

**Entendendo a fragmentação da Internet a partir de aspectos fundamentais sobre  
regulação, soberania digital e a experiência da União Europeia**  
*Understanding Internet fragmentation starting from fundamental aspects of regulation,  
digital sovereignty and the European Union experience*

Marcos Wachowicz<sup>1</sup>

Pedro de Perdigão Lana<sup>2</sup>

**RESUMO:** O advento da sociedade informacional e da Internet criaram sérias dificuldades para o mundo do direito. Apesar da perspectiva pela auto regulação ter sido muito forte e permanecer robusta em algum nível, diversas propostas foram elaboradas para efetivamente impor regras legais. Esse processo não ocorreu sem críticas, que ressaltam a necessidade de cuidado dobrado ao criar normas imperativas para o mundo digital, a fim de não afetar as potencialidades tecnológicas e de evitar uma fragmentação da Internet global, considerada por muitos um dos maiores problemas digitais atuais. Essa fragmentação é mais preocupante no caso de estabelecimento, por governos, de redes separadas da global, sob o argumento da soberania digital. Apesar de comumente esconderem medidas autoritárias, existe sólido embasamento para defesa dessas soberanias, em especial no que tange a desigualdade entre as nações na capacidade de influenciar o desenvolvimento da Internet. A atuação da União Europeia é um campo fértil para análises desses tópicos, tanto pelo impacto internacional de seus atos legislativos como pelos seus recentes movimentos visando avançar na regulação da Internet. Sugere-se aprofundar uma planejada e menos romantizada abordagem multissetorial, focando na diminuição da influência de grandes empresas que agem quase monopolisticamente, evitando um escalonamento das tensões e preservando o ambiente inovativo, competitivo e aberto do ciberespaço.

**PALAVRAS-CHAVES:** Internet, soberania, fragmentação, regulação, digital

**SUMMARY:** The advent of the Internet and the information society have created serious difficulties for the world of law. Although the perspective of self-regulation has been dominant and remains very robust, several proposals have been effectively applied to impose legal rules. This regulation wasn't implemented without criticism, highlighting the necessary extra care when creating imperative norms for the digital world, in order not to affect the technological potential and avoid a fragmentation of the global Internet, considered by many one of the greatest digital problems of our time. This fragmentation is particularly worrisome when related to the establishment, by governments, of networks separated from the global one, under the argument of digital sovereignty. Although commonly concealing authoritarian measures, there are solid grounds to defend sovereignty concepts, especially the inequality between nations in their ability to influence the Internet development. The European Union is an appropriate field for analysis of these topics, both by the international impact of its legislative acts and by its recent moves to advance Internet regulation. We suggest, as an answer to the problem, to deepen a planned and less romanticized multistakeholder approach, focusing on reducing the influence from quasi-monopolist companies, avoiding escalation of tensions, and preserving the innovative, competitive and open environment of cyberspace.

**KEYWORDS:** Internet, sovereignty, fragmentation, regulation, digital

---

<sup>1</sup> Professor de Direito da Universidade Federal do Paraná – UFPR. Doutor em Direito pela UFPR. Mestre em Direito pela Universidade Clássica de Lisboa - Portugal. Professor da Cátedra de Propriedade Intelectual no *Institute for Information, Telecommunication and Media Law* - ITM da Universidade de Münster - ALEMANHA (2018/19). Coordenador do Grupo de Estudos em Direito Autoral e Industrial - GEDAI / UFPR vinculado ao CNPq.

<sup>2</sup> Doutorando em Direito na UFPR. Mestre em Direito pela Universidade de Coimbra - Portugal. Professor de Direito da ISULPAR. Pesquisador do Grupo de Estudos em Direito Autoral e Industrial – GEDAI/ UFPR vinculado ao CNPq.

## 1. Considerações iniciais

A interação entre a Internet e o Direito já foi uma área bastante obscura, com propostas regulatórias que hoje seriam consideradas no mínimo curiosas. Mas o avanço da sociedade informacional sobre os mais diversos aspectos da vida (CASTELLS, 1999), em particular sobre o setor comercial, fez com que esse ambiente se tornasse uma parte do cotidiano da maior parte da população (em países de maior nível de desenvolvimento), convertendo-se em uma preocupação central de reguladores e juristas, buscando consolidar níveis razoáveis de segurança jurídica.

Isso não é o mesmo que dizer que não existem mais lacunas e problemas a serem discutidos no setor. Pelo contrário, esse aumento de importância leva a problemas ainda mais relevantes e difíceis de serem resolvidos, tanto política quanto juridicamente. Um grande exemplo disso é a recente revigoração das discussões sobre fragmentação da Internet, muito ligadas às reivindicações sobre soberania digital.

Todavia, para entender essa discussão, consideramos proveitoso, metodologicamente, fazer uma revisão bibliográfica básica, de objetivo exploratório e abordagem qualitativa, que retome a origem do debate e sua construção até o estado atual. É importante também, quando chegarmos à discussão do problema em si, não se prender apenas aos textos acadêmicos, buscando análises de relatórios e notícias contemporâneas. Ao fim, cabe sugerir uma linha de solução considerada preferencial para tentar diminuir os conflitos apresentados.

## 2. Conceitos essenciais da discussão

A discussão é construída sobre termos comumente utilizados de forma intercambiável, cabendo apontar quais conceituações seguimos. O passo inicial é diferenciar a Internet da *World Wide Web*, o sistema informacional elaborado por Berners-Lee em 1989 e tornado público em 1991, marcado pela utilização de URLs (*Uniform Resource Locators*), formatação HTML (*Hypertext Markup Language*) e conexões em HTTP (*Hypertext Transfer Protocol*). A rede WWW é o que a maioria das pessoas identifica com a Internet, mas esta última é mais abrangente (englobando outras aplicações) e antiga, com insipiente origem militar na ARPANET norte-americana, no final da década de 1960 (detalhando, LEINER *et al*, 2009).

A versão moderna da Internet surgiu junto com uma popularização dos computadores apenas a partir da década de 1980 e mais intensamente a partir de 1991. Ela é comumente definida, em especial pelo FEDERAL NETWORKING COUNCIL (2005) dos EUA, como um sistema global de redes de computadores logicamente interconectadas por meio dos protocolos IP e TCP/IP (*Transmission Control Protocol/Internet Protocol*) e protocolos derivados, sendo essa forma de conexão que a diferencia de outras redes globais. Alguns autores preferem uma concepção teórica

ampliativa, abrangendo a totalidades das redes de comunicação e informação digitais globais (“rede das redes”), incluindo os níveis inferiores de infraestrutura, como os equipamentos de *hardware*, e superiores de conteúdo (KUNER, 2017, p. 4 e SOLUM, 2009, pp. 48-50).

Para definir os atores envolvidos, adota-se a classificação de SVANTESSON: usuários; provedores de serviços da Internet, que podem ser de vários tipos (como hospedagem e fornecimento de conteúdo); e provedores de acesso à Internet, que são as operadoras e proprietários da infraestrutura da rede (2016, pp. 38-49)<sup>3</sup>. Essas categorias não são mutuamente exclusivas, pois nada impede que uma empresa se enquadre em mais de uma delas ou seja usuária de uma terceira.

Ciberespaço e Internet são aqui utilizados como sinônimos, embora diversos autores apontem que o segundo conceito é mais abrangente que o primeiro, que é ligado especialmente a questões espaciais virtuais (LESSIG, 2006; MUELLER, 2019, p. 10).

Outra definição importante no campo jurídico é a de territorialidade, que é a prerrogativa de um Estado para legislar e jurisdicionar as atividades em seu território, excluindo em geral a mesma competência de outros Estados. As regras de aplicação de leis e competência de tribunais são historicamente marcadas pelas conexões geográficas, como parte da própria ideia de soberania estatal (BIAZATTI & VILELA, 2017, pp. 6-7).

