--dcpr>.

491. Internet & Jurisdiction Policy Network. (2017, agosto). Tanzania Deputy Minister of Communications calls for social media regulation similar to China's. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6235_2017-08>.

492. Internet & Jurisdiction Policy Network. (2017, agosto). Tanzania Deputy Minister of Communications calls for social media regulation similar to China's. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6235_2017-08>.

493. Creating a French Framework to make social media platforms more accountable. (2019, maio). Disponível em: <https://minefi.hosting.augure.com/Augure_Minefi/r/ContenuEnLigne/Download?id=AE5B7ED5-2385-4749-9CE8-E4E1B36873E4&filename=Mission%20Régulation%20des%20réseaux%20sociaux%20-ENG.pdf>.

494. District of Columbia contra Facebook Inc, Complaint. Disponível em: <http://oag.dc.gov/sites/default/files/2018-12/Facebook-Complaint.pdf>.

495. Internet & Jurisdiction Policy Network. (2019, julho). Federal Trade Commission fines Facebook US$5 billion and orders oversight layers for data protection. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiY2FtYnJpZGdlIGFuYWx5dGljYSIsImZyb20iOiIyMDE5LTAxIiwidG8iOiIyMDE5LTA4In0=>.

496. Internet & Jurisdiction Policy Network. (2019, junho). Italy fines Facebook for data breach. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaXRhbHkiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9>.

497. Internet & Jurisdiction Policy Network. (2019, abril). Canada Privacy Commissioner's investigation concludes that Facebook broke Canadian privacy laws. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiY2FuYWRhIiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDgifQ==>.

498. Comissão Europeia. (18 de julho) de 2018. AAnti-trust: Comissão aplica coima de 4.34 mil milhões de EUR à Google por práticas ilegais relacionadas com dispositivos móveis Android destinadas a reforçar a posição dominante do motor de pesquisa da Google. [Comunicado de Imprensa]. Disponível em: <https://ec.europa.eu/commission/presscorner/detail/pt/IP_18_4581>. Acesso em: 28 de setembro de 2020.

499. European Commission. (20 de março de 2019). Statement by Commissioner Vestager on Commission decision to fine Google € 1.49 billion for abusive practices in online advertising. [Press Release]. Brussels. Disponível em: <https://europa.eu/rapid/press-release_STATEMENT-19-1774_en.htm>.

500. Yun Chee, F. (13 de setembro de 2019). EU may need to regulate tech giants' data use: EU antitrust chief. Reuters. Disponível em: <https://www.reuters.com/article/us-eu-antitrust-data-idUSKCN1VY1GU>.

501. Kottasova, I. (7 de fevereiro de 2019). Germany orders Facebook to change the way it gathers data. CNN Business. Disponível em: <https://edition.cnn.com/2019/02/07/tech/facebook-germany-data-collection/index.html>.

502. Ahmed, A. & Phartiyal, S. (27 de dezembro de 2018). India tightens e-commerce rules, likely to hit Amazon, Flipkart. Reuters. Disponível em: <https://www.reuters.com/article/us-india-ecommerce/india-tightens-e-commerce-rules-likely-to-hit-amazon-flipkart-idUSKCN1OP14M>.

503. Internet & Jurisdiction Policy Network. (fevereiro de 2019). India: Proposed E-Commerce Policy calls for increased data localization and increased protection of data privacy and consumer rights. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaW5kaWEiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9>.

504. Gupta, N,. (24 de julho de 2019). Why DOJ Antitrust Review Is bad news for Facebook. Market Realist. Disponível em : <https://articles2.marketrealist.com/2019/07/doj-antitrust-review-is-bad-news/> .

505. New York Attorney General. (6 de setembro de 2019). AG James investigating Facebook for possible antitrust violations. [Press Release]. New York. Disponível em: <https://ag.ny.gov/press-release/2019/ag-james-investigating-facebook-possible-antitrust-violation>.

506. Sweeney, M. (4 de julho) de 2019. Google and Facebook under scrutiny over UK ad market dominance. The Guardian. Disponível em: <https://www.theguardian.com/business/2019/jul/03/google-facebook-investigated-over-dominance-of-uk-digital-advertising-market>.

507. White, S. (2019, fevereiro). Japan sets sights on tighter antitrust regulations for Big Tech. Reuters. Disponível em: <https://www.reuters.com/article/us-japan-economy-tech/japan-sets-sights-on-tighter-anti-trust-regulations-for-big-tech-idUSKCN1Q20YB?feedType=RSS&feedName=technologyNews>.

508. UK House of Lords Select Committee on Communications. (2019, março). Regulating in a digital world. Disponível em: <https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf>.

509. Federal Trade Commission. (26 de fevereiro de 2019). FTC's Bureau of Competition launches task force to monitor technology markets. [Press Release]. Disponível em: <https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology>.

510. OECD. (5 de dezembro de 2017). Extra-territorial reach of competition remedies. Disponível em: <http://www.oecd.org/daf/competition/extra-territorial-reach-of-competition-remedies.htm>.

511. Ver, por exemplo: Trimble, M. (2013). Proposal for an international convention on online gambling. In Cabot, A. & Pindell N. (Eds.), Regulating Internet gaming. Disponível em: <https://ssrn.com/abstract=2089935> e Hörnle, J. & Zammit, B. (2010). Cross-border online gambling law and policy. Cheltenham, United Kingdom: Edward Elgar.

512. Brussel principles on the sale of medicines over the Internet. Disponível em: <https://www.brusselsprinciples.org/>.

513. Garnett, R. (2017). Arbitration of cross-border consumer transactions in Australia: A way forward?. Sydney Law Review, 39(4), 569-599.

514. 2017 SCC 33. Ver mais em: Harris, L. W. (2019). Understanding public policy limits to the enforceability of forum selection clauses after Douez contra Facebook. Journal of Private International Law, 15(1), 5096.

515. Internet & Jurisdiction Policy Network. (2017, junho). Canadian Supreme Court says Facebook privacy lawsuit can be heard in British Columbia instead of California. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6109_2017-06>.

516. Nomeadamente: Directiva 93/13/CEE do Conselho de 5 de Abril de 1993 relativa às cláusulas abusivas nos contratos celebrados com os consumidores. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31993L0013&from=EN>. Acesso em: 28 de setembro de 2020.

517. Processo C191/15 Verein für Konsumenteninformation contra Amazon EU Sàrl.

518. Processo C673/17 Planet49.

519. Parecer do Advogado Geral Szpunar em Planet49 (Processo C673/17).

520. Processo C673/17 Bundesverband der Verbraucherzentralen und Verbraucherverbände. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=218462&pageIndex=0&doclang=PT&mode=lst&dir=&occ=-first&part=1&cid=3969308>. Acesso em: 28 de setembro de 2020.

521. Hunton, A. K. (23 de junho de 2019). CNIL publishes new guidelines on cookies and similar technologies. Disponível em: <https://www.huntonprivacyblog.com/2019/07/23/cnil-publishes-new-guidelines-on-cookies-and-similar-technologies/>.

522. Ver, por exemplo: El Diretor-Geral De Impuestos y Aduanas Nacionales. (19 de outubro de 2018). Resolución Número 000051. Disponível em: <https://www.dian.gov.co/normatividad/Normatividad/Resoluci%C3%B3n%20000051%20de%2019-10-2018.pdf>.

523. Joint Chiefs of Global Tax Enforcement. (2 de julho de 2018). Tax enforcement authorities unite to combat international tax crime and money laundering. [Press Release]. Montreal. Disponível em: <https://www.irs.gov/pub/irs-utl/j5-media-release-7-2-18.pdf>.

524. Ver, por exemplo: Australian Taxation Office. Organised crime. Disponível em: <https://www.ato.gov.au/General/The-fight-against-tax-crime/Our-focus/Organised-crime/>.

525. OCDE. (2018). Tax challenges arising from digitalisation: Interim report 2018: Disponível em: <http://dx.doi.org/10.1787/9789264293083-en>, p. 3.

526. OECD. (2019). Public consultation document: Addressing the tax challenges of the digitalisation of the economy. Disponível em: <http://www.oecd.org/tax/beps/public-consultation-document-addressing-the-tax-challenges-of-the-digitalisation-of-the-economy.pdf>. Para os trabalhos da OCDE sobre este tema, ver também: OECD. (2019). Programme of work to develop a consensus solution to the tax challenges arising from the digitalisation of the economy. Disponível em: <www.oecd.org/tax/beps/programme-of-work-to-develop-aconsensus-solution-to-the-tax-challenges-arising-from-the-digitalisation-of-the-economy.htm>.

527. SmithMeyer, B. (28 de novembro de 2018). EU digital tax 'dead' as countries eye national paths. Politico Pro. Disponível em: <https://www.politico.eu/pro/eu-digital-tax-dead-as-countries-eye-national-paths/>. Ver mais em: Conselho da União Europeia. Tributação dos serviços digitais. Disponível em: <https://www.consilium.europa.eu/pt/policies/digital-taxation/>.

