

QUEM DEVE REGULAR A INTERNET?

WHO SHOULD REGULATE THE INTERNET?

Pedro Henrique de Moura Gonet Branco¹

Resumo: A regulação da internet é tarefa complexa, que envolve muitos atores no cenário internacional. É difícil o estabelecimento de bases comuns entre os países que se propõem a regular o ciberespaço. Essa atividade se tornará praticamente impossível se cada país estiver dividido internamente. Por esse motivo, os Estados soberanos devem adotar posições únicas no cenário global para que não se inviabilize a existência do mundo virtual.

Palavras-chave: Regulação da Internet; Soberania; Direito Internacional; Direito Constitucional; Repartição de Competências.

Abstract: The regulation of the internet is a complex task that involves many actors on the international scene. It is difficult to establish common bases between all the countries that tries to regulate the cyberspace. This activity will be practically impossible if each country gets internally divided. That is why sovereign States must adopt unique positions in the global scenario, so that the existence of the virtual world does not become unfeasible.

Keywords: Regulation of the Internet; Sovereignty; International Law; Constitutional Law; Division of Legislative Competences.

Sumário: Introdução. 1. Regulação do ciberespaço. 2. Ciberlibertarismo. 3. Bem público global. 4. Ciberpaternalismo. 5. Pathetic dot theory. 6. Competência para influenciar o código. 7. O papel da União na gestão da internet no Brasil. 8. A atuação do STF no assunto. Conclusão.

INTRODUÇÃO

O desenvolvimento tecnológico nos séculos XX e XXI promoveu, na concepção de Murray², a transição de um mundo de átomos para um mundo de *bits*. Esse processo começou na

¹ Graduando em Direito pela Universidade de Brasília (UnB), *visiting student* na University of California Berkeley, editor-chefe da Revista dos Estudantes de Direito da Universidade de Brasília (RED|UnB) e autor dos trabalhos *O Ensino Religioso Confessional e a Laicidade Estatal à luz da ADI 4.439, Las 100 Reglas de Brasilia y el acceso a la justicia en Brasil* e *Structural ways of governing the Internet – the Brazilian position*.

² MURRAY, 2016.

década de 1970 e representa a transformação de uma sociedade industrial em uma sociedade conectada (*network society*).

Manuel Castells, um dos principais teóricos dessa nova forma de organização social, define sociedade como uma estrutura social contraditória, baseada em conflitos e negociações entre diferentes atores político-sociais, em contraste com comunidades, que partilham valores e interesses³. Ressalta que sociedades sempre tiveram fronteiras bem delimitadas, mesmo com o processo de globalização do século XX, pois sua formação espaço-temporal era restrita, em grande medida, a uma estrutura nacional. O que alterou esse quadro e permitiu o surgimento da sociedade conectada foi o que ele chamou de *network*, uma “complexa estrutura de comunicação [...] que garante unidade de propósitos e flexibilidade de execução dada sua adaptabilidade ao ambiente operacional”⁴.

Assim, a sociedade conectada – uma sociedade global – “é uma estrutura dinâmica altamente suscetível a forças sociais, a cultura, a política e a estratégias econômicas”⁵. O fato de ser uma sociedade global, entretanto, “não significa que pessoas de todos os lugares estejam incluídas nas *networks*. [...] A estrutura social é global, mas a maior parte da experiência é local, tanto territorial quanto culturalmente”⁶. Da mesma forma, ao contrário do que pode parecer à primeira vista, “a tecnologia não determina a sociedade. A sociedade molda a tecnologia de acordo com suas necessidades, seus valores e os interesses das pessoas que utilizam a tecnologia”⁷. Essa tese é corroborada com a ideia de que os governos devem influenciar a arquitetura da internet, como veremos adiante.

1. REGULAÇÃO DO CIBERESPAÇO

É, portanto, no contexto da sociedade global conectada que surgem as discussões mais interessantes a respeito do ciberespaço (*cyberspace*), onde está a internet. Nas palavras de Mueller, “o ciberespaço é um espaço virtual [isto é, definido por software] de interação”⁸. Muito se discutiu

³ CASTELLS, 2013, p. 14.

⁴ CASTELLS, 2013, p. 21. Tradução minha.

⁵ CASTELLS, 2013, p. 26. Tradução minha.

⁶ CASTELLS, 2013, p. 25. Tradução minha.

⁷ CASTELLS; CARDOSO, 2005, p. 3. Tradução minha.

⁸ MUELLER, 2019, p. 10.

a respeito da natureza jurídica do ciberespaço e das formas de se justificar a intervenção – ou ausência de intervenção – no mundo virtual.