Entretanto, o próprio conceito de territorialidade é uma construção, ainda que muito consistente, baseada nas práticas de seu tempo. Nesse sentido, há décadas já se apontava que a visão tradicional sobre territorialidade já estava se enfraquecendo antes da problemática do ciberespaço, com um reconhecimento de que poderiam existir várias jurisdições sobre a mesma atividade transnacional (GOLDSMITH, 1998, pp. 1205-1212; LAMBACH, 2019, p.7-9)

## **2. As dificuldades causadas pela Internet ao Direito**

Os problemas colocados pela Internet não se restringem a apenas um ou outro ramo jurídico. Essas dificuldades se devem a diversas características que, apesar de previamente existentes em outras tecnologias, assumem um grau de intensidade único no ciberespaço<sup>4</sup>. São comuns as comparações com outras tecnologias que levantaram problemas parecidos com o da Internet, mas em menor escala, como o telegrama para relações contratuais. Essas comparações são em geral imprecisas, pois a enorme diferença quantitativa de usuários e conexões aqui se converte em uma diferença qualitativa, especialmente quando essa tecnologia muda as próprias

---

<sup>3</sup> Essa classificação não é unívoca e existem diferentes formas de agrupar ou subdividir os atores envolvidos, a exemplo de tipologia diversa de ASCENSÃO (2008).

<sup>4</sup> Para uma lista dessas características, com as mais importantes listadas abaixo, cf. SVANTESSON, 2016, pp. 56-60 e 64-66.

relações sociais, tornando antigas exceções em regras (POST, 2002, pp. 1376-1380).

A característica mais importante é a deslocalização, ou ausência de localização bem definida. Ela engloba três aspectos: i) uma forte atenuação das fronteiras que definem as nações soberanas; ii) a relativa independência de localizações geográficas e instantaneidade dos atos, diminuindo o efeito das distâncias na forma de acesso e recursos envolvidos (POST, 2002, pp. 1382-1384); e iii) a portabilidade, que é a possibilidade de se conectar à Internet de qualquer lugar do mundo com o mesmo aparelho, desde que haja um ponto de acesso, questão acentuada no caso dos VPNs (*Virtual Private Networks*) e da hospedagem ou serviços em nuvem.

Para exemplificar o motivo dessas características causarem confusão no sistema jurídico, a ausência de localização precisa das partes e dos produtos no ambiente eletrônico faz com que múltiplas jurisdições incidam simultânea ou concorrentemente sobre a mesma situação, às vezes até de forma contraditória (SVANTESSON, 2018, p. 114).

A imaterialidade e interatividade já levantavam questões em tecnologias anteriores à Internet, mas em grau de importância muito menor (VICENTE, 2005, p. 86). A imaterialidade foi realçada pelo grande valor assumido pelos bens digitais e por terem sido escancaradas as dificuldades da regulamentação de certos produtos sem conexão geográfica bem definida. Na interatividade, por sua vez, há uma diferença do caráter reativo do ciberespaço em relação a outras tecnologias porque a reação no processo de troca de informações é também do emitente, e não só do receptor, o que é importante particularmente para aspectos de responsabilização dos envolvidos, incluindo os intermediários (SVANTESSON, 2016, pp. 68-72).

Podemos, rapidamente, mencionar outras características: i) a relativa independência de linguagens, com ferramentas de tradução imediata cada vez melhores e facilmente acessíveis; ii) a elevada quantidade de usuários que podem acessar a rede simultaneamente, estimulados pelas relativamente baixas exigências e custos de informação/comunicação (embora ainda existam severas limitações, principalmente em países menos desenvolvidos); iii) o potencial de comunicar uma mesma informação para uma grande quantia de pessoas ao mesmo tempo; iv) a descentralização por natureza e histórica falta de órgãos de controle central (embora ambos sejam tópicos controversos<sup>5</sup>); v) a convergência, que é a grande capacidade de digitalizar outros bens, serviços e tecnologias e torna-los também parte do ciberespaço; e, finalmente, vi) o papel central dos intermediários, tanto a nível de acesso quanto a nível de conteúdo.

Em razão dessas características, em especial a da deslocalização, as áreas onde o princípio

---

<sup>5</sup> LESSIG argumenta que não há uma “natureza” do ciberespaço, pois não existe apenas uma única arquitetura possível e o código pode(ria) ser formulado para uma maior ou menor centralização (1999, pp. 505-506 e 514).

da territorialidade é historicamente forte acabaram sendo as mais afetadas pelas transformações da sociedade informacional. Lembra-se aqui da imposição por força de lei de objetos imateriais a um espaço territorial, que passou a ser tensionado pelo rápido processo de globalização que ocorreu na segunda metade do século XX e foi se fragilizando com as tecnologias informáticas em rede, resultando em mudanças regulatórias que, apesar de terem acertado em alguns pontos, se mostraram profundamente disfuncionais em outros (SVANTESSON, 2016, pp. 31-33 e 82<sup>6</sup>).

### **3. Linhas teóricas e respostas às dificuldades**

Diante de todas essas dificuldades, respostas começaram a surgir dentro de uma gradação entre duas correntes extremas. Sintetizando-as simplificadamente, uma defendia que as regras tradicionais seriam em geral suficientes para lidar com os conflitos do ciberespaço, argumentando que as mudanças que surgiam eram essencialmente formais e, portanto, não tão diferentes dos conflitos que apareceram em outros meios de telecomunicação de alcance internacional (exemplos famosos mais próximos dessa ponta são EASTERBROOK, 1996; e, de maneira mais ponderada, GOLDSMITH, 1998). A outra defendia a necessidade de fórmulas novas diante da excepcionalidade da Internet, constatando a existência de situações radicalmente diferentes das que existiam antes (na ponta mais radical desse espectro, JOHNSON & POST, 1996; GAUTRAIS & LEFEBVRE & BENYEKHLEF, 1997).

Uma síntese interessante pode ser encontrada em SVANTESSON, ao apontar que mesmo quando não se constatam alterações profundas do sistema jurídico vigente é muito difícil afirmar que se trata de mera extensão das normas pré-existentes. Seria, no mínimo, uma expansão transformativa do escopo original das regras (2016, pp. 87-88).

Essas visões se combinavam para chegar em diferentes respostas sobre o que fazer, dentre as quais identificamos três que consideramos mais relevantes. Sublinhe-se que esses modelos apresentados não se separam de forma rígida, dialogando muito entre si na implementação prática ao redor do mundo.

A primeira é harmonizar ou mesmo uniformizar internacionalmente as leis materiais, o que diminuiria muito a preocupação com a lei aplicável. Isto pode ser alcançado tanto por meio de regras materiais internacionais quanto por coordenação de processos legislativos nacionais, posição bastante defendida pelos órgãos comerciais internacionais (por ex., CICP, 2011). Em

---

<sup>6</sup> O autor aponta que a propriedade intelectual é um dos aspectos centrais da regulação Internet, notando o seu papel central nos primeiros conflitos jurisdicionais, essencialmente sobre direitos de marca. Isso é complementado por Ascensão, que afirma ser praticamente impossível encontrar conteúdo *online* que não seja objeto (ao menos em potencial) de direitos intelectuais (2012, p. 48).

defesa de tal tese, o efeito harmonizador e formação de consensos relativos parecem de fato ser a tendência mais capaz de minimizar os conflitos para lidar com as características mais problemáticas do ciberespaço, estimulando que as diferentes nações ajam conjuntamente e, em geral, equilibrando os potenciais danos às potencialidades tecnológicas e a direitos fundamentais como a privacidade. Essa linha pode ser encontrada em Regulamentos e Diretivas da União Europeia (UE) e em acordos internacionais vinculativos de propriedade intelectual (VICENTE, 2005, p. 110).

A segunda linha busca trabalhar com a flexibilidade tecnológica como forma de se evitar o caminho de modificações legais profundas. Ou seja, reformula-se a própria estrutura e funcionamento da Internet para que ela se adeque às regulações existentes, modificando essas últimas de forma complementar (GOLDSMITH, 1998, pp. 1214-1230). Exigindo medidas menos drásticas e buscando evitar quebras ou reestruturações de sistemas legais em sua totalidade, essa posição busca um meio-termo para alcançar uma possibilidade de regulamentação efetiva por parte dos Estados. Está aqui enquadrada, dentre exemplos recentes, a elaboração de instrumentos de geolocalização que indiquem onde estão as partes envolvidas em uma troca virtual, ou bloqueiem o acesso de acordo com a região (SVANTESSON, 2016, p. 5).

A terceira é tratar a Internet como um espaço diferenciado e um sistema próprio dentro dos sistemas jurídicos nacionais internacionais, com particularidades suficientes para ensejar uma separação, em maior ou menor medida, dos ordenamentos tradicionais. Geralmente, os que defendem a auto regulação adotam esse caminho, argumentando que é uma realidade em apartado que seria prejudicada por formas de intervenção características do mundo físico. Esse caminho foi marcadamente defendido na consolidação e popularização do ciberespaço (BOMSE, 2007, p. 1723-1726; MUELLER, 2019, p. 15), em grande parte devido à posição norte-americana favorável à auto regulação, o que pode ser observado nos atos da Administração do Governo Clinton (CLINTON & AL GORE, 1997) e no julgamento do primeiro caso cibernético de peso pela Suprema Corte dos EUA<sup>7</sup>.

