



# O Direito do Cavalo: o que o Direito Cibernético pode ensinar

*Lawrence Lessig*<sup>†</sup>

*Tradução de*

Pedro André Guimarães Pires<sup>‡</sup> & Afonso Carvalho de Oliva<sup>§</sup>

**RESUMO**\*\* Neste ensaio, o fundador do *Creative Commons* discute a aplicabilidade e a relevância de um “direito cibernético” numa também já clássica resposta às observações de Frank Easterbrook, que, para ressaltar sua irrelevância, comparou a área a um “direito do cavalo”. O autor argumenta que, ao contrário da afirmação de Easterbrook, o estudo do direito cibernético oferece *insights* importantes sobre os limites do direito como regulador e sobre as técnicas para superar esses limites. O ensaio estrutura-se em três partes: a primeira apresenta exemplos de regulação no ciberespaço; a segunda aplica essas abordagens a outros contextos regulatórios; e a terceira identifica lições gerais, como os limites do poder regulatório, a importância da transparência e a necessidade de ajustes precisos na regulação. O autor conclui que o estudo do direito cibernético pode trazer lições relevantes para o direito em geral, ao desafiar e expandir o entendimento sobre a regulação em diferentes espaços.

**PALAVRAS-CHAVE** Ciberespaço, regulação, limites do direito

---

\* Original: LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*, v. 113, p. 501-549, 1999. Licenciado com *Creative Commons*.

† Professor de Direito e Liderança na Harvard Law School. Fundador do Center for Internet and Society e da Equal Citizens. Membro fundador do Conselho da Creative Commons. Atua no Conselho Científico do AXA Research Fund. Membro da American Academy of Arts and Sciences e da American Philosophical Society. Ganhador de vários prêmios, como o Webby, o Free Software Foundation’s Freedom Award, o Scientific American 50 Award e o Fastcase 50 Award.

‡ Mestre e bacharel em direito pela Universidade Federal de Sergipe. Diretor de Pesquisa e Extensão da Faculdade de Direito 8 de Julho. Advogado. Possui, ainda, *Certificat d’études politiques* pelo Institut d’Études Politiques de Lyon (Sciences Po Lyon). Professor de Direito Civil, Direito & Linguagem e Direito & Arte da Faculdade de Direito 8 de Julho. EDITOR-ADJUNTO da DIKÉ.

§ Doutorando em Direito Privado pela Universidade do Minho, Portugal. Mestre em direitos humanos e bacharel em direito pela Universidade Tiradentes. Diretor de Graduação da Faculdade de Direito 8 de Julho. Especialista em Direito da Tecnologia da Informação pela Fundação Getúlio Vargas. Pós-Graduado em Direito do Consumidor pela UNIDERP/LFG (2011). Pós-Graduado no MBA em Direito Eletrônico pela EPD. Avaliador do Banco de Avaliadores do Sistema Nacional de Avaliação da Educação Superior, Ministério da Educação/Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira/Diretoria de Avaliação da Educação Superior. Pesquisador em Novas Tecnologias e o Impacto nos Direitos Humanos. Possui Certificação em Privacidade e Proteção de Dados pela *EXIN - Privacy & Data Protection Foundation*.

\*\* Resumo elaborado pelos EDITORES.

## Introdução

Alguns anos atrás, em uma conferência sobre “Direito do Ciberespaço” na Universidade de Chicago, o juiz Frank Easterbrook disse aos ouvintes ali reunidos, um auditório lotado de devotos (ou pior) do “direito cibernético”<sup>1</sup>, que não existia um “direito do ciberespaço” mais do que existia um “Direito do Cavallo”<sup>2</sup>, que o esforço de falar como se existisse um tal direito iria só confundir em vez de esclarecer, e que os acadêmicos do direito (“diletantes”) deveriam apenas dar um passo atrás e deixar que juizes e advogados e tecnólogos lidassem com os problemas cotidianos que esse telefone incrementado apresentasse. “Vão para casa”, com efeito, foram as boas-vindas do juiz Easterbrook.

Como costuma acontecer quando meu então colega dá uma palestra, a intervenção, embora brilhante, produziu um silêncio constrangedor, alguns aplausos educados e depois uma passagem rápida para o próximo palestrante. Foi um pensamento interessante — o de que esta conferência era tão significativa quanto uma conferência sobre o direito do cavalo. (Um estudante ansioso que estava sentado atrás de mim sussurrou que nunca tinha ouvido falar do “direito do cavalo”.) Mas esse não parecia um pensamento muito útil, a duas horas do início dessa conferência que durou o dia inteiro. Por isso, tendo sido marcado como pouco útil, ele foi rapidamente posto de lado. No balanço do dia, e no balanço das contribuições, a conversa mudou para a ideia de que ou o direito do cavalo era importante no final das contas, ou o direito do ciberespaço era algo a mais.

Alguns de nós, no entanto, não conseguiram deixar essa questão para lá. Eu sou um desses. Confesso que passei tempo demais só pensando no que um direito do ciberespaço pode ensinar. Este ensaio é a introdução a uma resposta.<sup>3</sup> A preocupação de Easterbrook é justa. As disciplinas da faculdade de direito, argumentou Easterbrook, “deveriam ser limitadas a matérias que podem iluminar o direito inteiro”<sup>4</sup>. “[A] melhor forma de aprender o direito aplicável a empreitadas especializadas”, ele argumenta, “é estudando regras gerais”<sup>5</sup>. Esse “novo direito do ciberespaço”, concebido como responsabilidade civil no ciberespaço, contratos no ciberespaço, propriedade no ciberespaço etc., não.

Meu argumento vai no sentido contrário. Concordo que nosso foco deveria ser em disciplinas que “iluminam todo o direito”, mas, diferentemente de Easterbrook, eu acredito que há uma importante observação geral que vem de pensar especificamente sobre como o direito e o ciberespaço se conectam.

Essa observação diz respeito aos limites do direito como regulador e às técnicas para

---

<sup>1</sup> *Cyberlaw*, no original. (N. dos T.)

<sup>2</sup> V. EASTERBROOK, Frank H. *Cyberspace and the Law of the Horse*. University of Chicago Legal Forum, 1996, p. 207. A referência é a um argumento de Gerhard Casper, que, quando era reitor da Faculdade de Direito da Universidade de Chicago, gabou-se de que a faculdade de direito não oferecia um curso sobre “The Law of the Horse”. Idem na p. 207 (aspas internas omitidas). A frase é originalmente de Karl Llewellyn, que comparou o CCU com as “regras para transações idiossincráticas entre amadores”. Idem na p. 214.

<sup>3</sup> Eu desenvolvi em outro lugar um relato completo dessa resposta, ou o mais completo que o meu relato pode ser. V. LESSIG, Lawrence. *Code and Other Laws of Cyberspace*. 1999.