Há autores que sustentam ser um ambiente que não pode ser regulado – os adeptos do ciberlibertarianismo –, completamente distinto do mundo real, onde as leis e os governos não teriam legitimidade⁹. Há outros que defendem que princípios do Direito Internacional deveriam guiar as relações *online*, tratando o ambiente como bem público global. Há, ainda, os que sustentam a necessidade de regulação do ciberespaço – os adeptos do ciberpaternalismo –, tanto enquanto um espaço à parte, quanto como extensão da soberania nacional¹⁰.

2. CIBERLIBERTARISMO

O principal teórico da doutrina do ciberlibertarismo é John Perry Barlow, que escreveu em 1996 a Declaração da Independência do Ciberespaço. Sua teoria baseava-se na falta de legitimidade de governos e leis do mundo real para interferir no espaço em tese soberano e separado do espaço real. Afirmava que o ciberespaço é um lugar onde é preciso cruzar uma fronteira virtual para entrar e, portanto, os internautas estariam além do mundo real.

Barlow argumenta que apenas com o consentimento dos cidadãos do ciberespaço um sistema regulatório prosperaria. Ele acreditava que seria possível ingressar nesse novo mundo virtual da mesma forma que alguém pega um avião para entrar em outro país. Este novo “país” proposto seria um “mundo onde qualquer um, em qualquer lugar, pode expressar suas crenças, por mais singulares que sejam, sem medo de ser coagido ao silêncio ou à conformidade”.¹¹

Não é difícil perceber quão utópica é essa perspectiva. Não existe uma nítida divisória entre o mundo real e o virtual. Sempre que alguém está no ciberespaço está também em, no mínimo, um ambiente físico. As relações sociais sempre se iniciam e terminam fora do ciberespaço – no caso extremo, perpassa o cérebro da pessoa que interage, que está no mundo real. Por isso, escapa ao bom senso a tese de que é possível sair do mundo real e ingressar no ciberespaço, como se ele fosse

⁹ BARLOW, 1996.

¹⁰ Vide SCHMITT; VIHUL, 2016; e REIDENBERG, 1996.

¹¹ BARLOW, 2001. Tradução minha.

um local à parte. Também não prospera a ideia de que seria possível estar em um lugar do ciberespaço com um equivalente exato no mundo físico.

Um pequeno comerciante francês, por exemplo, que acessa do seu território nacional um *website* hospedado no Reino Unido, de uma empresa norte-americana de distribuição de produtos, que vende produtos também no Brasil, estará em alguma medida subordinado às determinações legais da França, do Reino Unido, dos Estados Unidos e do Brasil. Percebe-se, portanto, que o indivíduo estará sempre em diferentes lugares e sujeito à incidência de diferentes sistemas normativos.

3. BEM PÚBLICO GLOBAL

Há quem defenda, por isso, que ciberespaço deve ser tratado como um bem público global (*global common*), como o oceano, o espaço sideral, a Antártica¹². Para os adeptos dessa linha:

[...] os estados não podem afirmar sua soberania sobre o ciberespaço. Eles só podem regular a maneira como as pessoas (ou coisas) sujeitas à sua autoridade acessam o ciberespaço global. Não existe um ciberespaço nacional sobre o qual eles exercem controle supremo; em vez disso, existe um ciberespaço global compartilhado e eles aproveitam sua soberania sobre atores e dispositivos físicos em seu território para restringir, de maneira imperfeita e limitada, as conexões com determinados sites ou aplicativos. As autoridades territoriais simplesmente não estão no controle de quem entra no ciberespaço fora do seu território ou dos serviços ou aplicativos que os atores externos fornecem sobre ele. Eles só podem identificar e bloquear as coisas após o fato. Essas limitações não conferem soberania aos estados sobre o ciberespaço, assim como o licenciamento de navios de um país e a aprovação de sua entrada e saída de seus portos não lhes confere soberania sobre o oceano, tampouco o faz a posse de satélites e instalações de lançamento de um Estado no o espaço sideral. A situação se assemelha muito ao regime de governança oceânica, onde os estados têm propensão a territorializar ou estabelecer jurisdição sobre o máximo de território possível, mas o alto mar ainda é reconhecido como um espaço não-soberano e existem importantes limitações à soberania, mesmo nas zonas territorializadas.¹³

Apesar de engenhosa a solução de tratar o ciberespaço como um bem público global, o *locus* digital se distingue dos bens que de fato se enquadram nessa categoria por depender de

¹² BETZ; STEVENS, 2011.