528. Kayali, L. (17 de dezembro de 2018). French tax on Google, Facebook to apply from January 1, 2019. Politico. Disponível em: <https://www.consilium.europa.eu/pt/policies/digital-taxation/>.

529. Ekblom, J. & Shepardson, D. (20 de agosto de 2019). U.S. tech industry leaders: French digital service tax harms global tax reform. Reuters. Disponível em: <https://www.reuters.com/article/us-france-tax-usa/u-s-tech-industry-leaders-french-digital-service-tax-harms-global-tax-reform-idUSKCN1V91UC>.

530. Australian Taxation Office. (10 de agosto de 2017). Combating multinational tax avoidance – a targeted anti-avoidance law. Disponível em: <https://www.ato.gov.au/Business/International-tax-for-business/In-detail/Doing-business-in-Australia/Combating-multinational-tax-avoidance---a-targeted-anti-avoidance-law/>.

531. Eschenbacher, S., Graham, D., Love, J., & Solomon, D. B. (9 de setembro de 2019). Mexico eyes sales tax on digital businesses to boost revenue. Reuters. Disponível em: <https://www.reuters.com/article/us-mexico-budget-digitalplatforms/mexico-eyes-sales-tax-on-digital-businesses-to-boost-revenue-idUSKCN1VU1H1>.

532. Internet Society. (2018, setembro). The Internet and extraterritorial application of laws. Disponível em: <https://www.internetsociety.org/wp-content/uploads/2018/10/The-Internet-and-extra-territorial-application-of-laws.pdf>, p. 9.

533. Toussi, S. (12 de setembro de 2019). Overview of Cameroon's digital landscape. Collaboration on International ICT Policy in East and Southern Africa. Disponível em: <https://cipesa.org/2019/09/overview-of-cameroons-digital-landscape/>.

534. Jefriando, M. (29 de março de 2019). Indonesia retracts e-commerce regulation to avoid confusion. Reuters. Disponível em: <https://www.reuters.com/article/us-indonesia-tax-ecommerce/indonesia-retracts-e-commerce-regulation-to-avoid-confusion-idUSKCN1RA0ZU>.

535. Inland Revenue Authority of Singapore. E-Commerce. Disponível em: <https://www.iras.gov.sg/irashome/GST/GST-registered-businesses/Specificbusiness-sectors/e-Commerce/>.

536. TechinAsia. (27 de agosto de 2019). In brief: Thailand to implement e-commerce tax in 2020. Disponível em: <https://www.techinasia.com/thailand-implement-ecommerce-tax-2020>.

537. Samuel, P. (de 201925 de julho). Vietnam's tax administration law reform to take effect in July 2020. Vietnam Briefing. Disponível em: <https://www.vietnam-briefing.com/news/vietnams-tax-administration-law-reform-take-effect-july-2020.html/>.

538. EY. (2019). Malaysia publishes updated Guidelines on Taxation of e-Commerce Transactions. Disponível em: <https://www.ey.com/gl/en/services/tax/international-tax/alert—malaysia-publishes-updated-guidelines-on-taxation-of-e-commerce-transaction>.

539. White, S. & Strupczewski, J. (8 de junho de 2019). G20 agrees to push ahead with digital tax: communique. Reuters. Disponível em: <https://www.reuters.com/article/us-g20-japan-tax/g20-agrees-to-push-ahead-with-rules-on-corporate-tax-targeting-tech-giants-idUSKCN1T903D?feedType=RSS&feedName=technologyNews>.

540. Reserve Bank of India. (6 de abril de 2018). Storage of payment system data. Disponível em: <https://www.rbi.org.in/scripts/NotificationUser.aspx?Id=11244&Mode=0>.

541. Baroudy, K., Kishore, S., Nair, S. & Patel, M. (2018, março). Unlocking value from IoT connectivity: Six considerations for choosing a provider. McKinsey & Company. Disponível em: <https://www.mckinsey.com/industries/high-tech/our-insights/unlocking-value-from-iot-connectivity-six-considerations—for-choosing-a-provider>.

542. PwC. (2018). How businesses can build the resilience needed to withstand disruptive cyberattacks. Disponível em: <https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey/strengthening-digital-society-against-cyber-shocks.html>.

543. Internet Society. (19 de setembro de 2019). Policy brief: IoT privacy for policymakers. Disponível em: <https://www.internetsociety.org/policybriefs/iot-privacy-for-policymakers/>.

544. Federal Trade Commission. (2019, janeiro). Internet of Things: Privacy and Security in a Connected World. Disponível em: <https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf>.

545. Siemens. (2018). Charter of Trust on cybersecurity. Disponível em: <https://www.siemens.com/content/dam/webassetpool/mam/tag-siemens-com/smdb/corporate-core/topic-areas/digitalization/cybersecurity/180514-charter-of-trust-standard-presentation-v03.pdf>.

546. World Bank Group. (2017). Internet of Things: The new government to business platform a review of opportunities, practices, and challenges. Disponível em: <http://documents.worldbank.org/curated/en/610081509689089303/internet-of-things-the-new-government-to-business-platform-a-review-of-opportunities-practices-and-challenges>.

547. Internet Governance Forum. (2018). IGF 2018 DC Internet of Things: Global good practice in IoT: a call for commitment. Disponível em: <https://www.intgovforum.org/multilingual/content/igf-2018-dc-internet-of-things-global-good-practice-in-iot-a-call-for-commitment>.

548. Google Cloud. Cloud IoT Core. Disponível em: <https://cloud.google.com/iot-core/?utm_source=bing&utm_medium=cpc&utm_campaign=japac-AU-all-en-dr-bkws-all-all-trial-e-dr-1003987&utm_content=text-ad-none-none-DEV_c-CRE_75110457775562-ADGP_Hybrid+%7C+Bing+SEM+%-7C+BKWS+%7E+T3+%7C+EXA+%7C+Others+%7C+M%3A1+%7C+AU+%7C+en+%-7C+IOT-KWID_43700033430033742-kwd-75110536580611:loc-9&utm_term=KW_iot&gclid=CMn78pnbu94CFQ7kjgodz00CXA>.

549. IoT World Alliance. Disponível em: <http://www.iotworldalliance.org/#section_intro>.

550. McGee, M.K. (11 de janeiro de 2016). Fitbit hack: What are the lessons? Data Breach today. Disponível em: <https://www.databreachtoday.com/fitbit-hack-what-are-lessons-a-8793>.

551. McGee, M.K. (4 de junho de 2018). Another fitness app exposes users' data. Data Breach today. Disponível em: <https://www.databreachtoday.com/another-fitness-app-exposes-users-data-a-11055>.

552. Osborne, C. (9 de outubro de 2018). Garmin's Navionics exposed data belonging to thousands of customers. ZD Net. Disponível em: <https://www.zdnet.com/article/garmins-navionics-exposed-data-belonging-to-thousands-of-boat-owners/>.

553. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Disponível em: <https://bitcoin.org/bitcoin.pdf>.

554. BBC News. (23 de janeiro de 2014). Bitcloud developers plan to decentralise Internet. Disponível em: <http://www.bbc.co.uk/news/technology-25858629>.

555. Internet & Jurisdiction Policy Network. (2014, janeiro). Bitcoin developers plan to create a new, decentralized Internet. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-4940_2014-01>.

556. Powles, J. (27 de janeiro de 2014). Scottish company Maidsafe claims to have built a bitcloudlike system. Wired. Disponível em: <http://www.wired.co.uk/news/archive/2014-01/27/maidsafe-bitcloud>.

557. Dubai International Financial Centre. (30 de julho de 2018). DIFC Courts and Smart Dubai launch joint taskforce for world's first Court of the Blockchain. [Press Release]. Disponível em <https://www.difc.ae/newsroom/news/difc-courts-and-smart-dubai-launch-joint-taskforce-worlds-first-court-blockchain/>.

558. Zhang, L. (21 de setembro de 2018). China: Supreme Court issues rules on Internet courts, allowing for blockchain evidence. Library of Congress. Disponível em: <http://www.loc.gov/law/foreign-news/article/china-supreme-court-issues-rules-on-internet-courts-allowing-for-blockchain-evidence/>.

559. Ver mais em: Kuner. C., Cate, F., Lynskey, O., Millard, C., Loideain, N. W. & Svantesson, D. (2018, maio). Blockchain versus data protection. International Data Privacy Law, 8(2), 103–104. Disponível em: <https://academic.oup.com/idpl/article/8/2/103/5047578>.

560. Bambrough, B. (24 de setembro de 2019). Bitcoin, Ethereum, Ripple's XRP, And Litecoin In shock meltdown. Forbes. Disponível em: <https://www.forbes.com/sites/billybambrough/2019/09/24/bitcoin-ethereum-ripples-xrp-and-litecoin-in-shock-meltdown/#700f5fd73391>.