Essa não é, contudo, uma posição defendida apenas pelos que avançam ideias de auto regulação. Uma proposta teórica com elevado envolvimento governamental ou intergovernamental é a criação de um Tribunal Internacional da Internet (ALMEIDA, 2018) ou, pensando em institutos já existentes e plenamente atuantes, os Tribunais da Internet chineses<sup>8</sup>.

---

<sup>7</sup> Reno v. American Civil Liberties Union, 521 U.S. 844 (1997). Ressalta-se trecho do Justice Stevens: “(...) *the phenomenal growth of the Internet seems to indicate that government regulation is not necessary in order to foster rapid growth of a new communications medium such as this (...), perhaps a lack of regulation may have done more to foster growth of the medium than the regulation itself might have.*”.

<sup>8</sup> Cf. <https://english.bjinternetcourt.gov.cn/>

Pelos viés da auto regulação, essa linha acaba sendo muito ligada à regulação por *soft law*, baseada em argumentos consequencialistas, em especial sobre benefícios econômicos, pois essa opção é: i) mais flexível e com proposições mais rapidamente criadas ou modificadas, o que é particularmente importante no caso na regulação de objetos altamente mutáveis, como são os bens tecnológicos; ii) surge do seio das situações que a ensejam, precisando ser validada e aceita na prática, diminuindo assim os riscos do rechaço contra imposições feitas de cima pra baixo; e iii) facilita que uma uniformização global seja alcançada ao não estabelecer regras obrigatórios, que usualmente encontram maior resistência (VICENTE, 2005, pp. 95-97; GAUTRAIS & LEFEBVRE & BENYEKHLEF, 1997, pp. 551-552).

Como um posicionamento mais radical dessa última linha, pode-se encontrar a defesa feita pelos chamados “ciberanarquistas” ou “ciberlibertários” de uma total (ou quase) auto regulação da Internet pelas mãos de seus usuários e programadores, se opondo à intervenção estatal. O texto mais conhecido talvez seja a Declaração de Independência do Ciberespaço de John Perry BARLOW (1996) e, de forma um pouco mais moderada e mais refinada técnica e juridicamente, os textos de David Johnson e David Post (JOHNSON & POST, 1996<sup>9</sup>; POST, 2002).

Resumidamente, esses autores argumentavam que os Estados e suas fronteiras tradicionais não seriam capazes de se adaptar à rápida dinâmica e particularidades da Internet, ocorrendo uma substituição por fronteiras tecnológicas. Apontavam a existência de problemas de regulação alegadamente incontornáveis, como a impossibilidade de notificar o usuário cada vez que acessava um site em outra jurisdição, ou a censura de conteúdos que seria estabelecida a partir dos parâmetros mais restritivos de único país. Defendiam que a ausência de coerção permitia uma organização mais natural do ciberespaço e que as restrições das liberdades seriam todas voluntárias. Para além disso, a estrutura do ciberespaço seria singularmente propícia para resolver por si só várias das falhas de mercado que justificavam a intervenção estatal no mundo físico, sendo um espaço profundamente frutífero para a auto regulação (GAUTRAIS & LEFEBVRE & BENYEKHLEF, 1997, 549-553).

A mistura dessas três linhas nas respostas apresentadas no curso da história para os problemas concretos evidencia que não são incompatíveis entre si. Entretanto, a proposta ciberlibertária, inicialmente muito chamativa, aparenta ter perdido muito de sua força original, apesar de ainda aparecer frequentemente em discursos e em críticas às novas normas regulatórias

---

<sup>9</sup> A conclusão desse texto é um excelente resumo das propostas ciberlibertárias: *"Global electronic communications have created new spaces in which distinct rule sets will evolve. (...) Just as a country's jurisprudence reflects its unique historical experience and culture, the law of Cyberspace will reflect its special character. (...) Law, defined as a thoughtful group conversation about core values, will persist. But it will not, could not, and should not be the same law as that applicable to physical, geographically-defined territories."*

do ciberespaço. O que ocorreu para que essa visão, que parecia se encaixar bem nas promessas da nova tecnologia, fosse tão reduzida? (ASCENSÃO, 2005, p. 789, LAMBACH, 2019, p. 2)

#### **4. Razões de regulamentação da Internet**

A participação estatal não é algo novo: se observa desde os tempos de ARPANET um papel ativo dos Estados em financiamento e administração, com a influência das empresas comerciais explodindo a partir do processo de rápida expansão da sociedade informacional (LAMBACH, 2019, pp. 12-13). Mas uma intervenção regulatória mais rígida e impositiva não foi bem vista durante muitos anos.

Um dos pontos mais notáveis e mais citados é que Estados e instituições intergovernamentais (como órgãos da ONU) tinham dificuldades de entender a nova tecnologia e de redigir leis efetivas nos passos iniciais desse novo cenário, embora alguns autores, como Timothy WU, afirmem que a falta de regulação estatal nessa etapa se deveu principalmente a uma falta de interesse ou atenção dos governos (1997). Contudo, a busca pela preservação de sua jurisdição causou crescente apreensão dos reguladores e juízes em relação à garantia de sua soberania. Afinal, leis ou decisões judiciais que não podem ser executadas ou que se mostram ineficazes na prática acabam por desmoralizar todo o sistema normativo (SVANTESSON, pp. 11-14 e 25-26).

Em paralelo a esse aumento de preocupações, os desenvolvimentos tecnológicos a partir do final do século XX tornaram cada vez menos factível ver a Internet como um mundo separado. Coroando a transformação desse cenário inicialmente indecifrável, várias das dificuldades jurídicas inicialmente levantadas se mostraram não só perfeitamente superáveis (VICENTE, 2005, pp. 91-92; GOLDSMITH, 1998), como algo que era exigido por diferentes setores da sociedade.

Uma das críticas mais importante nesse sentido foi a feita por Lawrence LESSIG, que apontou existirem quatro modalidades de regulação no “mundo real” e no ciberespaço: as leis, as normas sociais, o mercado e a arquitetura. No caso do mundo virtual, a arquitetura é o seu código e é permeado por determinados valores e objetivos dos programadores, que limitam ou ampliam as possibilidades de ações dos usuários nesse espaço. Em outras palavras, enquanto a arquitetura da Internet poderia ser (em teoria) neutra, seria quase impossível que as decisões sobre sua estrutura o fossem. O autor apontava o sério risco de passar de uma “arquitetura de liberdade” do

ciberespaço para uma “arquitetura de controle” sob um ideal de auto regulação (LESSIG, 2006)<sup>10</sup>.

Esse e outros argumentos embasaram diversas propostas governamentais sobre novas formas de regulamentação (BURK, 1997), indo desde a camada de infraestrutura da Internet até a de aplicações. Governos mais fortes no cenário internacional conseguiram inclusive instrumentalizar a Internet para aumentar sua influência e formular novos modos de coação transfronteiriços, com certos atos atingindo extensões verdadeiramente globais (LAMBACH, 2019, p. 15). Essas ferramentas de expansão foram geralmente construídas por meio de *soft power* em diferentes graus, como o fornecimento de auxílio tecnológico e apoio de técnica legislativa para países terceiros, propaganda internacional de legislações-modelo sobre questões digitais e coerção comercial. (KUNER, 2017, pp. 22-26)

Um dos mais famosos exemplos hoje é o Regulamento Geral de Proteção de Dados (RGPD) da UE, que indiretamente impôs um nível elevado de proteção em todo o mundo para evitar prejuízos concorrenciais ao mercado europeu, erigindo barreiras comerciais com empresas de países terceiros se elas (e os próprios governos) não adotassem níveis similares de proteção de dados (POLIDO *et al*, 2018, pp. 14-21).

Essa regulamentação implementada por entes públicos comumente surgiu a partir de reivindicações dos próprios agentes particulares, como empresas, consumidores e ciberusuários (DIEDRICH, 2000; ASCENSÃO, 2008). À medida que a Internet foi se tornando parte da vida comum e aumentando o contato com outras culturas e valores, fortaleceram-se as vontades de impor sobre ela as leis tradicionais que existiam no mundo físico, com ou sem adaptações (SCHULTZ, 2008, p. 804). No exemplo do comércio eletrônico, estenderam-se as garantias dos consumidores nas compras físicas para o meio virtual, ao mesmo tempo em que se elaboravam novos direitos para inibição de particularidades do *forum shopping* ou *law shopping* pelos grandes comércios *online* (BIAZATTI & VILELA, 2017, pp. 6-7).