¹³ MUELLER, 2019. Tradução minha.

infraestrutura que, necessariamente, existe em determinada localização geográfica e pertence a alguma entidade, que realiza sua operação e manutenção¹⁴.

Parece mais razoável, portanto, compreender o ciberespaço não como um bem público global, mas como um ambiente artificial – criado pelo ser humano e passível de modificação por ele – que perpassa várias soberanias ao mesmo tempo e precisa de um tratamento diferenciado para salvaguardar a soberania dos Estados que entram em contato com esse ambiente digital.

Nessa vertente, é interessante a aplicação das determinações do Manual de Tallinn, um documento elaborado em 2013 por acadêmicos e profissionais das áreas do Direito Internacional e da cibersegurança. Esses especialistas, nacionais de países-membros da Organização do Tratado do Atlântico Norte (OTAN), reuniram-se em Tallinn, na Estônia, para elaborar diretrizes relacionadas a operações cibernéticas que se enquadrariam como ataques armados. A primeira versão do Manual tratava principalmente sobre as regras de reação a equivalentes a ataques armados, como a legítima defesa, um paralelo ao artigo 51 da Carta das Nações Unidas.

Em 2017, uma extensão do estudo foi publicada para compreender também circunstâncias que não se enquadram nas duas hipóteses analisadas na primeira edição do documento (*jus ad bellum*¹⁵ e *jus in bello*¹⁶). O chamado Manual de Tallinn 2.0 foi assinado por dezenove especialistas em Direito Internacional, com a pretensão de analisar legalmente os incidentes cibernéticos mais comuns que os Estados encontram no cotidiano, em períodos de paz. Apesar de não ser um documento oficial, o Manual foi elaborado por especialistas em Direito Internacional e em operações cibernéticas e militares sob a supervisão de mais de cinquenta Estados e organizações internacionais, o que reforça sua relevância para o Direito.¹⁷

Dividido em vinte capítulos, o Manual de Tallinn dedica suas primeiras cinco regras à soberania. Os especialistas concordaram que “os Estados gozam de soberania sobre qualquer infraestrutura cibernética localizada em seu território e sobre as atividades associadas a essa infraestrutura”¹⁸. Analisou-se a hipótese de compreender o ciberespaço como bem público global, mas descartou-se essa possibilidade, pois todas as ações realizadas no espaço virtual “são tomadas por indivíduos ou entidades sujeitos à jurisdição de um ou mais Estados”¹⁹. Também por isso os

¹⁴ BARCOMB et al., 2012.

¹⁵ Direito que regula o uso da força pelos Estados.

¹⁶ Direito que regula a condução de operações militares em períodos de guerra.

¹⁷ SCHMITT, 2017, p. 2-6.

¹⁸ SCHMITT, 2017, p. 11. Tradução minha.

¹⁹ SCHMITT, 2017, p. 12. Tradução minha.

Estados não podem reivindicar soberania sobre o ciberespaço, dado que a infraestrutura que permite a sua existência está, via de regra, localizada no território soberano de outros Estados²⁰.

Os autores do Manual foram claros, portanto, em fazer a distinção entre o espaço virtual e a estrutura que permite a existência desse espaço. Os servidores físicos, por exemplo, que são condição para a criação do ciberespaço, são diferentes do espaço virtual em si. É sobre essa estrutura que os Estados podem reivindicar soberania, não sobre o ciberespaço.

4. CIBERPATERNALISMO.

O chamado ciberpaternalismo, por sua vez, afirma que o ciberespaço não é resistente aos reguladores do mundo real. Joel Reidenberg foi um dos primeiros estudiosos a endossar essa ideia. Ele trouxe do século XI a ideia da *Lex Mercatoria*, código originado nas atividades dos comerciantes que precisavam regular seus negócios independentemente de sua localização. Uma vez que a lei podia variar em questões substanciais entre os locais onde costumavam fazer comércio, esses comerciantes começaram a resolver seus problemas com base nos costumes mercantis. A codificação que resultou dessa desse compilado de normas foi capaz de dar segurança à atividade econômica dos comerciantes, independentemente da jurisdição a que estivessem submetidos.

A ideia de Reidenberg era adaptar a ideia posta em prática pelos comerciantes do século XI para a realidade dos usuários da Internet. Buscava, assim, garantir segurança jurídica aos cidadãos online que, como visto, podem estar sob diferentes e numerosas jurisdições ao mesmo tempo. Defendia, igualmente, a noção de que uma lei feita pelo governo não é a única fonte de regulamentação, mas que “as capacidades tecnológicas e as opções de design do sistema impõem regras aos participantes”. Esse conjunto de regras forma o que ele chamou de *Lex Informatica*.