<sup>4</sup> EASTERBROOK, *supra*, nota 2, p. 207.

<sup>5</sup> Idem.

escapar desses limites. Essa escapatória, tanto no espaço real quanto no ciberespaço<sup>6</sup>, vem do reconhecimento da coleção de ferramentas que uma sociedade tem à mão para afetar as limitações ao comportamento. O direito, no seu sentido tradicional — uma ordem garantida por uma ameaça direcionada ao comportamento primário<sup>7</sup> — é apenas uma dessas ferramentas. A observação geral é a de que o direito pode afetar essas outras ferramentas — que elas próprias limitam o comportamento, e podem funcionar como ferramentas do direito. A escolha entre ferramentas obviamente depende de sua eficácia. Mas, com efeito, a escolha também vai levantar uma questão sobre valores. Ao lidar com esses exemplos do direito interagindo com o ciberespaço, vamos pôr em relevo um conjunto de questões gerais sobre a regulação do direito fora do ciberespaço.

Não estou argumentando que qualquer área especializada do direito produziria a mesma percepção. Não estou defendendo o direito do cavalo. Meu argumento é específico para o ciberespaço. Quando pensamos sobre a regulação do ciberespaço, conseguimos enxergar algo que outras áreas não nos mostrariam.

Meu ensaio se estrutura em três partes. Começo com dois exemplos que são paradigmas do problema da regulação no ciberespaço. Em seguida, eles vão sugerir uma abordagem específica sobre a questão da regulação em geral. No balanço da Parte I, eu esboço um modelo dessa abordagem geral.

Na Parte II, eu aplico essa abordagem geral a um conjunto mais abrangente de exemplos. É nos detalhes desses exemplos que serão encontradas as lições gerais. Essas lições têm um alcance maior do que o do âmbito do ciberespaço. São lições para o direito em geral, embora a não-plasticidade da regulação do espaço real tenha a tendência de obscurecê-las.

A Parte final descreve três dessas lições — a primeira sobre os limites do poder do direito sobre o ciberespaço, o segundo sobre a transparência, a terceira sobre um ajustamento preciso.

A primeira lição é sobre limitações constitucionais — não constituição no sentido de um texto jurídico, mas uma constituição compreendida de forma mais geral. Assim como a divisão de poderes estabelece limitações sobre até onde o governo federal pode ir, os caracteres do ciberespaço que irei descrever também estabelecem limites sobre até onde o governo pode ir.

A lição sobre transparência é mais familiar, embora eu suspeite que sua relação com o ciberespaço não seja. Ao tornar a “não-transparência” fácil e aparentemente natural, o ciberespaço fornece uma oportunidade especial de apreciar tanto o valor quanto os custos da transparência. A lição final, sobre ajustamento preciso, é menos familiar ainda, embora seja potencialmente o aspecto mais significativo da interação entre o ciberespaço e o direito do espaço real. Nos exemplos de regulação no ciberespaço, veremos a ameaça que um fracasso no “ajuste” representa. As lições sobre transparência e ajustamento preciso, ambas, são significativas para além do mundo dos engenheiros. Ou melhor, as regulações feitas pelos engenheiros terão implicações importantes para nós.

Eu concluo com uma resposta ao desafio de Easterbrook. Se meu argumento colar, então

---

<sup>6</sup> Eu discuti de forma consideravelmente detalhada que estamos sempre em um espaço real enquanto estamos no ciberespaço, ou, alternativamente, que o ciberespaço não é um espaço separado. V. LESSIG, Lawrence. *The Zones of Cyberspace*. Stanford Law Review, v. 48, p. 1403, 1996.

<sup>7</sup> V., por exemplo, HART, H.L.A. *The Concept of Law* 2. ed. 1994. pp. 6-7, 18-25.

essas três lições levantam questões sobre o direito do espaço real tão provocativas quanto as que levantam sobre o ciberespaço. Isto é, elas são preocupações gerais, não particulares. Elas sugerem uma razão para estudar o direito do ciberespaço além das particularidades do ciberespaço.

## I. Espaços Regulatórios, Real e “Cibernético”

Consideremos dois ciberespaços, e os problemas que cada um cria para dois diferentes objetivos sociais. Ambos os espaços têm problemas de “informação” — no primeiro, não há o suficiente; no segundo, há demais. Ambos os problemas derivam de um fato sobre *código* — sobre o *software* e o *hardware* que fazem o ciberespaço ser o que é. Como eu argumento de forma mais completa nas seções a seguir, o desafio regulatório central no contexto do ciberespaço é como compreender esse efeito do código.

### A. Dois problemas sobre o conteúdo zoneado

1. *Zoneamento de conteúdos.* — Pornografia no espaço real é zoneada em relação às crianças. Seja em razão de leis (banir a venda de pornografia a menores), normas sociais (encorajar a rejeitar aqueles que vendem pornografia a menores) ou o mercado (pornografia custa dinheiro), para crianças é difícil comprar pornografia no espaço real. Em geral, não em todo lugar; difícil, não impossível. Mas, no geral, as regulações do espaço real têm um efeito. Esse efeito mantém crianças longe da pornografia.

Essas regulações do espaço real dependem de certos caracteres do “design” do espaço real. No espaço real, é difícil esconder que você é uma criança. Idade, no espaço real, é um fato autoautenticado. Claro — uma criança pode tentar esconder que é uma criança: ele pode colar um bigode ou andar de pernas-de-pau. Mas disfarces são caros, e não são terrivelmente eficientes. E é difícil andar de pernas-de-pau. Normalmente, uma criança transparece que é uma criança; normalmente, o vendedor de pornografia sabe que uma criança é uma criança<sup>8</sup>, e por isso o vendedor de pornografia, em razão de normas jurídicas ou sociais, pode pelo menos identificar clientes menores de idade. A autoautenticação facilita o zoneamento do espaço real.

No ciberespaço, a idade não é autoautenticada da mesma forma. Ainda que as mesmas normas jurídicas e sociais realmente se aplicassem no ciberespaço, e ainda que as condicionantes do mercado fossem as mesmas (e não são), qualquer esforço de zonestar pornografia no ciberespaço encontraria um problema muito difícil. Idade é extremamente difícil de certificar. Para um site que aceita tráfego, todos os pedidos são iguais. Não existe uma maneira simples de um site distinguir adultos de crianças, e, da mesma forma, não existe uma maneira simples de um adulto provar que é adulto. Esse *aspecto* do espaço faz com que o zoneamento de conteúdos nele seja custoso — tão custoso que a Suprema Corte concluiu em *Reno v. ACLU*<sup>9</sup> que a Constituição pode proibi-lo.