561. University of Hawaii at Manoa. (29 de outubro de 2018). Bitcoin can push global warming above 2 degrees C in a couple decades. ScienceDaily. Disponível em: <https://www.sciencedaily.com/releases/2018/10/181029130951.htm>.

562. University of Hawaii at Manoa. (29 de outubro de 2018). Bitcoin can push global warming above 2 degrees C in a couple decades. ScienceDaily. Disponível em: <https://www.sciencedaily.com/releases/2018/10/181029130951.htm>.

563. Europol. (2018). Internet Organised Crime Threat Assessment 2018. Disponível em: <https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf>, p.8.

564. Europol. (2018). Internet Organised Crime Threat Assessment 2018. Disponível em: <https://www.europol.europa.eu/sites/default/files/documents/iocta_2018_0.pdf>, p.8.

565. Considere, por exemplo, a lei de Fintech do México. Ver: Kurc, C. & Portilla, A. (10 de maio de 2019). Mexico: Fintech 2019. International Comparative Legal Guides. Disponível em: <https://iclg.com/practice-areas/fintech-laws-and-regulations/mexico>.

566. Artigo técnico sobre o Libra. Disponível em: <https://libra.org/pt-BR/white=-paper/?noredirect-pt-BR>. Disponível em: 30 de setembro de 2020.

567. Szabo, N. (1997). The idea of smart contracts. Wayback Machine. Disponível em: <http://web.archive.org/web/20140406003401/szabo.best.vwh.net/idea.html>.

568. World Trade Organization. The General Agreement on Trade in Services (GATS): objectives, coverage and disciplines. Disponível em: <https://www.wto.org/english/tratop_e/serv_e/gatsqa_e.htm>.

569. Artigo 14.5.

570. World Economic Forum. (2017, outubro). White paper: Making deals in cyberspace: What's the problem? Disponível em: <http://www3.weforum.org/docs/WEF_White_Paper_Making_Deals_in_Cyberspace.pdf> , p. 8.

571. EU-Japan Economic Partnership Agreement (2018, abril). Disponível em: <http://trade.ec.europa.eu/doclib/press/index.cfm?id=1684>, Capítulo 8 Seção F.

572. United States-Mexico-Canada Agreement. (30 de novembro de 2018). Disponível em: <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>.

573. World Trade Organization. The WTO and Internet privacy. Disponível em: <https://www.wto.org/english/tratop_e/serv_e/gats_factfiction10_e.htm>.

574. Acordo Geral sobre o Comércio de Serviços (GATS) Artigo XIV. Disponível em: <http://mdic.gov.br/arquivos/dwnl_1244492330.pdf>. Acesso em: 30 de setembro de 2020.

575. Resolução do Parlamento Europeu, de 12 de dezembro de 2017, relativa ao «Rumo a uma estratégia comercial digital» (2017/2065(INI)). Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52017IP0488&qid=1601501422353&from=PT>. Acesso em: 30 de setembro de 2020.

576. Kalra, A. (13 de outubro de 3018). Exclusive: U.S. senators urge India to soften data localization stance. Reuters. Disponível em: <https://www.reuters.com/article/us-india-data-localisation-exclusive/exclusive-u-s-senators-urge-india-to-soften-data-localization-stance-idUSKCN1MN0CN>.

577. Internet & Jurisdiction Policy Network. (2018, outubro). US Senators send letter to Indian PM to argue against central bank's data localization requirements. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7559_2018-10>.

578. Internet & Jurisdiction Policy Network. (2017, agosto). Apple removes Iranian apps, arguing US sanctions make it necessary. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6239_2017-08>.

579. Toor, A. (25 de agosto de 2017). Apple removes popular apps in Iran due to US sanctions. The Verge. Disponível em: <https://www.theverge.com/2017/8/25/16201434/apple-iran-app-store-removal-sanctions-trump>.

580. Roth, A. (16 de maio de 2017). In new sanctions list, Ukraine targets Russian socialmedia sites. The Washington Post. Disponível em: <https://www.washingtonpost.com/world/in-new-sanctions-list-ukraine-blocks-russian-social-media-sites/2017/05/16/a982ab4e-3a16-11e7-9e48-c4f199710b69_story.html>.

581. Internet & Jurisdiction Policy Network. (2017, maio). Ukraine blocks Russian Internet platforms in new round of sanctions. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-5931_2017-05>.

Notas do Capítulo 04
Abordagens jurídicas e técnicas

4.1

582. Keller, D. (29 de janeiro de 2019). Who do you sue? State and platform hybrid power over online speech. Aegis Series Paper No.1902. Disponível em: <https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf>, p. 7.

583. BBC News. (20 de agosto de 2018). Apple 'pulls gambling apps from China App Store'. Disponível em: <https://www.bbc.com/news/business-45243271> .

584. Internet & Jurisdiction Policy Network. (2018, agosto). Apple removes gambling apps from Chinese App Store. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7260_2018-08>.

585. Silviana, C. (4 de julho de 2018). Indonesia bans Chinese video app Tik Tok for 'inappropriate content'. Reuters. Disponível em: <https://www.reuters.com/article/us-indonesia-bytedance-ban/indonesia-bans-chinese-video-app-tik-tok-for-inappropriate-content-idUSKBN1JU0K8?feedType=RSS&feedName=technologyNews>.

586. Silviana, C. & Potkin, F. (11 de julho de 2018). Indonesia overturns ban on Chinese video app Tik Tok. Reuters. Disponível em: <https://www.reuters.com/article/us-indonesia-bytedance/indonesia-overturns-ban-on-chinese-video-app-tik-tok-idUSKBN1K10A0>.

587. Internet & Jurisdiction Policy Network. (julho de 2018). Indonesian authorities ban Chinese video app Tik Tok over pornography and blasphemy. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7189_2018-07>.

588. Internet & Jurisdiction Policy Network. (2018, março). Indonesia blocks access to Tumblr after the platform fails to remove inappropriate content. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6888_2018-03>.

589. MuHyum, C. (22 de junho de 2018). Tumblr to cooperate with Korean authorities to monitor porn. ZD Net. Disponível em: <https://www.zdnet.com/article/tumblr-to-cooperate-with-korean-authorities-to-monitor-porn/>.

590. Internet & Jurisdiction Policy Network. (junho de 2018). Tumblr agrees to better monitor illegal adult content in South Korea, says regulator. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7073_2018-06>.

591. Internet & Jurisdiction Policy Network. (2018, dezembro). Russia: Regulator fines Google 500 000 rubles for failing to remove search entries results. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7728_2018-12>.

592. Internet & Jurisdiction Policy Network. (2019, julho). Russia fines Google for failing to remove links for search results. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-8298_2019-07>.

593. Internet & Jurisdiction Policy Network. (2019, agosto). Russia demands Google stop advertising illegalprotests on YouTube. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoicnVzc2lhIiwiZnJvbSI6IjIwMTItMDIiLCJ0byI6IjIwMTktMDgifQ==>.

594. Internet & Jurisdiction Policy Network. (2018, dezembro). Twitter publishes transparency report, showing sharp increase in public authorities' request for content removal. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7733_2018-12>.

595. Bennetts, M. (10 de setembro de 2018). Russian police arrest hundreds protesting against Putin pension plan. The Guardian. Disponível em: <https://www.theguardian.com/world/2018/sep/09/google-pulls-youtube-ad-by-putin-critic-alexei-navalny>.

596. Internet & Jurisdiction Policy Network. (2018, setembro). YouTube complies with Russian request to remove dissident's videos. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7468_2018-09>.

597. Processo C18/18 Eva GlawischnigPiesczek contra Facebook Ireland Limited. Disponível em: <http://curia.europa.eu/juris/document/document.jsf?text=&docid=202866&pageIndex=0&doclang=PT&mode=lst&dir=&occ=first&part=1&cid=4855084>. Acesso em: 30 de setembro de 2020.. Para uma discussão aprofundada sobre as implicações da liberdade de expressão nesta matéria, ver: Keller. D. (2019). Dolphins in the net: Internet content filters and the Advocate General's GlawischnigPiesczek contra Facebook Ireland Opinion. Disponível em: <https://cyberlaw.stanford.edu/files/Dolphins-in-the-Net-AG-Analysis.pdf>.

598. John William Fierro Caicedo contra Google Inc. e outros. T063A/ 17. Disponível em: <http://www.corteconstitucional.gov.co/relatoria/2017/t-063a-17.htm>.

599. Internet & Jurisdiction Policy Network. (2017, outubro). Colombian Constitutional Court rules that Google must delete a Blogger.com blog that contained defamatory statements. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6369_2017-10>.

600. X contra Twitter Inc [2017] NSWSC 1300. Disponível em: <http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html>, para 36.

601. X contra Twitter Inc [2017] NSWSC 1300. Disponível em: <http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html>, para 37.