5. PATHETIC DOT THEORY

O conceito criado por Reidenberg está intimamente ligado ao apresentado por Lawrence Lessig, a *Pathetic Dot Theory*, ou Teoria do Ponto Patético. Lessig defende que os indivíduos são controlados por quatro forças que atuam em conjunto para regular suas vidas. São elas a Lei

²⁰ SCHMITT, 2017, p. 12.

(mecanismo tradicional que tem o Estado para exercer seu poder de coerção, pela ameaça de punição), as Normas Sociais (padrões de conduta esperados pelos indivíduos), o Mercado (influência que preços e outros elementos econômicos têm no comportamento dos cidadãos) e a Arquitetura (o *design* de um sistema, limites impostos pelo modo como algo foi criado)²¹.

A tese de Lessig é que essas restrições regulam as interações do mundo real e virtual. A venda de bebida alcoólica é um exemplo de atividade do mundo real regulada pelas quatro modalidades. No Brasil, a lei determina que é preciso ter mais de dezoito anos para comprar álcool. Esse requisito legal é uma restrição imposta pela lei para os indivíduos que ainda não somam dezoito anos de idade e que poderiam pretender beber. As normas sociais também atuam como uma restrição à relação entre indivíduos e bebidas alcoólicas. Essas normas preceituam, por exemplo, que não se deve beber de manhã cedo nem excessivamente. Aqueles que quebram essas expectativas sociais sofrem sanções, da crítica ao ostracismo. O mercado também interfere no uso do álcool, como quando estabelece preços que controlam a quantidade de bebidas que se pode comprar e, portanto, consumir. Finalmente, a arquitetura da bebida alcoólica inibe as pessoas de beber sem restrições. Após o consumo de determinada quantidade de álcool, o corpo reage de modo que se torna desconfortável continuar a ingerir bebidas alcoólicas.

A regulamentação do consumo de álcool, portanto, é determinada por esses quatro aspectos limitantes da vida - leis, normas, mercado e arquitetura. Eles interagem entre si e a soma de suas atividades tudo regula. É interessante observar como cada um desses quatro elementos prevaleceu em períodos específicos dos últimos três séculos. Lessig sugere que no século XIX as principais restrições da vida social eram impostas pelas normas sociais; no início do século XX, as leis eram preeminentes na orientação das ações humanas; em meados do século XX, o mercado era o grande regulador; e o século XXI estaria experimentando a prevalência da arquitetura como o mais importante moderador de comportamento.

Lessig argumenta que esses quatro padrões de regulação são observados, também, no ciberespaço. Ressalta que, dadas as peculiaridades do mundo virtual, as leis ali não são o elemento limitador mais importante. A arquitetura da Internet é o principal fenômeno que estabelece limites para atividades e escolhas.

²¹ LESSIG, 2006.

Explicando o elemento da arquitetura, Lessig destaca que, assim como tijolos e cimento modelam um edifício – funcionando como sua arquitetura –, um conjunto de códigos, presente em hardwares e softwares, é responsável pela estrutura do ciberespaço – a plataforma. “O software e o hardware, que tornam o ciberespaço o que ele é, constituem um conjunto de restrições sobre como o indivíduo pode se comportar. [...] Eles restringem determinados comportamentos, tornando outros comportamentos possíveis ou impossíveis”²².

Ele prossegue mencionando que o código “incorpora certos princípios; define os termos em que se utiliza o espaço; define o que é possível nesse espaço virtual. E esses termos e possibilidades afetam a inovação no espaço. Algumas arquiteturas convidam à inovação; outras inibem.”²³ É por isso que Lessig defende que o código é a restrição mais importante quando se trata de regulação da Internet.

O professor norte-americano argumenta que as pessoas obedecem a essas leis em forma de código não porque querem, mas porque não se pode fazer mais nada. Não há escolha possível entre ceder ou não à demanda feita pelo sistema para nele ingressar: se o usuário se negar a cumprir com o que determina o código, simplesmente não participará do ambiente virtual. Dessa suposição vem a famosa afirmação de Lessig de que o código é a lei (*code is law*), o que significa que o código é a principal entidade que controla o comportamento online.

6. COMPETÊNCIA PARA INFLUENCIAR O CÓDIGO

A grande dificuldade surge no momento de identificar quem tem competência para tentar exercer influência sobre o Código. Ao mesmo tempo que não se pode prescindir da regulação da internet, um espaço excessivamente regulado prejudicaria o desenvolvimento do mundo digital.