2. *Privacidade protegida.* — Se você entrasse numa loja e o guarda da loja registrasse seu

<sup>8</sup> Cf. *Crawford v. Lungren*, 96 F.3d 380, 382 (9<sup>o</sup> Cir. 1996) (defendendo a constitucionalidade de uma lei da Califórnia que proíbe a venda de “material nocivo” em máquinas de venda automática de calçadas sem supervisão, em razão do razoável interesse estatal em proteger menores de literatura voltada para adultos).

<sup>9</sup> 521 US 844 (1997).

nome; se câmeras rastreassem todos os seus passos, anotando quais itens você olha e quais itens você ignora; se um empregado ficasse seguindo você, calculando o tempo que você passa em um dado corredor; se antes de você comprar um item que você selecionou, o caixa demandasse que você revele quem é você — se alguma dessas coisas acontecesse no espaço real, você perceberia. Você perceberia, e poderia então escolher se iria querer fazer compras em uma loja assim. Talvez os mais vaidosos apreciassem a atenção; talvez os pechincheiros fossem atraídos pelos preços baixos resultantes. Eles poderiam não ter nenhum problema com esse regime de coleta de dados. Mas pelo menos eles saberiam. Seja qual fosse a razão, seja qual fosse a escolha consequente, no espaço real eles saberiam o suficiente para saber escolher.

No ciberespaço, eles não saberiam. Eles não perceberiam um tal monitoramento porque esse rastreamento no ciberespaço não é assim visível. Como Jerry Kang acertadamente descreve<sup>10</sup>, quando você entra numa loja no ciberespaço, a loja pode registrar quem você é; *click monitors* (observar o que você escolhe com o seu mouse) vão rastrear por onde você navega, quanto tempo você visualiza uma página específica; um “empregado” (ou pelo menos um bot<sup>11</sup>) pode seguir você, e quando você faz uma compra, ele pode registrar quem você é e de onde você veio. Tudo isso acontece no ciberespaço — de forma invisível. Dados são coletados, mas sem seu conhecimento. Assim você não pode (ou pelo menos não tão facilmente) escolher se irá participar ou consentir com essa vigilância. No ciberespaço, a vigilância não é autoautenticada. Nada revela se você está sendo observado<sup>12</sup>, então não há uma base real com o qual se pode consentir.

Esses exemplos espelham um ao outro, e apresentam um padrão comum. Em cada um deles, alguma pequena porção de dados está faltando, o que quer dizer que, em cada um, um objetivo não pode ser buscado. No primeiro caso, esse objetivo é coletivo (zonestar a pornografia); no segundo, é individual (fazer escolhas sobre privacidade). Mas, em ambos, é um aspecto do ciberespaço que interfere nesse objetivo específico. E, por conseguinte, em ambos o direito deve fazer uma escolha — entre regulamentar a mudança desse aspecto arquitetônico ou deixar o ciberespaço livre e inviabilizar esse objetivo coletivo ou individual. A lei deveria mudar em resposta a essas diferenças? Ou deveria mudar os caracteres do ciberespaço, para torná-los conformes à lei? E, se a opção for a primeira, então quais limitações deverá haver sobre o esforço do direito em mudar a “natureza” do ciberespaço? Que princípios devem regular os arroudes jurídicos sobre esse espaço? Ou, novamente, como o direito deve *regular*?

\* \* \*

Para muitos essa pergunta vai soar muito esquisita. Muitos acreditam que o ciberespaço simplesmente não pode ser regulado. O comportamento no ciberespaço, como insiste esse meme, está fora do alcance do governo. A anonimidade e a multijurisdicionalidade do

<sup>10</sup> V. KANG, Jerry. Information Privacy in Cyberspace Transactions. *Stanford Law Review*, v. 50, p. 1193, 1998, pp. 1198–99; cf. DEVELOPMENTS IN THE LAW. The Law of Cyberspace. *Harvard Law Review*, v. 112, p. 1574, 1999, p. 1643. [doravante, “Developments”] (sugerindo que a invisibilidade da filtragem upstream é um problema potencial de uma solução proposta para o acesso de crianças a pornografia)

<sup>11</sup> Um “bot” é um programa de computador que age como agente para um usuário e desempenha uma tarefa, geralmente de forma remota, em resposta a um pedido.

<sup>12</sup> V. FEDERAL TRADE COMMISSION (FTC). Privacy Online: A Report To Congress. 1998, p. 3, nota 9. [doravante, “Privacy Online”].

ciberespaço tornam impossível seu controle pelo governo. A natureza desse espaço torna o comportamento nele *irregulável*<sup>13</sup>.

Essa crença sobre o ciberespaço está errada, mas errada de um jeito interessante. Ela presume que ou a natureza do ciberespaço é fixa — que sua arquitetura, e o controle que ela possibilita, não podem ser alteradas — ou que o governo simplesmente não é capaz de tomar atitudes para mudar essa arquitetura.

Nenhuma dessas presunções está correta. O ciberespaço não tem uma natureza; ele não tem uma arquitetura específica que não pode ser mudada<sup>14</sup>. Sua arquitetura é uma função do seu design — ou, como vou descrever na seção a seguir, seu código<sup>15</sup>. Esse código pode mudar, seja porque evoluiu de maneira diferente, seja porque o governo o forçou a evoluir de uma maneira específica. E embora versões específicas de ciberespaço realmente resistam a uma regulação efetiva, disso não se segue que toda versão do ciberespaço também seja assim. Em outras palavras, há versões de ciberespaço onde o comportamento pode ser regulado, e onde o governo pode tomar atitudes para aumentar essa regulabilidade.

Para entender como, deveríamos pensar de forma mais ampla a questão da regulação. O que significa dizer que alguém é “regulado”? Como essa regulação é atingida? Quais são suas modalidades?

## B. Modalidades de regulação

### 1. Quatro modalidades de regulação no espaço real e no ciberespaço. — O

<sup>13</sup> V., e.g., JOHNSON, David R.; POST, David. Law and Borders — The Rise of Law in Cyberspace. *Stanford Law Review*, v. 48, p. 1367, 1996, p. 1375; KUSHNER, David. The Communications Decency Act and the Indecent Indecency Spectacle. *Hastings Communications and Entertainment Law Journal*, v. 19, p. 87, 1996, p. 131; POST, David G. Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace. *Journal of Online Law*, art. 3, p. 12–17, 1995.; STEINERT-THRELKELD, Tom. Of Governance and Technology. Interactive Week Online, Oct. 2, 1998.

<sup>14</sup> Ver *Developments*, nota 10 *supra*, p. 1635 (“A diferença fundamental entre [espaço real e ciberespaço] é que a arquitetura do ciberespaço é aberta e maleável. Qualquer um que entenda como ler e escrever código é capaz de reescrever as instruções que definem o possível”).