O aumento de controle sobre o ciberespaço pode ocorrer de forma mais indireta e aberta, como se vê em alguma medida nas instituições europeias. Mas também pode ocorrer de maneira mais explícita e fechada, controlando acesso e conexão, característica de governos mais autoritários (CLAESSEN, 2020, pp. 142-143).

Esses dois modelos de avanços regulatórios quase sempre ocasionaram discussões sobre

---

<sup>10</sup> Esclarecendo uma confusão comumente feita, isso não significa que esse autor norte-americano era um defensor de intervenções governamentais. Pelo contrário, como um teórico do *copyright*, ele desconfiava profundamente dos governos na forma que existiam à época e permanecem existindo hoje. Um dos agravantes da possibilidade de arquiteturas de controle no ciberespaço é que ela pode competir ou reforçar as determinações legais, o que se torna um problema tanto pela não sujeição do código aos controles jurídicos legislados, quanto pela utilização do código por políticos ou mesmo agentes privados para impor valores e comportamentos sem que isso seja efetivado pelos procedimentos formais existentes (LESSIG, 1999).

conflitos com valores tradicionalmente liberais, como os direitos de liberdade de expressão ou de informação. Cabe abrir um parêntese aqui para lembrar que os valores ligados à diferentes noções de liberdade são um dos principais fundamentos da sociedade informacional e um dos alicerces da ética digital, dos direitos humanos aplicáveis ao ambiente virtual (como o artigo 19 da Declaração Universal de Direitos Humanos) e das políticas de desenvolvimento econômico baseados na Internet (VICENTE, 2005, pp. 88-89 e CASTELLS, 2014).

Por outro lado, não se pode identificar sempre a liberdade com a ausência de intervenção estatal. Pelo contrário, às vezes é essa própria intervenção que a garante (LESSIG, 1999, p. 542 & VICENTE, 2005, p. 92), mesmo em perspectivas liberais clássicas, como as sanções ao descumprimento contratual. A perspectiva de que foi somente o ambiente de auto regulação que proporcionou o rápido crescimento da Internet não parece ser verdadeira ao se lembrar que a popularização do ciberespaço, mesmo em sua fase eminentemente comercial, se deveu em grande parte às políticas públicas que levaram infraestrutura e educação digital para diversas categorias da população, especialmente para aquelas que eram, inicialmente, pouco interessantes comercialmente (BOMSE, 2007, pp. 1745-1748).

Essa tensão entre liberdades/valores e regras imperativas no cenário digital pode ser analisada de forma frutífera a partir do cenário europeu, assim como a recente escalada de conflitos entre os diferentes atores nos últimos anos.

## **5. A regulamentação Europeia e seus impactos globais**

Quando se fala do desequilíbrio de forças no direcionamento do ciberespaço no cenário internacional, usualmente o primeiro país a ser lembrado é os EUA, por serem de fato o agente mais importante no desenvolvimento dessa tecnologia. Contudo, para entender como a regulação governamental pode estimular a fragmentação da Internet, é valioso analisar a experiência da União Europeia na sua busca por protagonismo, algo que é feito mais raramente na doutrina.

A regulamentação da Internet pela UE sempre foi um campo tensionado. Mesmo internamente, apesar da cada vez maior prevalência das regras comunitárias, constata-se uma histórica disputa entre essa entidade e os Estados-membros sobre a competência para regular a Internet e a sociedade informacional (PEREIRA, 2001, p. 637; KUNER, 2017, pp. 7-11).

Assim como em outras regiões e países, na UE o processo regulatório não ocorre apenas no campo legislativo. Ele também se dá a nível do Judiciário, o que na Europa ocorre de forma ainda mais notável, especialmente nos casos em que decisões relacionadas à Internet tomam proporções globais. Uma decisão paradigmática é o controverso julgamento pelo Tribunal de Justiça da União Europeia (TJUE) do caso *Google Spain v. AEPD y Mario Costeja González*,

famoso por estabelecer o direito à desindexação (popularmente conhecido como “direito ao esquecimento”). Dentre as diversas questões analisadas, a mais importante aqui é a determinação do TJUE que uma tutela eficaz deveria ultrapassar o território espanhol, estendendo-se para a empresa matriz e com efeitos globais. Essa decisão reforçou intensamente a tendência de expansão das competências jurisdicionais dos tribunais mais influentes (LUGARESI, 2017, pp. 307-315; KOWALIK-BAŃCZYK & POLLICINO, 2016, pp. 425-428).

Complexificando ainda mais esse contexto, não é apenas esse tribunal que toma decisões importantes sobre a Internet na Europa. Além dos tribunais nacionais, a Corte Europeia de Direitos Humanos (CEDH) já assumiu posições de protagonismo, ainda que de maneira mais contida, na supressão de infrações de direitos humanos no âmbito da Internet, nomeadamente em questões de acesso à informação, liberdade de expressão, crimes virtuais, propriedade intelectual e proteção de dados (ECHR RESEARCH DIVISION, 2015). Não obstante, a doutrina aponta que TJUE está, pelo menos nas temáticas tecnológicas, ofuscando o papel da CEDH mesmo nos litígios cujo objeto são direitos humanos (KOWALIK-BAŃCZYK & POLLICINO, 2016, p. 336).

O aumento dessas decisões nos últimos anos ajuda a indicar a recente intensificação de proposições e ações regulatórias da Internet, das quais a UE é um dos principais agentes de um modelo sutil (SVANTESSON, 2018, p. 124), embora seja, inclusive na figura de seus estados-membros, extremamente crítica dos modelos mais fortes.

No espaço europeu foram frequentes os atos oficiais na última década que expuseram o objetivo de regulamentar com maior intensidade e força o ciberespaço. Isso ocorreu especialmente após a crise dos ciberataques contra a Estônia em 2007 e dentro do quadro do mercado único digital, argumentando-se por mais segurança e uma melhor governança da Internet (ver a Comunicação da Comissão COM(2015) 192 final). Na Comunicação (COM/2014/072 final), por exemplo, afirmou-se que essa tecnologia deveria estar submetida “às mesmas leis e normas que se aplicam noutros domínios da nossa vida quotidiana”.

Trata-se de um robustecimento da estratégia europeia para se firmar como protagonista do mundo digital, em contraposição principalmente aos EUA, o principal polo histórico de desenvolvimento da Internet e onde estão hoje localizadas boa parte das mais importantes instituições do ecossistema de Governança da Internet (LUGARESI, 2017, p. 307). Uma importante diferença é que o país americano tende mais para a não intervenção (VICENTE, 2005, p. 94), enquanto as abordagens da UE usualmente se fundamentam em visões mais protetivas e

indicam transformações muito mais profundas da rede<sup>11</sup>.

Há sem dúvida um lado positivo, que é o relativo maior cuidado das instituições europeias com determinados direitos fundamentais valorizados na cultura ocidental. Essa precaução pode ser vista no fortalecimento das discussões sobre privacidade e proteção de dados pessoais causados pelo RGPD no mundo, ou nos mencionados julgamentos da CEDH. A normatização pela UE pode também controlar a intemperança legislativa dos estados-membros, vedando leis sobre determinado assunto ou uniformizando e simplificando regras confusas e díspares dos estados membros (vide Comunicação da Comissão COM (2011) 942 final). Pode mesmo avançar na construção de uma sociedade internacional em áreas como o direito internacional privado (RAMOS, 2016, pp. 71-72), diminuindo os conflitos cibernéticos como um todo.

No entanto, a apreensão de outras nações é grande porque mesmo as regulações direcionadas para os estados-membros da UE acabam transbordando para além de suas fronteiras, na medida em que a Internet borra a distinção entre o direito comunitário voltado para o ambiente externo e o ambiente interno. Enquanto a regulação pesada de países como a China acaba sendo relevante principalmente para seu espaço interno devido ao isolamento de sua rede, há um potencial de influência internacional muito maior quando feita pela União Europeia (KOWALIK-BAŃCZYK & POLLICINO, 2016; KUNER, 2017), inclusive porque essa coordenação para criação de leis de Governança da Internet no mundo todo é um dos objetivos declarados das instituições europeias (CLAESSEN, 2020).