O Reino Unido tem interessantes leis de regulação da internet que se destinam a influenciar o Código, com o objetivo de coibir, em seu território, alguns crimes que consideram graves. Exige-se, por exemplo, que os Provedores de Serviços de Internet (*ISP*) “adotem medidas técnicas para evitar que seus clientes acessem sites que contenham imagens ilegais de abuso infantil”. A identificação desses sites é feita em parceria com a *Internet Watch Foundation (IWF)*. Influencia-

²² LESSIG, 2006, p. 124

²³ Palestra ministrada no pcForum, em 2000, nos Estados Unidos.

se a Arquitetura porque se o *ISP* bloquear o acesso a um site o usuário final não poderá ver o conteúdo ilegal. É por isso que Lessig diz que obedecer à lei como um código não é *uma* opção, mas é a *única* opção.

Também nos Estados Unidos há exemplos de regulação do ciberespaço que influenciam o Código. O *website* do Canadá iCraveTV transmitia ao vivo pela internet canais de televisão canadenses e norte-americanos. Nada obstante a intenção de permitir o acesso ao *website* apenas aos clientes que habitassem no Canadá, era fácil burlar o sistema de bloqueio geográfico, dando margem a que usuários estadunidenses assistissem aos canais disponíveis. Apesar de estar de acordo com a legislação canadense, grandes produtoras americanas questionaram a legalidade da plataforma nos EUA. Um tribunal da Pensilvânia, nos Estados Unidos, que julgou o pedido dessas produtoras, exigiu que a empresa canadense removesse o sistema de transmissão do seu *website* ou bloqueasse efetivamente o acesso ao portal no território norte-americano. O iCraveTV acabou encerrando suas operações.

Da mesma forma que o Reino Unido e os Estados Unidos, a grande maioria dos países adota medidas para preservar valores caros ao seu ordenamento por meio da regulação do ciberespaço. Também no Brasil existe essa preocupação.

É possível encontrar no sistema regulatório brasileiro eco da tese de Lessig, segundo a qual leis, mercado e normas sociais atuam para moldar o código – a arquitetura. Em outras palavras, o legislador brasileiro consegue, em alguma medida, valer-se desses elementos para estimular um comportamento online considerado desejável.

7. PAPEL DA UNIÃO NA GESTÃO DA INTERNET NO BRASIL

No ordenamento jurídico brasileiro, há legislações editadas em nível federal que dispõem sobre a regulação da internet. Destacam-se o Marco Civil da Internet (Lei n. 12.965, de 23 de abril de 2014), diploma legal que “estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria”, conforme o art. 1º da referida Lei; e a Lei Geral de Proteção de Dados Pessoais (Lei n. 13.709, de 14 de agosto de 2018), que regula o tratamento de dados pessoais, tema intimamente ligado à internet.

Ambas as legislações fazem referência à figura do Comitê Gestor da Internet no Brasil (GCI.br). O Comitê foi criado pela Portaria Interministerial n. 147, de 31 de maio de 1995, para “coordenar e integrar todas as iniciativas de serviços Internet no país”, “com o objetivo de assegurar qualidade e eficiência dos serviços ofertados, a justa e livre competição entre provedores, e a manutenção de padrões de conduta de usuários e provedores”, como se apreende do preâmbulo da referida Portaria.

Entre as atribuições do GCI.br, estão, conforme art. 1º da Portaria Interministerial n. 147/1995:

- “I - acompanhar a disponibilização de serviços Internet no país;
- II - estabelecer recomendações relativas a: estratégia de implantação e interconexão de redes, análise e seleção de opções tecnológicas, e papéis funcionais de empresas, instituições de educação, pesquisa e desenvolvimento (IEPD);
- III - emitir parecer sobre a aplicabilidade de tarifa especial de telecomunicações nos circuitos por linha dedicada, solicitados por IEPDs qualificados;
- IV - recomendar padrões, procedimentos técnicos e operacionais e código de ética de uso, para todos os serviços Internet no Brasil;
- V - coordenar a atribuição de endereços IP (Internet Protocol) e o registro de nomes de domínios;
- VI - recomendar procedimentos operacionais de gerência de redes;
- VII - coletar, organizar e disseminar informações sobre o serviço Internet no Brasil; e
- VIII - deliberar sobre quaisquer questões a ele encaminhadas.”

O Comitê conta com representantes governamentais – de Ministérios, de Agências Reguladoras e de Conselhos relacionados ao tema –, empresariais, acadêmicos, técnicos e do terceiro setor. Não se configura como órgão de governo e não goza de poder normativo, mas deve, por previsão legal, ser consultado em assuntos que envolvam a neutralidade de rede e a adequada prestação de serviços e aplicações.