<sup>15</sup> Na forma como defino o termo, *código* se refere ao software e ao hardware que constituem o ciberespaço como ele é — ou, mais precisamente, às regras e instruções inseridas no software e no hardware que, juntas constituem o ciberespaço como ele é. É óbvio que há muito “código” que atende a essa descrição e, obviamente, a natureza desse “código” varia dramaticamente a depender do contexto. Parte desse código está na camada do Protocolo de Internet (IP), onde operam os protocolos para troca de dados na Internet (incluindo TCP/IP) operam. Parte desse código está acima dessa camada de IP ou, nas palavras de Jerome H. Saltzer, em sua “ponta”: “No caso do sistema de comunicação de dados, esse intervalo inclui criptografia, detecção de mensagens duplicadas, sequenciamento de mensagens, garantia de entrega de mensagens, detecção de falhas no host, e recibos de entrega. Em um contexto mais amplo, o argumento parece se aplicar a muitas outras funções de um sistema operacional de computador, incluindo seu sistema de arquivos”. (SALTZER, Jerome H.; REED, David P.; CLARK, David D. End-to-End Arguments in System Design. In: PARTRIDGE, Craig (ed.). *Innovations in Internetworking*, p. 195-196, 1988). De modo mais geral, essa segunda camada incluiria quaisquer aplicativos que possam interagir com a rede (navegadores, programas de e-mail, clientes de transferência de arquivos), bem como as plataformas de sistema operacional nas quais esses aplicativos podem ser executados.

Na análise a seguir, a “camada” mais importante para os meus propósitos será a camada acima da camada de IP. As regulações mais sofisticadas ocorrerão nesse nível, dada a adoção pela net do design ponta-a-ponta de Saltzer. Ver também a nota 24 *infra*; cf. WU, Timothy. Application-Centered Internet Analysis. *Virginia Law Review*, v. 85, p. 1163, 1999, p. 1164. (argumentando que uma análise jurídica da internet que foque no usuário deve necessariamente focar nessa camada).

Finalmente, quando eu digo que o ciberespaço “não tem uma natureza”, quero dizer que qualquer número de designs ou arquiteturas possíveis pode afetar a funcionalidade que atualmente associamos ao ciberespaço. Não quero dizer que, dada sua arquitetura atual, não existam caracteres que, em conjunto, constituam sua natureza.

comportamento, podemos dizer, é regulado por quatro tipos de condicionantes<sup>16</sup>. O direito é só uma dessas condicionantes. O direito (em ao menos um dos seus aspectos), ordena as pessoas a se comportar de certas maneiras; ele ameaça punir quem não obedecer<sup>17</sup>. O direito me manda não comprar certas drogas, não vender cigarros sem licença, e não fazer comércio para além de fronteiras internacionais sem antes preencher um formulário aduaneiro. Assim, dizemos que o direito regula.

Mas não apenas o direito regula nesse sentido. Normas sociais também regulam. Normas sociais controlam onde eu posso fumar; afetam como eu me comporto com membros do sexo oposto; limitam o que posso vestir; influenciam se vou pagar meus tributos. Como o direito, normas sociais regulam pela ameaça de punição *ex post*. Porém, diferentemente do direito, as punições das normas sociais não são centralizadas. Normas sociais são aplicadas (quando o são) por uma comunidade, não por um governo. Desse modo, normas sociais condicionam comportamentos, e, portanto, regulam.

Também os mercados regulam. Eles regulam por meio de preços. O preço da gasolina limita a quantidade que alguém dirige — mais na Europa que nos Estados Unidos. O preço das passagens de metrô afeta o uso do transporte público — mais na Europa que nos Estados Unidos. É claro que o mercado só é capaz de condicionar comportamentos dessa maneira por causa das outras condicionantes do direito e das normas sociais: o direito das coisas e dos contratos governa os mercados; os mercados operam no âmbito permitido pelas normas sociais. Mas, dadas essas normas, e dado esse direito, o mercado apresenta um outro conjunto de condicionantes do comportamento individual e coletivo.

E, finalmente, há um quarto aspecto do espaço real que regula o comportamento: a “arquitetura”. Com “arquitetura”, refiro-me ao mundo físico tal como se encontra, mesmo que “*tal como se encontra*” seja simplesmente *como já tenha sido feito*. O fato de uma rodovia dividir dois bairros limita a extensão na qual esses bairros se integram. O fato de uma pequena cidade ter uma praça facilmente acessível com uma diversidade de lojas aumenta a integração dos residentes dessa cidade. O fato de Paris ter largas avenidas limita a capacidade de revolucionários protestar<sup>18</sup>. O fato de o Tribunal Constitucional da Alemanha ser em Karlsruhe, enquanto a capital é Berlim, limita a influência de um poder sobre o outro. Essas condicionantes funcionam de um modo que molda o comportamento. Desse modo, elas

---

<sup>16</sup> Eu adaptei essa análise do meu trabalho anterior sobre regulação. Ver, em geral, LESSIG, Lawrence. The New Chicago School. *Journal of Legal Studies*, v. 27, p. 661-666, 1998 (discutindo o modo como direito, normas sociais, mercados e arquitetura operam como modalidades de condicionantes). Ela está relacionada com a “abordagem ferramental sobre a ação governamental”, de John de Monchaux e J. Mark Schuster, mas eu conto quatro ferramentas enquanto ele conta cinco (DE MONCHAUX, John; SCHUSTER, J. Mark. Five Things to Do. In: SCHUSTER, J. Mark; DE MONCHAUX, John; RILEY II, Charles A. (eds.). *Preserving the Built Heritage: Tools for Implementation*, p. 3, 1997). Eu não acho que os números finais importam tanto, contudo. Mais importante é a compreensão de que existem formas funcionalmente distintas de alterar condicionantes de comportamento. Por exemplo, o mercado pode ou não ser simplesmente um agregado das outras modalidade; se o mercado funcionar e alterar condicionantes distintamente, porém, é melhor considerar o mercado algo distinto.

<sup>17</sup> Obviamente ele faz mais que isso, mas coloquemos de lado esse argumento sobre positivismo. Meu intuito aqui não é o de descrever a essência do direito; é apenas o de descrever uma parte do direito.

<sup>18</sup> Em 1853, Luís Napoleão III mudou o traçado de Paris, alargando as ruas para minimizar a oportunidade de revolta. V. PLESSIS, Alain. *The Rise and Fall of the Second Empire, 1852-1871*. Trad. Jonathan Mandelbaum. 1985. (Original publicado em 1979). P. 121; HAUSSMANN, George-Eugene Baron. In: *Encyclopaedia Britannica*: v. 5. 15. ed. 1993. P. 753.

também regulam.