602. Svantesson, D. (14 de novembro de 2017). Sydney to be become the Internet content blocking capital of the world? LinkedIn. Disponível em: <https://www.linkedin.com/pulse/sydney-become-internet-content-blocking-capital-world-svantesson/>.

603. Veja, no entanto: Keller, D. (29 de janeiro de 2019). Who do you sue? State and platform hybrid power over online speech. Aegis Series Paper No.1902. Disponível em: <https://www.hoover.org/sites/default/files/research/docs/who-do-you-sue-state-and-platform-hybrid-power-over-online-speech_0.pdf>.

604. Keller, D. (13 de setembro de 2018). Why DC Pundits' must-carry claims are relevant to global censorship. The Center for Internet and Society. Disponível em: <http://cyberlaw.stanford.edu/blog/2018/09/why-dc-pundits-must-carry-claims-are-relevant-global-censorship.>.

605. Masnick, M. (7 de setembro de 2018). German Court tells Facebook it can't delete comments, even though German law says it must delete comments. Tech Dirt. Disponível em: <https://www.techdirt.com/articles/20180907/00455240595/german-court-tells-facebook-it-cant-delete-comments-even-though-german-law-says-it-must-delete-comments.shtml>; <http://www.omci.org.br/m/jurisprudencias/arquivos/2018/tjsc_00004474620168240175_06022018.pdf>.

606. Keller, D. (13 de setembro de 2018). Why DC Pundits' must-carry claims are relevant to global censorship. The Center for Internet and Society. Disponível em: <http://cyberlaw.stanford.edu/blog/2018/09/why-dc-pundits-must-carry-claims-are-relevant-global-censorship>.

607. European Court of Human Rights. Case of Magyar Jeti Zrt contra Hungary (4 de dezembro de 2018).11257/16. Disponível em: <https://hudoc.echr.coe.int/eng#%7B%22itemid%22:%5B%22001-187930%22%5D%7D>.

608. Internet & Jurisdiction Policy Network. (2018, dezembro). ECHR rules that order to remove hyperlinks to defamatory statements infringe on news portal's freedom of expression. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7737_2018-12> .

609. 2nd Global Conference of the Internet & Jurisdiction Policy Network. (26-28 de fevereiro de 2018).Ottawa Roadmap. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/Secretariat-Summary-and-Ottawa-Roadmap-second-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pd>. , pp. 8-9. Para o último plano de trabalho, ver 3rd Global Conference of the Internet & Jurisdiction Policy Network. (3 - 5 de junho de 2019). Berlin Roadmap. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/Berlin-Roadmap-and-Secretariat-Summary-3rd-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf>.

610. Torrent Freak. (29 de novembro de 2018). Google, Facebook, VPNs and others risk huge fines under proposed law. Disponível em: <https://torrentfreak.com/google-facebook-vpns-and-others-risk-huge-fines-under-proposed-law-181129/>.

611. Internet & Jurisdiction Policy Network. (2018, novembro). Russian regulator announces civil case against Google for failing to remove search results linking to permanently banned websites. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7678_2018-11>.

612. Gupta, N,. (24 de julho de 2019). Why DOJ Antitrust Review Is bad news for Facebook. Market Realist. Disponível em : <https://articles2.marketrealist.com/2019/07/doj-antitrust-review-is-bad-news/>.

613. Government of Mauritius (Port Louis). (18 de novembro de 2018). Mauritius: ICT Act amended to regulate and curtail harmful and illegal contents and activities. All Africa. [Press Release]. Port Louis. Disponível em: <https://allafrica.com/stories/201811190697.html>.

614. Internet & Jurisdiction Policy Network. (2018, novembro). Mauritius: Parliament passes amendments to ICT Act increasing penalties for spreading harmful and illegal content online. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7693_2018-11>.

615. Coos, A. (21 de junho de 2019). India's Personal Data Protection Bill: What we know so far. Endpoint Protector. Disponível em: <https://www.endpointprotector.com/blog/indias-personal-data-protection-bill-what-we-know-so-far/>.

616. AttorneyGeneral for Australia Minister for Industrial Relations. (2019, março 24). Tougher Penalties to keep Australians safe online. Disponível em: <https://www.attorneygeneral.gov.au/media/media-releases/tougher-penalties-keep-australians-safe-online-24-march-2019>. Acesso em: 30 de setembro de 2020.

617. Federal Trade Commission. (24 de julho de 2019). FTC Imposes $5 Billion penalty and sweeping new privacy restrictions on Facebook. [Press Release]. Disponível em: <https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions>.

618. Proposta da Diretiva e-evidence , Art 3.

619. Proposta da Diretiva e-evidence Directive, Art.3(8).

620. Seção 36(5), na versão de setembro de 2018.

621. Internet & Jurisdiction Policy Network. (2018, outubro). Indian government orders social media platforms to establish content monitoring system to track objectionable content. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7547_2018-10>.

622. Nguyen, M. (14 de setembro de 2018). Vietnam urges Facebook to open office ahead of controversial cyber law. Reuters. Disponível em: <https://www.reuters.com/article/us-facebook-vietnam/vietnam-urges-facebook-to-open-office-ahead-of-controversial-cyber-law-idUSKCN1LU13O?feedType=RSS&feedName=technologyNews>.

623. Internet & Jurisdiction Policy Network. (2018, setembro). Vietnamese government asks Facebook to open local office to comply with new cybersecurity law. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7456_2018-09>.

624. Internet & Jurisdiction Policy Network. (2019, março). South Korea proposes the formulation of new Network Use Guidelines. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoic291dGgga29yZWEiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9>.

625. Internet & Jurisdiction Policy Network. (2014, março). Brazilian congress approves Marco Civil Bill. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-4980_2014-03>. <https://www.internetjurisdiction.net/publications/retrospect#article4980_201403>.

626. Internet & Jurisdiction Policy Network. (2014, abril). Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-5002_2014-04>.

627. Internet & Jurisdiction Policy Network. (2014, abril). Marco Civil puts Brazilian data stored abroad under Brazilian jurisdiction. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-5002_2014-04>.

628. Ver mais em: Svantesson, D. (2017). Solving the Internet jurisdiction puzzle. Oxford, United Kingdom: Oxford University Press, p.132-141.

629. 315 F 3d 256 No. 012340 (13 de dezembro 2002).

630. Young contra New Haven Advocate 315 F 3d 256 No. 012340 (13 de dezembro de 2002), p. 7.

631. Ward Group Pty Ltd contra Brodie & Stone plc (com Corrigendas de 19 de maio de 2005) [2005] FCA 471, para 37.

632. Processos conjuntos C585/ 08 Peter Pammer contra Reederei Karl Schlüter GmbH & Co KG and C144/ 09 Hotel Alpenhof GesmbH contra Oliver Heller. Para uma discussão detalhada da jurisprudência do TJUE sobre este tema em matéria de responsabilidade civil, ver: Gillies, L. E. (5 de julho de 2019). Conceptualising special jurisdiction for receipt orientated torts on the Internet: Lessons from CJEU jurisprudence. Disponível em: <https://ssrn.com/abstract=3416218> ou <http://dx.doi.org/10.2139/ssrn.3416218>.

633. Considerandos 23.

634. COM (2018) 226 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0226&from=PT>; <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0226&from=PT>. Acesso em: 01 de outubro de 2020; e COM(2018) 225 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>. Acesso em: 01 de outubro de 2020.

635. Burbidge, R. (15 de outubro de 2018). Argos goes to the Court of Appeal but leaves empty handed. The IPKat. Disponível em: <http://ipkitten.blogspot.com/2018/10/argos-goes-to-court-of--appeal-but.html?m=1>.

636. Svantesson, D. (2001, Setembro/Outubro). What should Article 7 – Consumer contracts, of the proposed Hague Convention, aim to accomplish in relation to ecommerce? Computer Law & Security Report, 17(5), pp.318 – 325.

637. COM (2018) 226 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0226&from=PT>; <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0226&from=PT>. Acesso em: 01 de outubro de 2020; e COM (2018) 225 final. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52018PC0225&from=PT>. Acesso em: 01 de outubro de 2020.

638. Wikipédia. Microsoft Corp. contra United States. Disponível em: <https://en.wikipedia.org/wiki/Microsoft_Corp._v._United_States>.

639. United States contra Microsoft Corp. Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party. Disponível em: <https://www.supremecourt.gov/DocketPDF/17/17-2/23655/20171213123137791_17-2%20ac%20European%20Commission%20for%20filing.pdf>, p. 7.

640. Gummow e Hayne JJ em Neilson/Overseas Projects Corporation of Victoria Ltd (2005) 223 CLR 331, n.o 90.

641. Svantesson, D. (2017). Solving the Internet jurisdiction puzzle. Oxford, United Kingdom: Oxford University Press, p.171-189.