A RGPD surge novamente como exemplo dessas preocupações. Mesmo ao se concordar que suas consequências foram positivas e até necessárias, devem ser reconhecidas as críticas que apontam que há sérios problemas no ato normativo. Dentre elas, sublinha-se um notável foco na proteção das empresas europeias, em vez da privacidade de usuários; elevada quantia de regras pouco claras ou precisas; e ter levantado barreiras para o desenvolvimento de pequenas e médias empresas e de pesquisas de alta tecnologia, ocasionando fuga de empreendimentos e pesquisadores para outros locais com regras mais favoráveis (SVANTESSON, 2018, p. 118).

Outro caso similar é o da Diretiva relativa aos direitos de autor no mercado único digital (2016/0280), cujos artigos 15º e 17º (11º e 13º, no texto da proposta) foram foco de muitas críticas pela comunidade virtual, muito além do espaço europeu. O ex-artigo 13º em especial, pois indiretamente obrigava os provedores de serviços de Internet a instalar filtros de conteúdo para evitar sanções, ao mudar o padrão de responsabilização vigente que poderiam causar mudanças no modelo de negócios e sistemas de empresas de atuação multinacional. Essas mudanças foram

---

<sup>11</sup> Embora estejamos falando da UE, vale lembrar que posturas interventivas são uma tendência internacional, mesmo nos bastiões historicamente liberais como os EUA (SVANTESSON, 2018, p. 124).

avaliadas como potenciais causadoras de danos à liberdade de expressão e informação no ciberespaço global (GREGORIO, 2018). Nesse sentido, pode-se pensar até nos danos acidentais da lei alemã NetzDG, elaborada para combater conteúdo ilegal (especialmente discurso de ódio) pressionando os agentes intermediários, mas que acabou sendo um modelo para normas de censura em países autoritário por todo o mundo (MCHANGAMA & FISS, 2019)

É preciso ainda lembrar que é em si controversa a tentativa de universalizar os valores fundamentais europeus no cenário digital, diante das diferenças culturais e de prioridades de cada país. Mesmo que assumíssemos uma perspectiva de objetivismo moral e eles fossem considerados intrinsecamente salutares, passaria a ser necessário distingui-los daquilo que seriam meramente interesses europeus de caráter mais político, com efeitos reflexos negativos. Os problemas do alcance internacional de atos regionais aparecem no próprio comportamento paradoxal das instituições da UE, que se dedicam para a máxima extensão de sua influência normativa enquanto apresentam forte resistência em relação à aplicação de regras de países terceiros em seu território (KUNER, 2017, pp. 25-36). Esse movimento é mais observável nas cortes europeias, que no campo de valores culturais se inclinam a “ensinar” outras jurisdições muito mais do que a “aprender” delas (KOWALIK-BAŃCZYK & POLLICINO, 2016, p. 333).

A defesa dos próprios interesses no âmbito global não é em si negativa. É, na verdade, uma atividade absolutamente normal nas relações internacionais. Todavia, ao se assumir essa posição, é natural que outras nações assumam comportamentos similares, realizando esforços para favorecer seus próprios objetivos e valores (WU, 1997, pp. 656-664). No caso de uma tecnologia que tem como uma de suas principais características o alcance global, essa disputa tem consequências potencialmente graves.

Isso explica, em parte, a enorme cautela necessária para se promover um controle ativo da Internet até em situações em que há um certo consenso, como inibir espionagem entre governos, combater “*fake news*” e proteger dados pessoais, pois uma corrida legal nessa busca pode iniciar um ciclo vicioso onde leis cada vez mais severas de diferentes governos entrem em conflito tentando obter supremacia (SVANTESSON, 2018, p. 125). Isso, evidentemente, implicaria em insegurança jurídica e danos diretos a diversos setores, especialmente os direitos humanos fundamentais e a potencialidade benéfica da Internet.

## **6. Os problemas gerados pela soberania digital e fragmentação da Internet**

A Internet foi aprimorada e modificada por diversas vezes durante sua história, tendo como um de seus grandes trunfos ter sido construída sobre protocolos e padrões comuns e abertos (*open standards*). Essa escolha facilitou que novas adições à tecnologia fossem feitas cumulativamente

como blocos de construção reutilizáveis, focando em compatibilidade com os anteriores e futuros. Isso possibilitou uma alta adaptabilidade da rede global a novos desafios (DAIGLE, 2015).

Parecem existir algumas características e valores considerados essenciais para que essa tecnologia não perca o seu potencial de inovação e continue sendo uma força benéfica para o desenvolvimento social e econômico humano. Não há um consenso absoluto sobre quais são esses aspectos, mas são bastante reconhecidas as invariantes da Internet elegidas pela Internet Society, uma organização global cuja missão declarada é a defesa de uma rede aberta, globalmente conectada, segura e confiável. Essas invariantes incluem a construção tecnológicas sobre blocos reutilizáveis, englobando também: (i) a integridade, acessibilidade e o alcance globais, com qualquer ponto da rede podendo se conectar a qualquer outro; (ii) o propósito geral, aceitando aplicações dos mais diferentes tipos, que se alia à ausência de favoritos, sem barreiras competitivas inerentes; (iv) a possibilidade de inovar sem requerer permissão de uma autoridade; (v) a interoperabilidade, colaboração e acordos mútuos entre os diferentes operadores da rede (INTERNET SOCIETY, 2012; DAIGLE, 2015, pp. 5-9)<sup>12</sup>.

Ao se reconhecer essas características como essenciais, passa a ser possível notar a ameaça intrínseca de uma fragmentação da Internet, considerado por muitos o desafio principal da governança da Internet nos tempos de hoje. Tal relevância pode ser observada, dentre outros exemplos, no tema do *Internet Governance Forum* 2019 (“Um mundo. Uma rede. Uma visão”).

O conceito de fragmentação da Internet não é unívoco. Sua conceituação, a especificação de suas características e suas consequências dependem das experiências, valores e prioridades de cada pessoa/instituição. Existe, inclusive, quem afirme que certos tipos de fragmentação não só são inevitáveis como são também benéficos, considerando a complexificação e diversificação do uso cultural da tecnologia (NOAM, 2013).

Uma definição útil consta em relatório comissionado pelo Fórum Econômico Mundial, que subdivide o conceito em outros três: fragmentação técnica, fragmentação comercial e fragmentação governamental. O primeiro trata de condições na infraestrutura que obstaculizam o funcionamento consistente da tecnologia e a habilidade dos sistemas de alcançar plena interoperabilidade para trocar de pacotes, e o segundo se refere às práticas comerciais que limitam ou impedem certas utilizações de criação, distribuição ou acesso de informações (DRAKE & CERF & KLEINWÄCHTER, 2016). A terceira subdivisão é a que mais importa para as ideias que estamos trabalhando, que trata das políticas governamentais que limitam ou impedem certas utilizações de criação, distribuição ou acesso de informações.

---

<sup>12</sup> A classificação original é diferente, no presente texto invariantes relacionadas foram apresentas conjuntamente.

A fragmentação governamental é essencialmente formada por decisões políticas e é observável em diferentes declarações, como o controle de conteúdo ilegal naquele país, o protecionismo sobre o comércio interno, a segurança nacional, e políticas de proteção de dados e da privacidade. A grande preocupação da comunidade internacional se foca nas reivindicações de soberania digital ou cibersoberania, ou seja, a capacidade de um país de exercer maior controle sobre a Internet cuja infraestrutura ou usuários estão localizados dentro de seu território. MUELLER argumenta que existem sim diversas fronteiras no ciberespaço, mas que elas não se alinham com as fronteiras territoriais tradicionais (2019, pp. 13-15).

Uma das soluções adotadas é, então, “territorializar” a Internet, criando versões nacionais dela. Isso não remete apenas a redes que conectam apenas usuários de certa nação, ou que só tem material produzido nesse território, mas sim também a redes nacionais que podem ser “desconectadas” do resto do mundo, como foi feito com RuNET russa, ou cuja comunicação com a rede externa é controlada nos pontos de acesso, como ocorre com o Grande *Firewall* chinês.

Mesmo que seja impraticável controlar todos os aspectos do ciberespaço, outras (em particular a infraestrutura, como o controle exercido nos Pontos de Troca de Tráfego de Internet) são mais suscetíveis à intervenção governamental (MUELLER, 2019, pp. 4-5), e até os que consideram que a fragmentação é um rumo natural do desenvolvimento da Internet observam essa tendência específica com preocupação (DRAKE, 2017).