Essas quatro modalidades regulam em conjunto. A “regulação em rede” de cada política pública em particular é a soma dos efeitos regulatórios das quatro modalidades em conjunto. Uma política é um *trade-off* entre essas quatro ferramentas regulatórias. Ela seleciona sua ferramenta a depender de qual funciona melhor.

Então, bem entendido, esse modelo também descreve a regulação do ciberespaço. Nele também podemos descrever quatro modalidades de condicionantes.

O direito regula comportamentos no ciberespaço: as legislações sobre direitos autorais, difamação e obscenidade continuam todas a fazer ameaças de sanção *ex post* para as violações. Quão eficientemente o direito regula comportamentos no ciberespaço é uma questão separada — em alguns casos ele o faz de modo mais eficiente, em outros menos. Melhor ou pior, o direito continua a ameaçar no sentido de uma resposta esperada. O Legislativo legisla<sup>19</sup>, o Ministério Público ameaça<sup>20</sup>, os tribunais condenam<sup>21</sup>.

Normas sociais também regulam comportamentos no ciberespaço: fale sobre a política democrata no fórum alt.knitting e você estará se sujeitando a sofrer “*flaming*” (uma resposta em texto furiosa). Faça “*spoofing*”<sup>22</sup> da identidade de outra pessoa em um “*MUD*” (uma realidade virtual baseada em texto) e você pode acabar sendo “*toaded*” (tendo seu personagem removido)<sup>23</sup>. Fale demais em uma lista de discussão, e é provável que você vá parar em um filtro “*bozo*” comum (que bloqueia mensagens suas). Em cada caso, normas sociais condicionam comportamentos, e, assim como no espaço real, a ameaça de sanções *ex post* (embora descentralizadas) garante a aplicação dessas normas.

Mercados também regulam comportamentos no ciberespaço. Estruturas de preço frequentemente condicionam o acesso a ele, e se não condicionarem, sinais de ocupado condicionarão<sup>24</sup>. (A America Online [AOL] aprendeu essa lição quando mudou seu plano de pagamento por hora para uma tarifa fixa.<sup>25</sup>) Alguns sites da web cobram pelo acesso, como serviços on-line fizeram por algum tempo. Anunciantes recompensam sites populares; serviços on-line cancelam fóruns impopulares. Esses comportamentos se dão todos em função das condicionantes e das oportunidades do mercado, e todos refletem seu papel regulatório.

E, finalmente, a arquitetura do ciberespaço, ou seu *código*, regula comportamentos nele.

<sup>19</sup> A ACLU (American Civil Liberties Union) lista onze estados que aprovaram regulações da Internet entre 1995 e 1997. V. ACLU, **Online Censorship in the States**.

<sup>20</sup> V., *e.g.*, a “Advertência a Todos os Usuários e Provedores de Internet”, publicada pelo Procurador-Geral do Estado de Minnesota a respeito de atividades ilícitas na Internet.

<sup>21</sup> V., *e.g.*, *United States v. Thomas*, 74 F.3d 701, 716 (6th Cir. 1996); *Playboy Enters. v. Chuckleberry Publ'g, Inc.*, 939 F. Supp. 1032, 1034 (S.D.N.Y. 1996).

<sup>22</sup> Em tecnologia da informação, o termo *spoofing* designa uma espécie de falsificação do endereço de IP ou de e-mail, com finalidade maliciosa. (N. dos T.)

<sup>23</sup> V. DIBBELL, Julian. A Rape in Cyberspace or How an Evil Clown, a Haitian Trickster Spirit, Two Wizards, and a Cast of Dozens Turned a Database Into a Society. **Annual Survey of American Law**, v. 2, p. 471, 1995, p. 477-78.

<sup>24</sup> Na época da publicação do texto original, o acesso ao ciberespaço se dava principalmente por meio de internet discada — o sinal de ocupado a que o autor se refere é o telefônico. (N. dos T.)

<sup>25</sup> V., *e.g.*, WALL STREET JOURNAL. America Online Plans Better Information About Price Changes. May 29, 1998, p. B2; NETWORK WORLD. AOL Still Suffering But Stock Price Rises. Jan. 31, 1997; HILZENRATH, David S. “Free” Enterprise, Online Style: AOL, CompuServe and Prodigy Settle FTC Complaints. *The Washington Post*, May 2, 1997, p. G1.

O código, ou o software e o hardware que fazer o ciberespaço ser como é, constitui um conjunto de condicionantes sobre como alguém pode se comportar<sup>26</sup>. O conteúdo dessas condicionantes varia — o ciberespaço não é um único lugar. Mas o que distingue as condicionantes arquitetônicas de outras condicionantes é a experiência que se tem delas. Assim como as condicionantes da arquitetura do espaço real — trilhos de trem que dividem bairros, pontes que bloqueiam o acesso de ônibus, tribunais constitucionais localizados a quilômetros da sede do governo — elas são vivenciadas como condições para acessar áreas do ciberespaço. Essas condições, contudo, são diferentes. Em alguns lugares, é necessário digitar uma senha para obter acesso<sup>27</sup>; em outros, é possível entrar com ou sem identificação<sup>28</sup>. Em alguns lugares, as transações feitas por um usuário deixam rastros, ou “*mouse droppings*”<sup>29</sup>, que ligam as transações de volta ao indivíduo<sup>30</sup>; em outros lugares, essa ligação só é realizada se o indivíduo consentir<sup>31</sup>. Em alguns lugares, pode-se escolher falar uma língua que só o destinatário é capaz de entender (por meio de criptografia)<sup>32</sup>; em outros, criptografia não é uma opção<sup>33</sup>. É o código que determina esses aspectos; eles são selecionados pelos programadores do código; eles condicionam alguns comportamentos (por exemplo, espionagem eletrônica) tornando outro comportamento possível (criptografia). Eles incorporam certos valores, ou tornam a realização de certos valores impossível. Nesse sentido, esses aspectos do ciberespaço também regulam, exatamente como a arquitetura do espaço real regula<sup>34</sup>.