642. Macquarie Bank Limited & Anor/Berg [1999] NSWSC 526, n.o 14. Comparar, no entanto, com X contra Twitter Inc [2017] NSWSC 1300. Disponível em: <http://www8.austlii.edu.au/cgi-bin/viewdoc/au/cases/nsw/NSWSC/2017/1300.html> (discutido no capítulo 4.1.1).

643. Google Inc. contra Equustek Solutions Inc 2017 SCC 34.

644. Processo C194/16 Bolagsupplysningen OÜ Ingrid Ilsjan contra Svensk Handel AB.

645. Processo C18/18 GlawischnigPiesczek.

646. Hassell contra Bird 234 Cal. Rptr.3d 867 (2018). A Seção 230(c)(1) do Communications Decency Act estabelece que: "Nenhum provedor ou usuário de um serviço de computador interativo deverá ser tratado como o editor ou emissor de nenhuma informação oferecida por outro provedor de conteúdo de informação". Tradução livre de: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider".

647. Hassell contra Bird 234 Cal. Rptr.3d 867 (2018), p. 4.

648. Lessig, L. (1999). The law of the horse: What cyberlaw might teach. Harvard Law Review, 113(506).

649. Bygrave, L.A. (2015). Internet governance by contract. Oxford, United Kingdom: Oxford University Press, p.45.

650. Mahler, T. (2019). Generic topLevel domains – A study of transnational private regulation. Cheltenham, United Kingdom: Eduardo Elgar Publishing; Bygrave, L.A. (2015). Internet governance by contract. Oxford, United Kingdom: Oxford University Press, p.50.

4.2

651. Para além das aqui discutidas, os especialistas consultados apontaram para uma série de outras medidas técnicas que são importantes, mas talvez um pouco mais indiretamente relacionadas no que diz respeito às questões de jurisdição da Internet. Exemplos incluem, por padrão, modelagem de conteúdo algorítmico e desativação de *cookies* de rastreamento de terceiros em navegadores.

652. OneWeb. Disponível em: <https://www.oneweb.world/>.

653. Iridium. Disponível em: <https://www.iridium.com/>.

654. Ver, por exemplo: Farrell, H. (5 de dezembro de 2018). Rudy Giuliani is Trump's cybersecurity adviser. He might want a refresher. The Washington Post. Disponível em: <https://www.washingtonpost.com/news/monkey-cage/wp/2018/12/05/rudy-giuliani-is-trumps-cybersecurity-adviser-he-might-want-a-refresher/?noredirect=on&utm_term=.603492432f39>, e BBC News. (15 de novembro de 2018). Japan's cybersecurity minister has 'never used a computer'. Disponível em: <https://www.bbc.com/news/technology-46222026>.

655. Pelo menos em inglês, o primeiro artigo em profundidade da revista jurídica dedicado ao tema das tecnologias de geolocalização é: Svantesson, D. (2004, Fall). Geolocation technologies and other means of placing borders on the 'borderless' Internet. John Marshall Journal of Computer & Information Law, XXIII (1), 101– 39.

656. International League Against Racism & Anti Semitism (LICRA) e Union of French Jewish Students (UEJF) contra Yahoo! Inc, County Court of Paris, decisão interina de 20 de novembro de 2000. No entanto, parece que um dos especialistas, Ben Laurie, mais tarde sentiu a necessidade de explicar sua declaração (B Laurie, An Expert Apology (em arquivo com o autor)).

657. Macquarie Bank Limited & Anor/Berg [1999] NSWSC 526, n.o 12.

658. Plixer International, Inc. contra Scrutinizer GMBH, n.o 181195 (1st edition 2018), p.14.

659. Ver, por exemplo: Processos conjuntos C 585/08 Peter Pammer contra Reederei Karl Schlüter GmbH & Co KG e C144/09 Hotel Alpenhof GesmbH contra Oliver Heller, bem como Processo conjuntos C509/09 e C161/10 eDate Advertising GmbH e outros contra X e Société MGN Limited.

660. Processo C194/16 Bolagsupplysningen OÜ e Ingrid Ilsjan contra Svensk Handel AB, para 48.

661. Ver mais em: Svantesson, D. (2008). How does the accuracy of geolocation technologies affect the law? Masaryk University Journal of Law & Technology, 2(1), pp. 11– 21.

662. Google France, e processo C-18/18 Glawischnig-Piesczek.

663. Processo C-50717 Google contra CNIL. Conclusões do Advogado Geral (, 10 de janeiro de 2019). Luxemburgo. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-01/cp190002pt.pdf>. Acesso em: 01 de outubro de 2020; Processo C-1818 Eva GLaWischnigpiesczek contra Facebook Ireland Limited. Conclusões do Advogado Geral. (4 de junho de 2019). Luxemburgo. Disponível em: <https://curia.europa.eu/jcms/upload/docs/application/pdf/2019-06/cp190069pt.pdf>. Acesso em: 01 de outubro de 2020.

664. Case C507/17 Google contra CNIL, para 70.

665. European Commission. Digital single market: Economy & society. Disponível em: <https://ec.europa.eu/digital-single-market/en/economy-society>.

666. European Commission. Digital single market: Geoblocking. Disponível em: <https://ec.europa.eu/digital-single-market/en/policies/geoblocking>.

667. Federal Law No.276FZ. Disponível em: <http://publication.pravo.gov.ru/Document/View/0001201707300002?index=0&rangeSize=1>.

668. Internet & Jurisdiction Policy Network. (2017, novembro). Russian regulation outlawing the use of tools to circumvent access restrictions such as VPNs enters into force. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6552_2017-11> .

669. Cadell, C. & Martina, M. (30 de março de 2018). Businesses, consumers uncertain ahead of China VPN ban. Reuters. Disponível em: <https://www.reuters.com/article/us-china-vpns/businesses-consumers-uncertain-ahead-of-china-vpn-ban-idUSKBN1H612F>.

670. Internet & Jurisdiction Policy Network. (2018, março). China: Ban on nonstate sanctioned VPNs entered into force. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6891_2018-03>.

671. Por exemplo, no caso da repercussão do GDPR, os jornais não europeus que bloqueavam os usuários europeus (<https://data.verifiedjoseph.com/dataset/websites-not-available-eu-gdpr>) na verdade utilizaram medidas de bloqueio geográfico com o argumento de que o custo potencial da não conformidade seria consideravelmente mais elevado.

672. Cimpanu, C. (11 de fevereiro de 2019). Russia to disconnect from the Internet as part of a planned test. ZD Net. Disponível em: <https://www.zdnet.com/article/russia-to-disconnect-from-the-internet-as-part-of-a-planned-test/>.

673. 2nd Global Conference of the Internet & Jurisdiction Policy Network. (26-28 fevereiro de 2018). Otawa Roadmap. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/Secretariat-Summary-and-Ottawa-Roadmap-second-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf> , pp. 10-11. Para as propostas concretas, ver: Internet & Jurisdiction Policy Network. Domains & Jurisdiction Program Operational Approaches. Disponível em: <http://internetjurisdiction.net/Domains-Jurisdiction-Program-Operational-Approaches>. Para o último plano de trabalho, ver 3rd Global Conference of the Internet & Jurisdiction Policy Network. (3 - 5 de junho de 2019). Berlin Roadmap. Disponível em: <https://www.internetjurisdiction.net/uploads/pdfs/Berlin-Roadmap-and-Secretariat-Summary-3rd-Global-Conference-of-the-Internet-Jurisdiction-Policy-Network.pdf>.

674. Roadshow Films Pty Limited contra Telstra Corporation Limited [2018] FCA 582, para. 3.

675. Ver mais em: Freedom House. (2017). Freedom on the net 2017. Disponível em: <https://freedomhouse.org/report/freedom-net/2017/france>

676. Cook. S, (24 de junho de 2019). China's Long, Hot Summer of Censorship. The Diplomat. Disponível em: <https://thediplomat.com/2019/06/chinas-long-hot-summer-of-censorship/>.

677. Van Graver. D, (4 de julho de 2019). The "new era" of digital authoritarianism. The Interpreter. Disponível em: <https://www.lowyinstitute.org/the-interpreter/new-era-digital-authoritarianism>.

678. Nadjitan, D.N. (14 de julho de 2019). Chad Lifts Ban on SocialMedia Usage After More Than a Year. Bloomberg. Disponível em: <https://www.bloomberg.com/news/articles/2019-07-14/chad-lifts-ban-on-social-media-usage-after-more-than-a-year>.

679. Internet & Jurisdiction Policy Network. (2018, maio). Papua New Guinea announces monthlong Facebook block over misinformation, adult content and fake accounts. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7038_2018-05>.

680. Abdellah, M., Ahmed, H. & Atallah, M.S. (2018, 26 de maio). Top Egypt court orders temporary YouTube ban over Prophet Mohammad video. Reuters. Disponível em: <https://www.reuters.com/article/us-egypt-youtube/top-egypt-court-orders-temporary-youtube-ban-over-prophet-mohammad-video-idUSKCN1IR0FD>.