Esse embate entre uma Internet única global e redes regionalizadas se reflete também na disputa de mais de 20 anos entre as perspectivas de multilateralismo e multisetorialismo (*multistakeholderism*) na Governança da Internet<sup>13</sup>. Enquanto a primeira se refere a uma escolha por decisões verticalizadas e centradas na cooperação entre Estados, a segunda, dominante na governança da Internet desde a década de 90, opta pela descentralização ao diminuir a relevância dos agentes governamentais em prol da participação de setores privados e da sociedade civil. A disputa é observável principalmente nas CMSI (*WSIS*) de 2002 e 2005 e nas CMTI (*WCIT*) da UIT/ONU de 2012 e 2014 (LAMBACH, 2019, p. 16; MUELLER, 2019, p. 3).

As já mencionadas China e a Rússia são dois notórios agentes da defesa de uma “nacionalização da Internet”, além dos seus mais relevantes exemplos (LEE & LIU, 2012; STADNIK, 2019). Mas outros países também avançam argumentos similares, como a África do Sul, Índia e Brasil. A negociação sobre a criação de uma Internet dos BRICS chegou a ser anunciada em 2017, embora tenha sido suspensa pouco depois em razão da mudança do governo brasileiro (ADEE, 2019). Recentemente, contudo, as negociações voltaram a ocorrer (BELLI,

---

<sup>13</sup> Para uma análise detalhada entre multilateralismo e multisetorialismo, conferir DUTTON, 2015, pp. 25-33.

2020). Países como França e Alemanha (DRAKE & CERF & KLEINWÄCHTER, 2016, pp. 45-48) também já avançaram argumentos similares, assim como as instituições da UE (COMISSÃO EUROPEIA, 2019) e mesmo alguns teóricos militares norte-americanos (FRANZESE, 2009; DEMCHAK & DOMBROWSKY, 2001).

As críticas à fragmentação vão além dos valores fundantes acima descritos. Pesquisas indicam uma correlação direta entre a abertura da Internet (em seu sentido técnico, econômico e social) e seus efeitos benéficos, para criação de riquezas, aumento do bem estar social e proteção de direitos humanos. Embora essa rede não tenha nunca sido e dificilmente possa ser absolutamente aberta, os indícios existentes mostram que maiores graus de abertura têm consequências positivas sobre a educação, pesquisa, comércio internacional, inovação empreendedora, coordenação da sociedade civil, dentre muitos outros exemplos (OECD, 2016).

Entretanto, não se nega que existem bons argumentos na defesa pela soberania digital, como questões importantes de segurança (a exemplo dos ciberataques contra a Estônia em 2007 ou intervenções em processos eleitorais), privacidade, estabilidade, otimização da infraestrutura e do fluxo de dados e impedimento da difusão de conteúdo ilegal (PINTO, 2018, CLAESSEN, 2020). Sublinha-se também as alegações contra espionagem digital estrangeira, como foi notoriamente exposta na denúncia de Snowden em 2013. A defesa da cibersoberania é marcada, legitimamente, por denúncias de colonialismo digital, que se estende por duas principais vias.

A primeira via expõe como por trás da retórica da Internet aberta e global existe uma influência determinante de alguns atores ocidentais nos rumos tomados por essa tecnologia, em particular dos governos dos EUA e da União Europeia (MUELLER, 2019, p. 9, SCHULTZ, 2008, p. 804). Os técnicos e políticos que criaram e foram responsáveis por todos os passos iniciais do ciberespaço eram geralmente norte-americanos ou europeus, e, mesmo que não intencionalmente, seus valores guiaram e estruturaram a arquitetura da rede (WU, 1997, p. 664). Denúncias sobre essa dominação tecnológica podem ser encontradas, para além de declarações de nações, em posicionamentos como o da população originária Māori da Nova Zelândia (WOLFGRAM, 2015).

Há momentos históricos que explicitam essas interferências governamentais diretas, como a subordinação contratual da ICANN (*Internet Corporation for Assigned Names and Numbers*), entidade responsável pela IANA (*Internet Assigned Numbers Authority*), ao Departamento de Comércio dos EUA até 2016 (SNYDER & KOMAITIS & ROBACHEVSKY, 2017, pp. 11-12). Ou, mais significativamente, a ameaça feita em 1998 pelo governo dos EUA contra o pioneiro da Internet Jon Postel, à época responsável pela função da IANA, para que revertesse uma importante mudança nos servidores que ele havia ordenado sem autorização governamental prévia (FROOMKIN, 2000, pp. 63-70). Um exemplo contemporâneo é a pressão feita pelo Procurador-

Geral (*Attorney General*) do estado da Califórnia sobre a ICANN, o que foi fundamental para impedir a venda do *Public Interest Registry* (PIR, entidade responsável por gerir o gTLD .org) pela ISOC para uma empresa com fins lucrativos, a Ethos Capital (ICANN, 2020).

A segunda via, que não deixa de estar ligada à primeira, lembra a influência das *Big Techs*, gigantescas empresas multinacionais de tecnologia (Google, Amazon, Facebook, Microsoft, Apple, dentre outros), cujas principais sedes estão em território norte-americano e europeu, sendo mais suscetíveis à pressão dos países onde se localizam (LAMBACH, 2019, pp. 5). Esses aglomerados empresariais têm um enorme peso econômico e capacidade de *lobby*. São agentes importantes na dinamização e expansão do acesso à Internet, mas muitas vezes atuam de forma quase monopolista no ciberespaço e têm uma influência internacional maior do que países inteiros (SASSEN, 1998; PINTO, 2018, pp. 15-21).

É difícil discordar que as reivindicações de soberania digital comumente servem para esconder casos de censura, perseguição política ou étnica, e infrações ao direito à privacidade (MUELLER, 2019; LEE & LIU, 2012; STADNIK, 2019). Existem muitos casos de governos autoritários instrumentalizando o controle do meio digital para objetivos que inclusive ofender direitos humanos consolidados. Mas essas posições, infelizmente, têm uma forte base discursiva, construída sob o argumento que os rumos da Internet global serem muito mais direcionados por certos países e setores, beneficiando e prejudicando de forma desigual os interesses envolvidos.

## **7. Considerações finais: prudência legislativa e maior abordagem multisetorial**

O primeiro passo de uma potencial solução desse conflito deve atacar a desigualdade na representação de interesses na Internet. Isso significa, como pontos mais urgentes, um comportamento auto restritivo dos países que notoriamente detêm maior poder sobre a Internet global, um empoderamento efetivo de instituições que representam interesses transnacionais (como ONGs e associações de defesa do direito do consumidor, ou seja, não apenas comerciais) e de mecanismos capazes de proporcionar soluções internacionais.

Novas normas imperativas com consequências globais devem ser construídos de forma a minimizar os impactos transfronteiriços. Caso eles sejam necessários, isso deve ser feito considerando que o ciberespaço é uma espécie de domínio comum (MUELLER, 2019, p. 19), reconhecendo os outros interesses nacionais envolvidos e buscando soluções consensuais, com diálogo e cooperação com outros Estados<sup>14</sup>.

---

<sup>14</sup> No entanto, cabe aqui a crítica que nesse caminho faria mais sentido atuar através de organizações internacionais e tratados multilaterais, e não com legislações nacionais/regionais com fortes efeitos extraterritoriais.

Essa moderação na criação de regulações ou outras medidas imperativas não é nada estranha ao ambiente cibernético (ver SCHULTZ, 2008, p. 839; WU, 1997, pp. 664-665). Para além de defesas mais radicais da auto regulação nos momentos iniciais, Internet colocou em evidência múltiplas instituições ou sistemas que surgiram e cresceram eficientemente de maneira mais ou menos independente da orientação por governos, a partir da cooperação e coordenação de agentes não-estatais, como a IETF (*Internet Engineering Task Force*), principal responsável pela padronização, aprimoramento e manutenção técnica da rede (MUELLER, 2019, p. 17).

No entanto, a limitação da atuação governamental na busca por soluções não pode ser feita de maneira acrítica, pelo risco já apontado por Lessig de simplesmente se trocar o controle pelo Estado por um controle pelo setor privado. Afinal, é necessário distinguir aquilo que pode ser chamado de um “espaço público” da Internet, que privilegia a comunicação entre pessoas e mesmo a ação política direta, do seu espaço comercial, com cada qual tendo sua função própria e princípios de funcionamento distintos (SASSEN, 1998).