Essas quatro condicionantes — tanto no espaço real como no ciberespaço — operam em conjunto. Para qualquer dada política, sua interação pode ser cooperativa, ou competitiva<sup>35</sup>. Assim, para entender como uma regulação pode ser bem-sucedida, podemos observar essas

<sup>26</sup> Cf. *Developments*, nota 10 *supra*, p. 1635 (sugerindo que alterações no código podem ser utilizadas para resolver os problemas do ciberespaço). Por “código”, neste ensaio, não me refiro aos protocolos básicos da Internet — como, por exemplo, o TCP/IP. V., de modo geral, HUNT, Craig. **TCP/IP Network Administration**. 2. ed. 1998. (explicando como o TCP/IP funciona); KROL, Ed. **The Whole Internet: User's Guide & Catalog**. 2. ed. 1992. (idem); LOSHIN, Pete. **TCP/IP Clearly Explained**. 2. ed. 1997. (idem); SEGAL, Ben. **A Short History of Internet Protocols at CERN** (descrevendo a história dos protocolos da Internet em geral, incluindo o protocolo TCP/IP). Em vez disso, refiro-me ao código do “espaço de aplicação” — ou seja, o código de aplicativos que opera sobre os protocolos básicos da Internet. Conforme descrito por Tim Wu. O TCP/IP pode ser pensado de forma útil como a grade elétrica da Internet; aplicativos “conectam-se” à Internet. Veja Wu, nota 15 *supra*, em 1191-92 (1999). Ao utilizar o termo “código” aqui, estou descrevendo os aplicativos que se conectam à Internet.

<sup>27</sup> Um exemplo de um tal lugar são os serviços online como a America Online (AOL).

<sup>28</sup> Por exemplo, as postagens no USENET podem ser anônimas.

<sup>29</sup> Algo como “cocô de rato”, num trocadilho com “*mouse*” (N. dos T.).

<sup>30</sup> Navegadores de rede disponibilizam essa informação, tanto em tempo real como arquivada em um arquivo *cookie*.

<sup>31</sup> Navegadores de rede também permitem que os usuários desativem alguns desses dispositivos de rastreamento, como os cookies.

<sup>32</sup> PGP, por exemplo, é um programa oferecido tanto comercial quanto gratuitamente para criptografar mensagens.

<sup>33</sup> Em alguns contextos internacionais, por exemplo, o emprego de criptografia é fortemente restringido. V. BAKER, Stewart A.; HURST, Paul R. *The Limits of Trust*. 1998, p. 130.

<sup>34</sup> Muitos pesquisadores estão começando a focar na ideia do direito como incorporado no código. V. *e.g.*, Johnson; Post, nota 13 *supra*, p. 1378-87 (1996); KATSH, M. Ethan. *Software Worlds and the First Amendment: Virtual Doorkeepers in Cyberspace*. **University of Chicago Legal Forum**, v. 1996, p. 335, 1996, pp. 348-354; REIDENBERG, Joel R. *Governing Networks and Rule-Making in Cyberspace*. **Emory Law Journal**, v. 45, p. 911, 917-920; SHAPIRO, Andrew L. *The Disappearance of Cyberspace and the Rise of Code*. *Seton Hall Constitutional Law Journal*, v. 8, p. 703, 1998, pp. 715-723. Para um tratamento excepcional do mesmo tema no espaço real, v. FRUG, Gerald E. **City Making: Building Communities Without Building Walls**. 1999.

<sup>35</sup> O modo como eles regulam é diferente, claro. O direito regula (nesse sentido estrito) por meio da ameaça de punição *ex post*; normas sociais regulam (quando regulam de modo eficaz) por meio de punição *ex post*, bem como por internalização *ex ante*; mercados e arquitetura regulam por uma condicionante presente — não é necessária uma condicionante *ex ante* ou uma punição *ex post* para impedir uma pessoa de caminhar através de uma parede de tijolos.

quatro modalidades agindo no mesmo campo, e entender como elas interagem.

Os dois problemas do início desta seção são um exemplo simples desse ponto:

(a) *Zoneamento de conteúdos*. — Se existe um problema no zoneamento de conteúdos no ciberespaço, este problema é causado (ao menos em parte) por uma diferença na arquitetura desse lugar. No espaço real, a idade é (relativamente) autoautenticada. No ciberespaço, não é. A arquitetura básica do ciberespaço permite que os atributos do usuário permaneçam invisíveis. Então as normas sociais ou as leis que se voltam à idade de um consumidor são mais difíceis de aplicar no ciberespaço. Leis e normas sociais são incapacitadas por essa arquitetura diferente.

(b) *Proteção da privacidade*. — Uma história similar pode ser contada sobre o “problema” da privacidade no ciberespaço<sup>36</sup>. A arquitetura do espaço real torna a vigilância geralmente autoautenticável. Normalmente, conseguimos perceber se estamos sendo seguidos, ou se dados de uma carteira de identidade estão sendo coletados. Saber disso nos possibilita recusar a dar informações se não queremos que essas informações sejam conhecidas. Assim, o espaço real interfere com a coleta de dados não consensual. Esconder espionagem é relativamente difícil.

A arquitetura do ciberespaço não escancara a presença do espião da mesma maneira. Nós navegamos pelo ciberespaço alheios às tecnologias que coletam e rastreiam nosso comportamento. Nós não somos capazes de funcionar na vida se presumimos que, aonde quer que vamos, essas informações são coletadas. Práticas de coleta variam a depender do site e dos seus objetivos. Para consentir com o rastreamento, precisamos saber que dados estão sendo coletados. Mas a arquitetura anula (em relação ao espaço real) nossa capacidade de saber quando estamos sendo monitorados, e tomar atitudes para limitar esse monitoramento.

Em ambos os casos, a diferença na possibilidade de regulação — a diferença na *regulabilidade* (tanto coletiva quanto individual) do espaço — ativa diferenças nas modalidades de condicionantes. Assim, como primeiro passo para entendermos por que um dado comportamento no ciberespaço pode ser diferente de um no espaço real, devemos entender essas diferenças nas modalidades de condicionantes.

### C. Como as modalidades interagem

1. *Efeitos diretos e indiretos*. — Apesar de eu ter descrito essas quatro modalidades como distintas, obviamente elas não operam de maneira independente. Elas interagem de maneiras óbvias. Normas sociais vão afetar quais objetos serão negociados no mercado (normas contra venda de sangue<sup>37</sup>); o mercado vai afetar a plasticidade, ou maleabilidade, da arquitetura (materiais de construção mais baratos criam maior plasticidade nos projetos); arquiteturas vão afetar quais normas sociais terão maior probabilidade de se desenvolver (espaços comuns

<sup>36</sup> Para uma visão muito mais sofisticada e sutil que a minha, v. BRIN, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom?* 1998. Brin detalha as crescentes tecnologias do espaço real para monitorar comportamentos, incluindo muitas que seriam tão invisíveis quanto as tecnologias que argumenta que definem a rede. V. pp. 5-8.

<sup>37</sup> V. e.g., WRIGHT, Karen. *The Body Bazaar*. **Discover**, out. 1998, p. 114-116 (descrevendo a proliferação da venda de sangue nos últimos anos).

afetam a privacidade<sup>38</sup>); todos os três vão influenciar quais leis serão possíveis.