681. Internet & Jurisdiction Policy Network. (2018, maio). Egypt Supreme Administrative Court orders onemonth block of YouTube over 2012 antiIslamic video. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7049_2018-05>.

682. MacFarquhar, N. (13 de abril de 2018). Russian court bans Telegram app after 18minute hearing. The New York Times. Disponível em: <https://www.nytimes.com/2018/04/13/world/europe/russia-telegram-encryption.html>.

683. Transparency International. (16 de maio de 2018). Russia: Telegram block leads to widespread assault on freedom of expression online. Disponível em: <https://www.transparency.org/news/pressrelease/russia_telegram_block_leads_to_widespread_assault_on_freedom_of_expression.>.

684. Internet & Jurisdiction Policy Network. (2018, abril). Russian court orders block of Telegram, regulator blocks millions of IP addresses belonging to Google and Amazon. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6952_2018-04>.

685. Safi, M. (15 de março de 2018). Sri Lanka accuses Facebook over hate speech after deadly riots. The Guardian. Disponível em: <https://www.theguardian.com/world/2018/mar/14/facebook-accused-by-sri-lanka-of-failing-to-control-hate-speech>.

686. Internet & Jurisdiction Policy Network. (2018, março). Sri Lanka temporarily blocks access to Facebook for not doing enough in combatting hate speech on their platforms. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6885_2018-03>.

687. Internet & Jurisdiction Policy Network. (2019, abril). Sri Lanka blocks access to social media in wake of terrorist attacks. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6885_2018-03>.

688. Silviana, C. (8 de novembro de 2017). Indonesia plans automated system to flag contentious Internet material. Reuters. Disponível em: <https://www.reuters.com/article/us-indonesia-internet/indonesia-plans-automated-system-to-flag-contentious-internet-material-idUSKBN1D815Z?feedType=RSS&feedName=technologyNews>.

689. Internet & Jurisdiction Policy Network. (2017, novembro). Indonesia plans to launch automated flag system to better detect pornography and extremist content online. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6556_2017-11>.

690. Internet & Jurisdiction Policy Network. (2019, maio). Indonesia restricts access to social media in response to riots. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaW5kb25lc2lhIiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDgifQ==>.

691. Mamabolo, M. (6 de setembro de 2017). Reports of Togo Internet shutdown as anti-govt protests intensify. IT Web Africa. Disponível em: <http://www.itwebafrica.com/networks/890-togo/240006-reports-of-togo-internet-shutdown-as-anti-govt-protests-intensify?utm_content=bufferf190a&utm_medium=social&utm_source=twitter.com&utm_campaign=buffer>.

692. Internet & Jurisdiction Policy Network. (2017, setembro). Togo shuts down WhatsApp and slows down Internet access as antigovernment protests intensify. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6279_2017-09>.

693. Internet & Jurisdiction Policy Network. (2017, maio). Thailand: Facebook complies with requests to remove content deemed illegal. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-5928_2017-05>.

694. LeesAnguansuk, S. & Tortermvasana, K. (9 de maio de 2017). Facebook to block local content. Bangkok Post. Disponível em: <http://www.bangkokpost.com/news/politics/1246010/facebook-to-block-local-content>.

695. Gumrukcus, T. (5 de maio de 2017). Turkish court rejects Wikipedia's appeal over website's blocking: Anadolu. Reuters. Disponível em: <http://www.reuters.com/article/us-turkey-security-internet-wikipedia-idUSKBN18117M>.

696. Gumrukcus, T. (5 de maio de 2017). Turkish court rejects Wikipedia's appeal over website's blocking: Anadolu. Reuters. Disponível em: <http://www.reuters.com/article/us-turkey-security-internet-wikipedia-idUSKBN18117M>.

697. Internet & Jurisdiction Policy Network. (2017, maio). Turkey: Wikipedia appeals blocking order in constitutional court. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-5926_2017-05>.

698. Internet & Jurisdiction Policy Network. (2019, maio). Wikimedia petitions European Court of Human Rights to overturn two year block on Wikipedia in Turkey. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoidHVya2V5IiwiZnJvbSI6IjIwMTktMDEiLCJ0byI6IjIwMTktMDgifQ==>.

699. Twitter Public Policy. (25 de novembro de 2017). Pakistani action to block Twitter. Disponível em: <https://twitter.com/policy/status/934471989963689984>.

700. Internet & Jurisdiction Policy Network. (2017, novembro). Twitter announces that it is being blocked by the Pakistani government. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6563_2017-11>.

701. Bradsher, K. (25 de setembro de 2017). China blocks WhatsApp, broadening online censorship. The New York Times. Disponível em: <https://www.nytimes.com/2017/09/25/business/china-whatsapp-blocked.html>.

702. Internet & Jurisdiction Policy Network. (2017, setembro). China blocks WhatsApp messaging app. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6277_2017-09>.

703. Taye, B. (15 de janeiro de 2019). Zimbabwe orders a threeday, countrywide Internet shutdown. Access Now. Disponível em: <https://www.accessnow.org/zimbabwe-orders-a-three-day-country-wide-internet-shutdown/>.

704. Dzirutwe, M. (21 de janeiro de 2019). Zimbabwe court says Internet shutdown illegal as more civilians detained. Reuters. Disponível em: <https://www.reuters.com/article/us-zimbabwe-politics/zimbabwe-court-says-internet-shutdown-during-protests-was-illegal-idUSKCN1PF11M>.

705. The Guardian. (6 de janeiro de 2019). DRC officials postpone presidential election results. Disponível em: <https://www.theguardian.com/world/2019/jan/06/drc-officials-postpone-presidential-election-results>.

706. Internet & Jurisdiction Policy Network. (2018, dezembro). Democratic Republic of Congo: Internet access restricted following general election. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7739_2018-12>.

707. Rahman Alfa Shaban, A. (12 de dezembro de 2017). Ethiopia restricts Internet access amidst new protests. Africa News. Disponível em: <http://www.africanews.com/2017/12/12/ethiopia-restricts-internet-access-amidst-new-protests/>.

708. Internet & Jurisdiction Policy Network. (2017, dezembro). Ethiopia restricts Internet access as student protests grow violent. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6627_2017-12>.

709. Rahman Alfa Shaban, A. (27 de novembro de 2017). Internet restriction in Cameroon's Anglophone region hitting 60day mark. Africa News. Disponível em: <http://www.africanews.com/2017/11/27/internet-restriction-in-cameroon-s-anglophone-region-hitting-60-day-mark/>.

710. Internet & Jurisdiction Policy Network. (2017, novembro). Internet access restriction in Cameroon's Anglophone regions reaches 60day mark. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6565_2017-11>.

711. Internet & Jurisdiction Policy Network. (2019, agosto). India shuts down Internet access in Kashmir. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoiaW5kaWEiLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9>.

712. Internet & Jurisdiction Policy Network. (2019, março). Algeria blocks access to the Internet in order to crackdown on protests. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoic3VkYW4iLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9>.

713. Internet & Jurisdiction Policy Network. (2019, julho). Partial restoration of Internet access in Sudan. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#eyJxIjoic3VkYW4iLCJmcm9tIjoiMjAxOS0wMSIsInRvIjoiMjAxOS0wOCJ9>.

714. Amnesty International. (28 de abril de 2019). Benim: Internet shutdown on election day is a blunt attack on freedom of expression. Disponível em: <https://www.amnesty.org/en/latest/news/2019/04/benin-internet-shutdown-on-election-day-is-a-blunt-attack/>.

715. AFRINIC. (2 de junho de 2017). Common statement by AF* on Internet shutdowns in Africa. Disponível em: <https://www.afrinic.net/en/library/news/2141-common-statement-by-af-on-internet-shutdowns-in-africa>.

716. Internet & Jurisdiction Policy Network. (2017, junho). African Internet organizations criticize government shutdowns in joint statement. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6101_2017-06>.

717. United Nations, General Assembly. Human Rights Council: Resolution: Promotion and protection of all human rights, civil, political economical, social and cultural rights, including the right to development. A/HRC/38/L.10 (2018) p.3.

718. Cost of Shutdown Tool. Disponível em: <http://netblocks.org/projects/cost>.

719. AccessNow. #KeepItOn. Disponível em: <https://www.accessnow.org/keepiton/>.

720. Gupta, K. (10 de setembro de 2018). Google agrees to comply with RBI's data localization norms. Live Mint. Disponível em: <https://www.livemint.com/Companies/xEAFZGZ9kOaMz6R4HIgwXK/Google-ready-to-comply-with-RBI-norms-for-payment-services.html>.

721. Internet & Jurisdiction Policy Network. (2018, setembro). Google agrees to India's central bank's data localization requirements. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-7463_2018-09>.