Entendemos que a regulação da Internet por legislações nacionais é plenamente possível, mas seus variados riscos exigem, por cautela, que essas medidas se voltem para problemas domésticos e com aplicabilidade limitada ao território da nação. Quando necessário, os efeitos extraterritoriais dessas leis deveriam ser necessariamente discutidos pelo menos em espaços multilaterais, como a União Internacional de Comunicação da ONU. Preferencialmente, contudo, parece ser prioritário um aprofundamento de respostas multisetoriais bem-estruturadas.

Idealmente, esses processos necessitam de uma alteração fundamental, envolvendo um empoderamento da sociedade civil, inclusive como uma maneira mais legítima (do que a simples intervenção governamental) de dirimir o fortalecimento exacerbado do setor privado comercial. Tal inclusão deve ser feito evitando posições que assumam uma imagem romantizada e milagrosa do multisetorialismo. Essa visão, na prática, acabar apenas por legitimar espaços dominados pelos governos ou, especialmente, pelo setor privado. Sem uma estrutura planejada, a sociedade civil, inerentemente diversa e por isso comumente permeada por contradições, não consegue avançar uma agenda unificada e forte e assume uma participação meramente simbólica (MUSIANI, 2020).

É importante fixar funções, métodos organizativos e possibilidades de atuação de forma clara, delegando uma maior capacidade para tomar decisões à sociedade civil ou tomando medidas para que as recomendações e discussões desenvolvidas em espaços multisetoriais tenham maior influência sobre agentes reguladores. Em ambos os casos, isso exigiria maiores níveis de coordenação e coerência dentro da sociedade civil, o que parece implicar em filtros de participação de acordo com o comprometimento e conhecimento acumulado dos líderes. Isso, infelizmente, provavelmente tem como custo uma perda de diversidade e inclusão nos níveis mais altos, mas

pode ser contrabalanceado ao se preservar e garantir uma ampla participação nas “portas de entrada” desse sistema de filtros de representação.

Outra sugestão interessante é feita por William DUTTON, ao aceitar que o multilateralismo tende a crescer na forma de maiores atribuições das organizações intergovernamentais, mas que esse processo deve ser supervisionado por instituições multisetoriais (2016, pp. 44-48). Um exemplo prático seria a existência de um comitê no âmbito do IGF que acompanhasse e aconselhasse legisladores e tribunais na elaboração de medidas que afetassem o ciberespaço.

Nesse sentido, é interessante consultar um artigo publicado em 2020 por conhecidos especialistas da área de Governança da Internet, sugerindo um modelo para criação de um “Corpo Consultivo sobre Políticas da Internet” multisetorial em diferentes países (BELLI *et al*, 2020, p. 13-18). Apesar do modelo de CCPI exposto ser planejado para atuar a nível nacional, as orientações ali presentes podem ser adaptadas como base para pensar um modelo internacional.

Pode-se ainda perguntar como a participação da sociedade civil poderia ter efeitos contra Estados que defendem maior influência governamental. A resposta está justamente no enfraquecimento de parte expressiva da base argumentativa que defende maiores níveis de soberania digital, que encontram bons argumentos contra um “colonialismo digital” no cenário atual. Afinal, constata-se hoje a existência de uma multiplicidade de instituições ou processos que são formalmente multisetoriais sem o serem substancialmente/materialmente, existindo um acentuado desequilíbrio entre os diversos interesses do ecossistema cibernético (RAYMOND & DENARDIS, 2016; MUSIANI, 2020, p. 2-3; BELLI *et al*, 2020, p. 1-2).

Um exemplo recente nos ajuda a entender como isso funciona na prática. Há alguns anos, houve um aumento das declarações e atos de determinados governos pró-multilateralismo, sugerindo maiores competências para órgãos intergovernamentais. Isso acabou respondido, para diminuir a pressão, com uma antecipação do processo de transição da supervisão do sistema de nomes de domínio e da IANA, transferindo-a do governo dos EUA para a comunidade internacional multisetorial. (DRAKE & CERF & KLEINWÄCHTER, 2016, pp. 46-47).

Como um apontamento final, reiteramos que essas sugestões não afastam ideias legítimas de soberania digital. Conforme assinala LAMBACH, o sistema territorial de Estados sempre comportou mais ambiguidades e dinamicidade do que pareceria em uma primeira observação, podendo ser adaptado e modificado para servir também ao ciberespaço (2019), desde que tomados os cuidados acima apontados. A ideia de soberania digital é importante enquanto a Internet continue sendo significativamente usada como uma forma de dominação cultural ou econômica, ou como um instrumento de espionagem ou guerra, especialmente enquanto persistir um desequilíbrio de forças disfarçado sob vestes de participação ampla e democrática.

## Referências Bibliográficas

Adee, Sally. (22 julho 2019). *Entenda por que a Internet está se desintegrando*. Disponível em: <<https://www.bbc.com/portuguese/vert-fut-48849540>>

Almeida, D. F. (2018). The organizational structure of an international tribunal for the internet. *Revista Científica sobre Cyberlaw*, vol. V.

Ascensão, J. O. (2008). A sociedade digital e o consumidor. In M. Wachowicz & M. P. Santos (orgs.) *Anais do II Congresso de Direito de Autor e Interesse Público* (pp. 39–67). Florianópolis: Fundação Boiteux.

\_\_\_\_\_. (2005). Direito de Autor versus Desenvolvimento Tecnológico? In *Estudos em Memória do Professor Doutor António Marques dos Santos*, vol. I, Coimbra: Almedina, 787-795.

\_\_\_\_\_. (2012). Questões críticas do direito da internet. In WACHOWICZ, M. & PRONER, C. (orgs.) *Inclusão tecnológica e Direito à Cultura: movimentos rumo à sociedade democrática do conhecimento* (pp. 39-68). Florianópolis: FUNJAB.

Barlow, J. P. (1996). *A declaration of the independence of cyberspace*. 1996. Disponível em: <<http://www.dhnet.org.br/ciber/textos/barlow.html>>

Belli, L. (Fevereiro 12, 2020). *BRICS countries to build digital sovereignty*. Disponível em: <<https://www.medianama.com/2020/02/223-brics-countries-to-build-digital-sovereignty-luca-belli-cyberbrics/>>

Belli, L., Canabarro, D., Herzog, J., Hill, R., Afonso, C., (2020). Explorando a Governança Multissetorial Na Internet: Rumo à Identificação de Um Modelo de Órgão Consultivo de Políticas Da Internet. *PolITICs*, 30.

Biazatti, B. O. & Vilela, P. (2017) *Jurisdição e internet - Competência Internacional dos Tribunais Domésticos e Litígios de Internet*. Belo Horizonte: IRIS, 29 p.

Bomse, A. L. (2007). The Dependence of Cyberspace. *Duke Law Journal*, 50(6), 1717-1749.

Burk, D. L. (1997). Jurisdiction in a World Without Borders. *Virginia Journal of Law and Technology*, 1 (3).

Castells, M. (1999) *A Sociedade em Rede: A Era da Informação*, v. 1. São Paulo: Paz e Terra.

\_\_\_\_\_. (2014). *El impacto de internet en la sociedad: una perspectiva global*. Cambio, Open Mind, 24p. Disponível em: <<https://www.bbvaopenmind.com/wp-content/uploads/2014/03/BBVA-OpenMind-El-impacto-de-internet-en-la-sociedad-una-perspectiva-global-Manuel-Castells.pdf.pdf>>

Claessen, E. 2020. *Reshaping the Internet – the Impact of the Securitisation of Internet Infrastructure on Approaches to Internet Governance: The Case of Russia and the EU*. *Journal of Cyber Policy*, 5(1), 140–57.

Clinton, W. J. & Gore Jr., A. (1997). *A Framework for Global Electronic Commerce*. Disponível em: <<https://clintonwhitehouse4.archives.gov/WH/New/Commerce/>>.

CICP (Committee for Information, Computer and Communications Policy). (2011). *The role of internet intermediaries in advancing public policy objectives - Part II*, OECD.

Comissão Europeia. (2019). *The von der Leyen Commission: For a Union That Strives for More*. EC Press Release. Disponível em: [https://europa.eu/rapid/press-release\\_IP-19-5542\\_en.htm](https://europa.eu/rapid/press-release_IP-19-5542_en.htm)

Daigle, L. (2015). *On the Nature of the Internet*. [Global commission on Internet governance paper series, Paper No. 7, CIGI and Chatham House]. Disponível em: [https://www.cigionline.org/sites/default/files/gcig\\_paper\\_no7.pdf](https://www.cigionline.org/sites/default/files/gcig_paper_no7.pdf)

Demchak, C. & Dombrowsky, P. (2011). Rise of a Cybered, Westphalian Age. *Strategic Studies Quarterly*, 5(1), 31–62

Diedrich, F. (2000). A Law of the Internet? Attempts to Regulate Electronic Commerce. *The Journal of Information, Law and Technology*, 3.