Assim, uma descrição completa da interação entre as quatro modalidades teria que identificar as influências de cada uma delas sobre as outras. Mas, no relato a seguir, irei focar em apenas dois. Um é o efeito do direito sobre o mercado, as normas sociais e a arquitetura; o outro é o efeito da arquitetura sobre o direito, o mercado e as normas sociais.

Eu isolo essas duas modalidades por diferentes razões. Eu foco no direito porque é o agente de regulação *autoconsciente* mais óbvio. E foco na arquitetura porque, no ciberespaço, ela será o agente mais onipresente e insidioso. A arquitetura será a primeira opção entre os reguladores; no entanto, como o balanço deste ensaio vai tentar demonstrar, nossas intuições para pensar em um mundo regulado pela arquitetura (ciberespaço) são incipientes. Nós percebemos coisas quando pensamos em um mundo regulado pela arquitetura (ciberespaço) que passam despercebidas quando pensamos em um mundo regulado pelo direito (espaço real).

Para cada modalidade, há dois efeitos distintos. Um é o efeito de cada modalidade no indivíduo que está sendo regulado. (Como direito, por exemplo, diretamente condiciona um indivíduo? Como a arquitetura diretamente condiciona um indivíduo?) O outro é o efeito de uma dada modalidade de regulação sobre uma segunda modalidade de regulação, um efeito que, por sua vez, altera o efeito da segunda modalidade sobre o indivíduo. (Como o direito afeta a arquitetura, que por sua vez afeta as condicionantes sobre um indivíduo? Como a arquitetura afeta o direito, que por sua vez afeta as condicionantes sobre um indivíduo? O primeiro efeito é *direto*; o segundo é *indireto*<sup>39</sup>).

Um regulador usa tanto o efeito direito como o indireto para provocar um dado comportamento<sup>40</sup>. Quando o regulador age indiretamente, podemos dizer que ele usa ou coopta a segunda modalidade de condicionante para provocar seu fim regulatório. Assim, por exemplo, quando o direito dispõe que a arquitetura seja alterada, ele o faz para usar a arquitetura para provocar um fim regulatório. A arquitetura se torna a ferramenta do direito quando a ação direta do direito sozinha não seria tão eficaz.

Qualquer número de exemplos seria capaz de expor o argumento, mas um será

<sup>38</sup> V., *e.g.*, MOORE, Barrington Jr. **Privacy: Studies in Social and Cultural History**. 1984, p. 7 (descrevendo como uma família de esquimós compartilhando um pequeno iglu torna a privacidade uma “*commodity* inatingível”).

<sup>39</sup> A distinção entre efeitos “diretos” e “indiretos” tem uma história problemática na filosofia, v. THOMSON, Judith Jarvis. The Trolley Problem. **Yale Law Journal**, v. 94, p. 1395, 1985, pp. 1395-1396 (discutindo o dilema moral do maquinista de um trem que deve escolher entre manter seu curso e matar cinco pessoas por sua ação indireta ou tomar uma atitude direta para alterar seu curso de modo a só matar uma pessoa), bem como no direito, v. *e.g.*, NLRB v. Jones & Laughlin Steel Corp., 301 U.S. 1, 34-41 (1937) (abordando o grau no qual os empregados de uma empresa de aço estavam envolvidos no comércio interestadual). Os problemas de distinguir entre consequências diretas e indiretas são similares àqueles que emergem na doutrina do duplo efeito. V. FOOT, Philippa. The Problem of Abortion and the Doctrine of the Double Effect. In: **Virtues and Vices and Other Essays in Moral Philosophy**, 1978, p. 19; v. também BOLE III, Thomas J. The Doctrine of Double Effect: Its Philosophical Viability. **Southwest Philosophical Review**, v. 7, p. 1, 1991, pp. 91-103 (discutindo e analisando problemas sobre a doutrina do duplo efeito); QUINN, Warren S. Actions, Intentions, and Consequences: The Doctrine of Double Effect. **Philosophy & Public Affairs**, v. 18, 1989, pp. 334-341 (idem). A dificuldade surge quando uma linha entre direto e indireto deve ser traçada; não há necessidade de traçar essa linha neste ensaio.

<sup>40</sup> Meu intuito com esse esboço não é o de representar todas as forças que podem influenciar cada condicionante. Sem dúvidas, mudanças no código influenciam o direito e mudanças no direito influenciam o código; e assim com as outras condicionantes. Um relato completo de como essas condicionantes evoluem teria que incluir um relato dessas influências entremeadas. Mas, para o momento, estou focando apenas na intervenção intencional por parte do estado.

suficiente.

2. *O fumo e o retrato da regulação moderna.* — Suponha que o governo busca reduzir o consumo de cigarros. Existem diversas maneiras pelas quais o governo poderia atingir esse fim específico. O direito poderia, por exemplo, proibir o fumo<sup>41</sup>. (Este seria o direito regulando diretamente o comportamento que ele quer mudar.) Ou o direito poderia tributar o cigarro<sup>42</sup>. (Este seria o direito regulando a oferta de cigarros no mercado, para diminuir seu consumo.) Ou o direito poderia financiar uma campanha publicitária pública contra o fumo<sup>43</sup>. (Este seria o direito regulando normas sociais, como meio de regular o comportamento de fumar.) Ou o direito poderia regular a nicotina do cigarro, obrigando os fabricantes a reduzir ou eliminar a nicotina<sup>44</sup>. (Este seria o direito regulando a “arquitetura” do cigarro como um meio de reduzir seu poder viciante e, com isso, reduzir o consumo de cigarros.)

De cada uma dessas ações pode ser esperado algum efeito (vamos chamá-lo seu benefício) sobre o consumo de cigarros; cada ação tem, também, um custo. A questão em relação a cada uma é se o custo supera o benefício. Se, por exemplo, o custo da educação para alterar normas sociais sobre o fumo fosse o mesmo que o custo de alterações na arquitetura, o valor que atribuímos à autonomia e à escolha individual pode virar a balança em favor da educação.

Este é o retrato da regulação moderna. O regulador está sempre fazendo uma escolha — uma escolha, dadas as regulações diretas que essas quatro modalidades podem efetivar, entre usar o direito direta ou indiretamente para algum fim regulatório. A questão não é binária: o direito não escolhe uma estratégia em detrimento de outra. Em vez disso, já sempre uma mescla de estratégias diretas e indiretas. A questão que o regulador deve perguntar é: *qual mescla é a ideal?*

A resposta vai depender do contexto da regulação. Em uma comunidade pequena e proximamente unida, normas sociais podem ser o modo ideal de regulação; à medida que essa comunidade se torna menos unida, o direito ou o mercado podem substituir as normas sociais como uma segunda melhor escolha. Na Europa do século X, mexer nas condicionantes arquitetônicas devia ser um pouco difícil, mas na era dos edifícios de escritórios modernos, a arquitetura se torna uma técnica regulatória viável e bastante eficaz (pense em cubículos transparentes como meio de fiscalizar comportamentos). A mescla ideal depende da

<sup>41</sup> V. e.g., ALASKA. Alaska Statutes § 18.35.305. Michie, 1990 (proibindo o fumo em lugares públicos); ARIZONA. Arizona Revised Statutes Annotated § 36-601.01. West, 1993 (idem); COLORADO. Colorado Revised Statutes Annotated § 25-14-103. West, 1990 (idem).