722. Singh Mankotia, A. (24 de julho de 2019). Changes likely in proposed data privacy rules: Only critical data may need to be housed in India. The Economic Times. Disponível em: <https://economictimes.indiatimes.com/tech/internet/changes-likely-in-proposed-data-privacy-rules-only-critical-data-may-need-to-be-housed-in-india/articleshow/70355298.cms?from=mdr>.

723. KPMG. (2017, fevereiro). Overview of China's Cybersecurity Law. Disponível em: <https://assets.kpmg/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf>.

724. Innis, M. & Wiyoso, A. (2018, julho). General data localization requirements in Indonesia. Baker McKenzie. Disponível em: <https://www.bakermckenzie.com/-/media/files/insight/publications/2018/07/al_generaldatalocalizationrequirements_july2018.pdf?la=en>.

725. Sputnik International. (18 de abril de 2018). Russia's watchdog may block Facebook if network fails to comply with laws. Disponível em: <https://sputniknews.com/russia/201804181063669626-russia-watchdog-may-block-facebook/>.

726. Internet & Jurisdiction Policy Network. (2018, abril). Russian regulator says Facebook will be blocked unless it complies with data localization requirements. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-6961_2018-04>.

727. Internet & Jurisdiction Policy Network. (2016, novembro). Russia blocks LinkedIn for noncompliance with data localization rules. I&J Retrospect Database. Disponível em: <https://www.internetjurisdiction.net/publications/retrospect#article-4192_2016-11>.

728. Moscow Times. (12 de abril de 2019). Russia fines Facebook for failing to provide information on user data. Disponível em: <https://www.themoscowtimes.com/2019/04/12/russia-fines-facebook-for-failing-to-provide-information-on-user-data-a65225>.

729. MacCarthy, M. (26 de outubro de 2018). AIdriven content moderation can never be perfect. CIO. Disponível em: <https://www.cio.com/article/3316562/artificial-intelligence/artificial-intelligence-driven-content-moderation-can-never-be-perfect.html>.

730. Ver, por exemplo: Hutt, J.J. (26 de abril de 2018). Why YouTube shouldn't over-rely on artificial intelligence to police Its platform. ACLU. Disponível em: <https://www.aclu.org/blog/privacy-technology/internet-privacy/why-youtube-shouldnt-over-rely-artificial-intelligence>.

731. PwC. (2018). Top policy trends of 2018. Disponível em: <https://www.pwc.com/us/en/risk-regulatory-consulting/assets/top-policy-trends-2018.pdf>, p.13.

732. Garcia, E. (19 de abril de 2018). The artificial intelligence race: US, China and Russia. Modern Diplomacy. Disponível em: <https://moderndiplomacy.eu/2018/04/19/the-artificial-intelligence-race-u-s-china-and-russia/>.

733. World Economic Forum. AI Government Procurement Guidelines. Disponível em: <https://www.weforum.org/whitepapers/ai-government-procurement-guidelines>.

734. G20. (2019, junho). G20 AI Principles. Disponível em: <https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/pdf/documents/en/annex_08.pdf>. Acesso em: 03 de outubro de 2020.

735. OCDE. OECD Principles on AI. Disponível em: <http://www.oecd.org/going-digital/ai/principles/>.

736. Personal Data Protection Commission Singapore. Proposed Model AI Governance Framework. Disponível em: <//www.pdpc.gov.sg/Resources/Model-AI-Gov>.

737. Personal Data Protection Commission Singapore. Proposed Model AI Governance Framework. Disponível em: <//www.pdpc.gov.sg/Resources/Model-AI-Gov>.

738. Monetary Authority of Singapore. (2018, novembro). Principles to promote fairness, ethics, accountability and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector. Disponível em: <https://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf>.

739. United Nations and International Telecommunication Union. (2018). United Nations activities on artificial intelligence. Disponível em: <https://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-UNACT-2018-1-PDF-E.pdf>.

740. European Commission's High-Level Expert Group on Artificial Intelligence. (18 de dezembro de 2018). Draft ethics guidelines for trustworthy AI. Disponível em: <https://ec.europa.eu/digital-single-market/en/news/draft-ethics-guidelines-trustworthy-ai>. Acesso em: 03 de outubro de 2018.

741. Comissão Europeia. (8 de abril de 2018). Orientações Éticas para uma IA de Confiança. Disponível em: <https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=60435>. Acesso em: 03 de outubro de 2020.

742. European Commission. The European AI Alliance. Disponível em: <https://ec.europa.eu/digital-single-market/en/european-ai-alliance>.

743. Council of Europe (4 de dezembro de 2018). Council of Europe adopts first European Ethical Charter on the use of artificial intelligence in judicial systems. Disponível em: <https://www.coe.int/en/web/artificial-intelligence/-/council-of-europe-adopts-first-european-ethical-charter-on-the-use-of-artificial-intelligence-in-judicial-systems>.

744. Council of Europe. (11 de setembro de 2019). The Council of Europe established an ad hoc committee on Artificial Intelligence – CAHAI. Disponível em: <https://www.coe.int/en/web/artificial-intelligence/-/the-council-of-europe-established-an-ad-hoc-committee-on-artificial-intelligence-cahai>.

745. Council of Europe. (2019, maio). Unboxing artificial intelligence: 10 steps to protect human rights. Disponível em: <https://rm.coe.int/unboxing-artificial-intelligence-10-steps-to-protect-human-rights-reco/1680946e64>.

746. Council of Europe. (14 de fevereiro de 2019). Declaration by the Committee of Ministers on the manipulative capabilities of algorithmic processes. [Press Release]. Strasbourg. Disponível em: <https://www.coe.int/en/web/data-protection/-/declaration-by-the-committee-of-ministers-on-the-manipulative-capabilities-of-algorithmic-processes>.

747. Council of Europe. (16 de novembro de 2018). Draft Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes MSIAUT(2018)07. Disponível em: <https://rm.coe.int/draft-declaration-on-the-manipulative-capabilities-of-algorithmic-proc/16808ef257>.

748. Council of Europe. (12 de novembro de 2018). Draft Recommendation of the Committee of Ministers to member States on human rights impacts of algorithmic systems MSIAUT(2018)06. Disponível em: <https://rm.coe.int/draft-recommendation-on-human-rights-impacts-of-algorithmic-systems/16808ef256>.

749. Council of Europe. (9 de novembro de 2018). A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework MSIAUT(2018)05. Disponível em: <https://rm.coe.int/draft-study-of-the-implications-of-advanced-digital-technologies-inclu/16808ef255>.

750. Council of Europe. (2017, dezembro). Algorithms and Human Rights: Study on the human rights dimensions of automated data processing techniques and possible regulatory implications DGI(2017)12. Disponível em: <https://rm.coe.int/algorithms-and-human-rights-study-on-the-human-rights-dimension-of-aut/1680796d10>.

751. UNESCO. (9 de setembro de 2019). UNESCO engages technology and policy experts for human centered AI in Africa. Disponível em: <https://en.unesco.org/news/unesco-engages-technology-and-policy-experts-human-centered-ai-africa>.

752. Die Bundesregierung. Nationale KI strategie. Disponível em: <https://www.ki-strategie-deutschland.de/home.html> A versão em inglês do documento de estratégia está disponível aqui: <https://www.ki-strategie-deutschland.de/home.html?file=files/downloads/Nationale_KI-Strategie_engl.pdf>.

753. Access Partnership and University of Pretoria. (2018, novembro). Artificial intelligence for Africa: An opportunity for growth, development and democratisation. Disponível em: <https://www.up.ac.za/media/shared/7/ZP_Files/ai-for-africa.zp165664.pdf>, p.3.

754. Gadzala, A. (2018, novembro). Coming to life: Artificial intelligence in Africa. Atlantic Council. Disponível em: <https://www.atlanticcouncil.org/images/publications/Coming-to-Life-Artificial-Intelligence-in-Africa.pdf>.

755. Gadzala, A. (2018, novembro). Coming to life: Artificial intelligence in Africa. Atlantic Council. Disponível em: <https://www.atlanticcouncil.org/images/publications/Coming-to-Life-Artificial-Intelligence-in-Africa.pdf>, p.1.

756. Access Now. (2018, novembro). Human rights in the age of artificial intelligence. Disponível em: <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>.

757. World Wide Web Foundation. (2018, setembro). Algorithms and artificial intelligence in Latin America. Disponível em: <http://webfoundation.org/docs/2018/09/WF_AI-in-LA_Report_Screen_AW.pdf>.

758. Subcommittee on Information Technology, Committee on Oversight and Government Reform of the U.S. House of Representatives. (2018, setembro). Rise of the machines: Artificial intelligence and its growing impact on U.S. Policy. Disponível em: <https://oversight.house.gov/wp-content/uploads/2018/09/AI-White-Paper-.pdf>.