Drake, W. J. (2017). *Framing Conversation: What Would Internet Fragmentation Mean for the Digital Economy?* [Working Paper, Columbia School of International and Public Affairs]. Disponível em: <[https://sipa.columbia.edu/sites/default/files/Drake\\_GDF\\_2017\\_FC1\\_final.pdf](https://sipa.columbia.edu/sites/default/files/Drake_GDF_2017_FC1_final.pdf)>

Drake, W., Cerf, V. & Kleinwächter, W. (2016). *Internet Fragmentation: An Overview*. Geneva: The World Economic Forum.

Dutton, W. H. (2016). *Multistakeholder Internet Governance?* [Background Paper for the World Development Report, Digital Dividends]. Disponível em: <<http://pubdocs.worldbank.org/en/591571452529901419/WDR16-BP-Multistakeholder-Dutton.pdf>>

Easterbrook, F. H. (1996). Cyberspace and the Law of the Horse. *University of Chicago Legal Forum*, 207, 207–216.

ECHR Research Division. (2015). *Internet: case-law of the European Court of Human Rights*. Disponível em: <[https://www.echr.coe.int/Documents/Research\\_report\\_internet\\_ENG.pdf](https://www.echr.coe.int/Documents/Research_report_internet_ENG.pdf)>.

Federal Networking Council. (2005). *Federal Networking Council Resolution: Definition of 'internet'*. Disponível em: <[https://www.nitrd.gov/fnc/internet\\_res.pdf](https://www.nitrd.gov/fnc/internet_res.pdf)>

Franzese, P. W. (2009). Sovereignty in Cyberspace: Can It Exist? *Airforce Law Review*, 64, 1–42.

Froomkin, A. M. (2000). Wrong Turn in Cyberspace: Using ICANN to Route Around the APA and the Constitution. *Duke Law Journal*, 50, 17-186.

Gautrais, V., Lefebvre, G. & Benyekhlef, K. (1997). Droit du commerce électronique et normes applicables: l'émergence de la lex electronica. *International Business Law Journal*, 5, 547-579.

Goldsmith, J. L. (1998). Against Cyberanarchy. *University of Chicago Law Review*, 65(4), 1199-1250.

Gregorio, G. (2018). Expressions on Platforms: Freedom of Expression and ISP Liability in the European Digital Single Market. *European Competition and Regulatory Law Review*, 2(1), 203-215.

ICANN Board (Abril 30 2020). ICANN Board Withholds Consent for a Change of Control of the Public Interest Registry. Disponível em: <<https://www.icann.org/news/blog/icann-board-withholds-consent-for-a-change-of-control-of-the-public-interest-registry>>

Internet Society. (2012). *Internet Invariants: What really matters*. Disponível em: <<https://www.Internetsociety.org/Internet-invariants-what-really-matters/>>

Johnson, D. R. & Post, D. G. (1996). Law and Borders - The Rise of Law in Cyberspace. *Stanford Law Review*, 48, 1367-1402.

Kowalik-Bańczyk, K. & Pollicino, O. (2016). Migration of European Judicial Ideas Concerning Jurisdiction Over Google on Withdrawal of Information. *German Law Journal*, 17(3), 315–337.

Kuner, C. (2017). *The Internet and the Global Reach of EU Law*. [LSE Legal Studies Working Papers, n. 4/2017], 37p.

Lambach, D. (2019). The Territorialization of Cyberspace. *International Studies Review*, 0, 1–25.

Lee, J-A. & Liu, C-Y. (2012). Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. *Minnesota Journal of Law, Science, and Technology*, 13(1).

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, 39(5), 22–31.

Lessig, L. (1999). The law of the horse: what cyberlaw might teach. *Harvard Law Review*, 113, 501–546.

\_\_\_\_\_. (2006). *Code: version 2.0*. New York: Basic Books.

Lugaresi, N. (2017). Internet Law Trends in Europe: a case law perspective. *Revista da Faculdade de Direito da UFMG*, v. Especial, n. 2nd Conference Brazil-Italy, 305–334

Mchangama, J. & Fiss, J. (2019). The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship. Copenhagen, Justitia. Disponível em: <[http://justitia-int.org/wp-content/uploads/2019/11/Analyse\\_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf](http://justitia-int.org/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf)>

Mueller, M. L. (2019). Against Sovereignty in Cyberspace. *International Studies Review*, 0, 1–23.

Musiani, F. (2020). Multissetorialismo: Ultrapassando o Status de ‘Remédio Milagroso’? *PoliTICs*, 30.

Noam, E. M. (2013). Towards a Federated Internet. *InterMEDIA*, 41(4).

OECD. (2016). *Economic and social benefits of Internet openness*. [OECD Digital Economy Papers, n. 257]. Disponível em: <https://www.oecd-ilibrary.org/docserver/5jlwqf2r97g5->

[en.pdf?expires=1577217455&id=id&accname=guest&checksum=5BEF017A69CEE211C71E56936612B7AD](https://www.cigionline.org/publications/multi-stakeholderism-anatomy-inchoate-global-institution)

Pereira, A. D. (2001). A jurisdição na internet segundo o regulamento 44/2001 (e as alternativas extrajudiciais e tecnológicas). *Boletim de Faculdade de Direito*, LXXVII, 633–687.

Pinto, R. A. (2018). Digital Sovereignty or Digital Colonialism. *Sur - International Journal on Human Rights*, 27, 15-28.

Polido, F., Machado, D., Anjos, L., Araújo, D. & Brandão, L. (2018). *GDPR e suas repercussões no direito brasileiro: primeiras impressões e análise comparativa*. Belo Horizonte, IRIS, 39p.

Post, D. G. (2002). Against ‘Against Cyberanarchy’. *Berkeley Technology Law Journal*, v. 17, 1365–1387.

Ramos, R. M. M. (2016). *Estudos de direito internacional privado da União Europeia*. Coimbra: Imprensa da UC.

Raymond, M & Denardis, L. (2016). *Multi-stakeholderism: Anatomy of an Inchoate Global Institution*. [Global Commission on IG Paper Series: no. 41, CIGI & Chatam House]. Disponível em: <<https://www.cigionline.org/publications/multi-stakeholderism-anatomy-inchoate-global-institution>>

Schultz, T. (2008). Carving up the Internet: Jurisdiction, legal orders, and the Private/ Public International Law Interface. *European Journal of International Law*, 19(4), 799–839.

Snyder, J., Komaitis, K. & Robachevsky, A. (2017). *The History of IANA: An Extended Timeline with Citations and Commentary*, Internet Society. Disponível em: <[https://www.Internetsociety.org/wp-content/uploads/2016/05/IANA\\_Timeline\\_20170117.pdf](https://www.Internetsociety.org/wp-content/uploads/2016/05/IANA_Timeline_20170117.pdf)>

Solum, L. B. (2009). Models of Internet Governance. In *Internet Governance* (pp. 48-91). Oxford: Oxford University Press.

Stadnik, I. (2019). *Sovereign RUnet: What Does it Mean?* [Internet Governance Project, Georgia Institute of Technology].

Svantesson, D. J. B. (2018). European Union Claims of Jurisdiction over the Internet. *Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, v. 1, 113–125.

\_\_\_\_\_. (2016). *Private international law and the Internet*, 3 ed. Netherlands: Kluwer Law International.

Vicente, D. M. (2005). *Problemática Internacional da Sociedade da Informação*. Coimbra: Almedina.

Vlavo, F. (2013). The Digital Hysterias of Decentralisation, Entrepreneurship and Open Community. *Transformations*, 23.

Wolfgram, T. (2015). *[Re]Claiming our Technological Sovereignty through co-creating the Māori Innovation, New Technology & ICT Sector*. [Position Paper, PlanetMaori]. Disponível em:

[http://planetmaori.com/Files/Content/2015/Re-Claiming\\_our\\_Technological\\_Sovereignty - Paper - Tania Wolfgramm 2014.pdf](http://planetmaori.com/Files/Content/2015/Re-Claiming_our_Technological_Sovereignty_-_Paper_-_Tania_Wolfgramm_2014.pdf)

Wu, T. S. (1997). Cyberspace Sovereignty? - The Internet and the International System. *Harvard Journal of Law & Technology*, 10(3), 647–666.