O Comitê, criado por iniciativa da União, foi objeto de análise pelo Tribunal de Contas da União (TCU), no Acórdão n 1.164/2012, de 16 de maio de 2012, relator o Ministro Raimundo Carreiro. No julgamento, ficou assentado que “não há como enquadrar os serviços de administração da Internet como serviços públicos, porquanto inexistente lei que assim os declare e confira suas titularidades ao Estado, em particular à União”²⁴.

²⁴ BRASIL, 2012.

Pode parecer, à primeira vista, que o TCU afastou da União a competência para regular a internet. Nada obstante essa possível interpretação, o Tribunal reconheceu que

o Comitê relaciona-se com a administração pública, como também com entidades privadas, estando em total compasso com a melhor prática internacionalmente aceita para a administração da Internet em diversos países, os quais têm tido a **participação da sociedade civil e do governo por intermédio de um comitê que represente de forma ampla toda a sociedade**. Ou seja, **o modelo que é adotado no Brasil segue a tendência mundial de boa governança no que concerne à administração da Internet**. (Grifos acrescidos)²⁵

Assim, se é necessária a representação de ampla parcela da sociedade na governança da internet, parece fazer sentido que à União compita o dever de legislar sobre o assunto, não aos Estados, aos Municípios ou ao Distrito Federal.

Como leciona Fernanda Dias de Almeida, “a preponderância da União no federalismo contemporâneo é um dado com que se tem de aprender a conviver”, reconhecendo-se que o sistema federativo “é o melhor para o Brasil, considerada sua vocação nata para equilibrar a diversidade na unidade, o que – como já se afirmou – é particularmente adequado a um país como o nosso, com grandes disparidades de toda ordem”²⁶.

Nada obstante, já há na realidade brasileira episódios de Estados-membros que tentam influenciar a Arquitetura da internet. O Estado de Pernambuco, por exemplo, que ganhou notoriedade por ser a primeira unidade da federação a instituir um Código Estadual de Defesa do Consumidor (Lei estadual n. 16.559, de 15 de janeiro de 2019), criou determinações para os comerciantes que desempenhavam suas atividades no ciberespaço:

Art. 42. O fornecedor é obrigado a informar em sua loja virtual:

I - a disponibilidade do produto em estoque para envio imediato; e,

II - o preço do produto de forma legível e ostensiva, sendo vedada a utilização de canais privados ou não acessíveis a outros consumidores para a divulgação do seu valor.

§ 1º Entende-se como produto em estoque para envio imediato aquele disponível na central de distribuição do próprio fornecedor, no momento em que consultado pelo consumidor.

§ 2º Não estando o produto disponível em estoque para envio imediato, tal circunstância deverá ser informada, sendo vedado ao fornecedor entregar produto diverso, salvo se permitido pelo consumidor.

²⁵ BRASIL, 2012.

²⁶ ALMEIDA, 2014.

§ 3º Em qualquer caso, a informação de que trata o caput deverá anteceder o momento do pagamento, independentemente da forma pela qual este seja realizado, ainda que por meio de boleto bancário.

§ 4º O descumprimento ao disposto no caput sujeitará o infrator à penalidade de multa prevista no art. 180, nas Faixas Pecuniárias B ou C, sem prejuízo da aplicação cumulativa de outras sanções previstas neste Código.

Imagine-se, no entanto, uma empresa multinacional que venda produtos pela internet para os mais diferentes países do globo. Ela seria obrigada a adicionar elementos ao seu *website* internacional para cumprir com as determinações do Estado de Pernambuco.

A situação seria ainda mais complexa se, além do Estado de Pernambuco, cada um dos Estados-membros da Federação decidisse obrigar os fornecedores que entregam produtos em seus territórios a expor determinada informação na página virtual de suas lojas.

Os pontos já levantados sobre a busca por um ciberespaço global, com pequenos ajustes para adaptar a internet aos valores inscritos nos ordenamentos jurídicos dos países soberanos, são suficientes para compreender que não se deve permitir uma descentralização da regulação do ciberespaço entre as unidades da federação.

8. ANÁLISE DO ASSUNTO PELO SUPREMO TRIBUNAL FEDERAL

A lei pernambucana foi objeto da Ação Direta de Inconstitucionalidade (ADI) n. 6.214²⁷, apreciada pelo Supremo Tribunal Federal. Os autores da ação questionavam uma série de dispositivos da legislação estadual, entre os quais o referido art. 42.