759. National Institution for Transforming India. (2018, junho). Discussion paper: National strategy for artificial intelligence. Disponível em: <http://niti.gov.in/writereaddata/files/document_publication/NationalStrategy-for-AI-Discussion-Paper.pdf>.

760. Amnesty International and Access Now. (2018, maio). Toronto Declaration: Protecting the rights to equality and nondiscrimination in machine learning systems. Disponível em: <https://www.accessnow.org/cms/assets/uploads/2018/08/The-Toronto-Declaration_ENG_08-2018.pdf>.

761. ARTICLE19 & Privacy International. (2018, abril). Privacy and freedom ofeExpression In the age of artificial intelligence. Disponível em: <https://privacyinternational.org/sites/default/files/2018-04/Privacy%20and%20Freedom%20of%20Expression%20%20In%20the%20Age%20of%20Artificial%20Intelligence.pdf>.

762. ARTICLE19. (2019, abril). Governance with teeth: How human rights can strengthen FAT and ethics initiatives on artificial intelligence. Disponível em: <https://www.article19.org/wp-content/uploads/2019/04/Governance-with-teeth_A19_April_2019.pdf>.

763. McKinsey Global Institute. (2017, abril). Artificial intelligence: Implications for China. Disponível em: <https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx>, p 1.

764. Luo, Y., Kaja, A. & Karch, T.J. (16 de julho de 2018). China's framework of AI standards moves ahead. The National Law Review.Disponível em: <https://www.natlawreview.com/article/china-s-framework-ai-standards-moves-ahead>.

765. G7. (2018). Annex B: G7 Innovation Ministers' Statement on Artificial Intelligence. Disponível em: <https://g7.gc.ca/en/g7-presidency/themes/preparing-jobs-future/g7-ministerial-meeting/chairs-summary/annex-b/>.

766. McKinsey Global Institute. (2017, abril). Artificial intelligence: Implications for China. Disponível em: <https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/China/Artificial%20intelligence%20Implications%20for%20China/MGI-Artificial-intelligence-implications-for-China.ashx>, p.4.

767. United Arab Emirates. (2017, outubro). UAE Artificial intelligence strategy. Disponível em: <http://www.uaeai.ae/en/>.

768. Svantesson. D, J. B. (4 de agosto de 2019). Vision for the future of private international law and the Internet – Can artificial intelligence succeed where humans have failed?. Harvard International Law Journal Blog. Disponível em: <https://harvardilj.org/2019/08/a-vision-for-the-future-of-private-international-law-and-the-internet-can-artificial-intelligence-succeed-where-humans-have-failed/>.

Notas do Capítulo 05
Grupos de conceitos relevantes

5.1

769. Para uma discussão detalhada do direito internacional privado, tal como aplicado à Internet, ver por exemplo: Svantesson, D. (2016) Private International Law and the Internet (3rd ed.). Alphen aan den Rijn, The Netherlands: Kluwer Law International.

770. Nagan, W.P. (1981-82). Conflicts theory in conflict: A systematic appraisal of traditional and contemporary theories. Journal of International and Comparative Law, 3(3), 343-546, 361.

5.2

771. McDougal, M. & Jasper, R. (1982). The Foreign Sovereign Immunities Act of 1976: Some suggested amendments. In M. Landwehr (Ed.), Private investors abroad—Problems and solutions in international business in 1981. New York, NY: M. Bender, 6.

772. Para uma discussão detalhada sobre jurisdição, tal como aplicada no direito internacional público, ver por exemplo: Ryngaert, C. (2015) Jurisdiction in International Law 2nd edn. Oxford, United Kingdom: Oxford University Press. Ver também: Schmitt, M. (Ed.) (2017) Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, United Kingdom, Cambridge University Press, 51-78.

773. Para uma visão sobre o tema da soberania, tal como aplicado on-line, ver por exemplo: Schmitt, M. (Ed.) (2017). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. Cambridge, United Kingdom, Cambridge University Press, 11-29.

774. Ver mais em: Polcak, R. & Svantesson, D. (2017). Information sovereignty – Data privacy, sovereign powers and the rule of law. Cheltenham, UK: Edward Elgar Publishing, 63-65.

775. Ver mais em: Ginsburg, T. (2017). Introduction to symposium on sovereignty, cyberspace, and Tallinn Manual 2.0. AJIL Unbound, 111, 205–206; Wright, J. (23 de maio de 2018). Cyber and international law in the 21st century. Disponível em: <https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century>.

776. Österdahl, I. (1992), Freedom of Information in Question. Uppsala, Sweden: Iustus Förlag AB, 136-137.

777. Österdahl, I. (1992), Freedom of Information in Question. Uppsala, Sweden: Iustus Förlag AB, 137.

5.3

778. Wikipédia. Microsoft Corp. contra United States. Disponível em: https://en.wikipedia.org/wiki/Microsoft_Corp._contra_United_States>.

5.4

779. Ver, por exemplo: Hilton contra Guyot 159 EUA 113 (1895) 164.

780. Ver, por exemplo: Crawford, J. (2012). Brownlie's principles of public international law (8th ed.). Oxford, UK: Oxford University Press.

781. Ver mais em: Corfu Channel (United Kingdom contra Albania) [1949] ICJ Rep 4.

5.5

782. Ver, por exemplo: Lawson contra Accusearch Inc dba Abika.com [2007] 4 FCR 314 e Weltimmo s.r.o.v. Nemzeti Adatvédelmi és Információszabadság Hatóság (Case C 230/ 14). Ver também: Svantesson, D. (2012). Extraterritoriality in the context of data privacy regulation. Masaryk University Journal of Law and Technology 7(1) 87-96, 92-93. Disponível em: <https://journals.muni.cz/mujlt/article/viewFile/2628/2192>.

783. SS 'Lotus' (France contra Turkey) (1927) PCIJ Series A, No 10.

5.6

784. Svantesson, D. (2016). Private international law and the Internet (3rd ed.). Alphen aan den Rijn, The Netherlands: Kluwer Law International.

785. De acordo com a doutrina do forum *non conveniens*, um tribunal pode recusar-se a exercer jurisdição por ser "um fórum claramente inadequado" (ao abrigo da lei australiana), ou mais comumente, devido à existência de outro tribunal que pode mais apropriadamente julgar um caso.

786. Lis alibi pendens [no direito brasileiro, usa-se a expressão "litispendência"] instrui um tribunal a suspender um processo quando outro processo está pendente em outro lugar. Assim, o objetivo final é evitar julgamentos contraditórios sobre o mesmo assunto.

5.9

787. Para uma discussão detalhada sobre isso, ver: Warken. C., van Zwieten, L. & Svantesson, D. (2019). Rethinking the categorisation of data in the context of law enforcement cross-border access to evidence. International Review of Law, Computers & Technology.

788. Comissão Europeia. (17 de abril de 2018). Proposta de Diretiva do Parlamento Europeu e do Conselho que estabelece normas harmonizadas aplicáveis à designação de representantes legais para efeitos de recolha de provas em processo penal. COM (2018) 226 final e Comissão Europeia, (17 de abril de 2018). Proposta de Regulamento do Parlamento europeu e do Conselho relativo às ordens europeias de entrega ou de conservação de provas eletrônicas em matéria penal. COM (2018) 225 final.

5.10

789. Romero-Moreno, F. (2018). 'Notice and stay-down' and social media: amending Article 13 of the Proposed Directive on Copyright. International Review of Law, Computers & Technology, 1–24.

5.14

790. Council of Europe, Glossary. Disponível em: <https://www.coe.int/en/web/artificial-intelligence/glossary>.

791. Council of Europe, Glossary. Disponível em: <https://www.coe.int/en/web/artificial-intelligence/glossary>.

792. Wikipédia. Machine learning. Disponível em: <https://en.wikipedia.org/wiki/Machine_learning>.

793. Wikipédia. Natural language processing. Disponível em: <ttps://en.wikipedia.org/wiki/Natural_language_processing>.

794. Para uma discussão detalhada da relação entre direito e mineração de dados, ver por exemplo: Colonna, L. (2016). Legal Implications of Data Mining. Tallinn, Estonia: Tallinna Raamatutrükikoda.

A Rede de Políticas Internet & Jurisdição é a organização multissetorial que trata da tensão entre a natureza transfronteiriça da Internet e jurisdições nacionais.

Seu Secretariado facilita um processo político global entre os principais atores, a fim de permitir a cooperação e coerência política transnacionais. Os participantes da Rede de Políticas trabalham em conjunto para preservar a natureza transfronteiriça da Internet, proteger os direitos humanos, combater abusos e permitir a economia digital global. Desde 2012, a Rede de Políticas Internet & Jurisdição envolveu mais de 300 importantes entidades de diferentes grupos de atores ao redor do mundo, incluindo os governos, as maiores empresas de Internet do mundo, grupos da sociedade civil e principais universidades e organizações internacionais.

www.internetjurisdiction.net

nic.br

Núcleo de Informação
e Coordenação do
Ponto BR