O redator para o Acórdão, Ministro Alexandre de Moraes, não analisou o fato de um Estado-membro tentar influenciar a arquitetura da internet. Limitou-se a identificar no dispositivo impugnado determinações semelhantes às existentes em lei federal, encontrando, na atuação do Estado de Pernambuco, legislação restrita à defesa dos direitos do consumidor, matéria de competência concorrente:

embora os arts. 40, 41 e 42 do Código estadual de Defesa do Consumidor disciplinem acerca de obrigações relativas à loja virtual dos fornecedores, apenas dispõe acerca de informações importantes ao consumidor que devem constar no espaço virtual, a fim de instruí-lo adequadamente sobre as especificações necessárias do produto ou serviço antes de o adquirir.

²⁷ No momento do fechamento deste artigo, 8 de junho de 2021, a ADI 6.214 está com embargos de declaração pendentes de julgamento e, portanto, a decisão ora analisada ainda não foi estabilizada pelo trânsito em julgado.

Notadamente em relação aos arts. 40, 41 e 42, cumpre ainda registrar que as normas contestadas estão em total consonância com a regulamentação federal sobre o tema (Decreto 7.962/2013), que assim dispõe:

Art. 2º Os sítios eletrônicos ou demais meios eletrônicos utilizados para oferta ou conclusão de contrato de consumo devem disponibilizar, em local de destaque e de fácil visualização, as seguintes informações:

I - nome empresarial e número de inscrição do fornecedor, quando houver, no Cadastro Nacional de Pessoas Físicas ou no Cadastro Nacional de Pessoas Jurídicas do Ministério da Fazenda;

II - endereço físico e eletrônico, e demais informações necessárias para sua localização e contato;

III - características essenciais do produto ou do serviço, incluídos os riscos à saúde e à segurança dos consumidores;

IV - discriminação, no preço, de quaisquer despesas adicionais ou acessórias, tais como as de entrega ou seguros;

V - condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e

V - condições integrais da oferta, incluídas modalidades de pagamento, disponibilidade, forma e prazo da execução do serviço ou da entrega ou disponibilização do produto; e

VI - informações claras e ostensivas a respeito de quaisquer restrições à fruição da oferta.

Não me parece, nessa linha, que a legítima e salutar preocupação com a informação ao consumidor, possibilitando o acesso a informações essenciais relativas a preços e condições dos produtos, serviços e das empresas e sem contrariar a legislação federal sobre os temas, possa ser considerada inconstitucional, sob pena de inviabilização de qualquer regulamentação sobre o tema.

A propósito, uma das grandes conquistas legislativas no que tange às relações de consumo é justamente o direito à ampla e correta informação sobre produtos e serviços oferecidos no mercado.

(...)

Assim, ao estabelecer as obrigações acessórias de veicular informações essenciais ao consumidor em anúncios e lojas virtuais dos fornecedores, tenho para mim que os arts. 30, 34, 37, 40, 41 e 42 da Lei estadual 16.559/2019 possuem reflexos tanto no campo da propaganda comercial e do comércio interestadual e eletrônico quanto também no rol de direitos do consumidor, porém, claramente, com especificidade e priorização deste, pois, embora a lei tenha como destinatários diversos fornecedores arrolados na legislação pernambucana, a principal razão de ser da norma não está na interferência na prestação de serviços e no fornecimento das mercadorias em si, mas na implementação de um modelo de informação ao consumidor usuário daqueles produtos e serviços. Desse modo, quando da análise dessas questões, deve o intérprete priorizar o fortalecimento das autonomias locais e o respeito às suas diversidades consagrando o já citado e imprescindível equilíbrio federativo.²⁸

Essa posição pode trazer consequências complexas no futuro. Se houver, por exemplo, mudanças na legislação federal e o legislador estadual não atualizar as suas determinações legais, será instaurada grave insegurança jurídica.

²⁸ BRASIL, 2021, p. 23 e 24.

O relator, Ministro Gilmar Mendes, compreendeu o perigo da determinação legal pernambucana e votou pela inconstitucionalidade do art. 42 do Código pernambucano:

“É cada vez maior a necessidade de se considerar a profunda alteração no quadro fático e econômico pela qual temos passado, marcada pela evolução dos meios de comunicação e, conseqüentemente, pelo significativo incremento do comércio eletrônico.
(...)

Como se vê, a preocupação atual é no sentido de se encontrar uma forma de regular o comércio eletrônico globalmente. Isso demonstra a necessidade de que os países busquem, domesticamente, normas uniformes.

No cenário brasileiro, o comércio eletrônico é regulamentado pelo Decreto n. 7.962, de 15 de março de 2013. O ato normativo federal já dispõe sobre as informações que devem constar dos sítios eletrônicos. Não pode o Estado-membro, portanto, determinar o modo como as empresas que exploram atividades comerciais *online* para o Estado de Pernambuco dispõem as informações em seus *websites*.”²⁹

O ministro concluiu que, a pretexto de legislar sobre direito do consumidor, matéria de competência concorrente, o legislador pernambucano se imiscuiu em matérias de competência privativa da União, nomeadamente informática e comércio interestadual.

O posicionamento do Ministro Gilmar Mendes acabou sendo minoritário – ficou vencido, com seis votos contrários e cinco favoráveis. Nada obstante não ter formado maioria, sua argumentação foi importante pontapé inicial na discussão sobre a competência legislativa para tentar influenciar a arquitetura internet.

Não é improvável que situações como a do Estado de Pernambuco se repitam em outras unidades federativas, motivo pelo qual é essencial o reconhecimento de que a gestão da internet compete privativamente à União.

CONSIDERAÇÕES FINAIS

A regulação da internet é tarefa complexa, que envolve muitos atores no cenário internacional. É difícil a tarefa de estabelecer bases comuns entre os países que se propõem a regular o ciberespaço. Essa atividade se tornará praticamente impossível se cada país estiver dividido internamente. Por esse motivo, os Estados soberanos devem adotar posições únicas no cenário global para que não se inviabilize a existência do mundo virtual.

²⁹ BRASIL, 2021, p. 22

Assim sendo, no contexto brasileiro, o Poder Público deverá se articular em nível federal para editar normas que possibilitem o desenvolvimento do ciberespaço conforme o conjunto de valores do ordenamento jurídico nacional. Apesar disso, não se pode olvidar de que o ciberespaço não é um ambiente doméstico sobre o qual se exerce plena soberania, mas de um espaço internacional, artificial e sem fronteiras, o que exige a consciência de que há limites à atuação de cada país. Essa postura, aliada a acordos internacionais, permitirá o pleno desenvolvimento das potencialidades da internet e, conseqüentemente, das nações que nela interagem.

REFERÊNCIAS

ALMEIDA, Fernanda D. M. Doutrina contemporânea do federalismo. Revista da Procuradoria Geral do Estado de São Paulo, São Paulo, n. 80, p. 13-36, 2014.

BARCOMB, Kris E.; KRILL, Dennis J.; MILLS, Robert F.; SAVILLE, Michael A. "Establishing cyberspace sovereignty." *International Journal of Cyber Warfare and Terrorism (IJCWT)* 2, no. 3, p. 26-38. 2012.

BARLOW, John. A Declaration of the Independence of the Cyberspace. In: LUDLOW, Peter. *Crypto Anarchy, Cyberstates, and Pirate Utopias*. Cambridge: MIT Press, 2001.

BETZ, David; STEVENS, Tim. *Cyberspace and the State: Towards a Strategy for Cyber Power*. Oxford: Routledge, 2011.

BRASIL. Supremo Tribunal Federal. *ADI n. 6.214*. Relator Ministro Gilmar Mendes, redator para o acórdão Min. Alexandre de Moraes, Tribunal Pleno, DJe 20.05.2021. 2021.

_____. Tribunal de Contas da União. Acórdão n. 1.164/2012, de 16 de maio de 2012, Relator Ministro Raimundo Carreiro. 2012.

CASTELLS, Manuel; CARDOSO, Gustavo (org.). *The Network Society: From Knowledge to Policy*. Washington, DC: Johns Hopkins Center for Transatlantic Relations, 2005

CASTELLS, Manuel. *Communication Power*. OUP Oxford, 2013.

LESSIG, Lawrence. *Code 2.0: Code and Other Laws of Cyberspace*. New York: Basic Books, 2006.

LESSIG, Lawrence. *The Zones of Cyberspace*. *Stanford Law Review* 48, no. 5, 1996.

MUELLER, Milton L. Against Sovereignty in Cyberspace. *International Studies Review*, 2019.

MURRAY, Andrew. *Information technology law: the law and society*. Orxford: Oxford University Press, 2016.

REIDENBERG, Joel. Governing networks and rule-making in cyberspace. *Emory Law Journal*, v. 45, p. 911, 1996.

REIDENBERG, Joel. *Lex informatica: The formulation of information policy rules through technology*. *Tex. L. Rev.*, 76, 1997.

SCHMITT, Michael; VIHUL, Liis. Respect for sovereignty in cyberspace. *Texas Law Review*, v. 95, p. 1639, 2016.