<sup>42</sup> V. e.g., 26 U.S.C. § 5701 (1994) (tributando fabricantes de cigarros); 26 U.S.C. § 5731 (1994) (idem).

<sup>43</sup> V. e.g., ADWEEK. **Feds Pick Up Arnold Spots**. 23 nov. 1998, p. 8 (reportando a decisão do U.S. Office of National Drug Control Policy [agência da política nacional de controle de drogas dos EUA] de levar ao ar em rede nacional sete comerciais antitabagismo direcionados à população jovem inicialmente criados para o Massachusetts Department of Public Health [departamento de saúde pública do estado de Massachusetts]); FERDINAND, Pamela. Mass. Gets Tough with Adult Smokers in Graphic TV Ads. **The Washington Post**, 14 out. 1998, p. A3 (descrevendo uma série de seis anúncios antitabagismo de 30 segundos, financiados pelo Massachusetts Department of Public Health, sobre a luta por sobrevivência de uma mulher lentamente asfixiada por um enfisema).

<sup>44</sup> Não está claro se a Food and Drug Administration (FDA) [agência reguladora de alimentos e medicamentos] tem autoridade para regular o teor de nicotina dos cigarros. Em agosto de 1996, a FDA publicou no Registro Federal suas *Regulações Restringindo a Venda e a Distribuição de Cigarros e de Tabaco Sem Fumaça para Proteger Crianças e Adolescentes*, 61 Fed. Reg. 44,396 (1996) (a serem codificadas no Código Federal de Regulações em 21 C.F.R. pts. 801, 803, 804, 807, 820, e 897). No caso *Brown & Williamson Tobacco Corp. v. FDA*, 153 F.3d 155 (4th Cir. 1998), a corte entendeu que a FDA não teria competência para regular a comercialização de produtos de tabaco porque tal regulação excederia o escopo pretendido pelo Federal Food, Drug, and Cosmetic Act [lei federal sobre alimentos, drogas e cosméticos]. V. p. 176.

plasticidade das diferentes modalidades. Claro, o que funciona em um contexto não vai necessariamente funcionar em todo lugar. Mas em um contexto específico, podemos ser capazes de inferir que certas modalidades vão dominar.

É o caso, sugiro eu, no ciberespaço. Como descrevo de forma mais completa na seção seguinte, a maneira mais efetiva de regular comportamentos no ciberespaço será por meio da regulação sobre o código — seja ela uma regulação direta do código do ciberespaço em si ou das instituições (desenvolvedores) que produzem esse código. Ao sujeitá-lo a uma qualificação cada vez mais importante<sup>45</sup>, podemos então esperar que os reguladores se concentrem mais nesse código com o passar do tempo<sup>46</sup>.

Meu objetivo nas próximas duas seções é o de explorar essa dinâmica de forma mais completa. Minha expectativa é mostrar (1) que o estado é capaz de regular comportamentos no ciberespaço (no sentido contrário de *slogans* sobre a irregulabilidade do ciberespaço); (2) que o modo ideal de regulação estatal será diferente quando ele regular comportamentos no ciberespaço; e (3) que essa diferença levantará questões urgentes que o direito constitucional ainda precisa responder satisfatoriamente. (Quais limites deve haver para a regulação indireta? Até que ponto devemos permitir que o direito coopte as outras estruturas de condicionantes?)

## II. Interações: direito e arquitetura

### A. O direito domando o código: aumentando a regulabilidade do ciberespaço.

Eu mencionei anteriormente a percepção geral de que o ciberespaço é irregulável — de que sua natureza o faz ser assim e que essa natureza é fixa. Argumentei que a questão sobre se o ciberespaço pode ser regulado não se dá em função da Natureza. Ela depende, antes, de sua arquitetura, ou de seu código<sup>47</sup>. Sua *regulabilidade*, como podemos chamá-la, se dá em função de seu design. Há designs nos quais os comportamentos na Rede estão fora do alcance do governo; e há designs nos quais os comportamentos na Rede estão totalmente ao alcance do governo. Minha alegação nesta seção é a de que o governo é capaz de tomar medidas para alterar o design da Internet. Ele pode, em outras palavras, afetar a regulabilidade da Internet.

Eu ofereço dois exemplos que, juntos, devem sugerir o argumento mais geral.

1. *Aumentando a regulabilidade coletiva: zoneamento.* Retornemos ao problema do zoneamento da Seção 1. Minha alegação é a de que, no espaço real, o aspecto autoautenticável de ser criança possibilita a aplicação de regras de acesso, enquanto no ciberespaço, onde a idade não é autoautenticável, as mesmas regulações são de difícil aplicação.

<sup>45</sup> V. nota 105 *infra* (discutindo código aberto).

<sup>46</sup> Um exemplo recente é o esforço do FBI para compelir a Internet Engineering Task Force (IETF) [*força-tarefa para engenharia de internet*] a mudar protocolos de Internet a fim de adequá-los ao Communications Assistance of Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codificada em 47 U.S.C. §§ 1001-1010). A IETF resistiu, mas esse esforço é precisamente o que esse modelo iria prever. V. MCCULLAGH, Declan. IETF Says "No Way" to Net Taps. **Wired News**.

<sup>47</sup> Por arquitetura ou "*design*", refiro-me tanto ao *design* técnico da Rede, como ao seu *design* social ou econômico. Como irei descrever de modo mais completo na nota 105 abaixo, um aspecto crucial do *design* da Rede que afeta sua regulabilidade é o seu domínio. Mais precisamente, a capacidade do estado de regular a Rede depende em parte de quem é o dono do código da Rede.

Uma resposta seria tornar a identidade autoautenticável modificando o código da Rede de modo que, quando eu me conecto a um site, informações sobre mim são transmitidas a ele. Esta transmissão possibilitaria aos sites determinar se, dado meu *status*, minha entrada deveria ser permitida.

Como?

De certa forma, a Rede já facilita algumas formas de identificação. Um servidor, por exemplo, é capaz de dizer se meu browser é Microsoft ou Netscape; é capaz de dizer se minha máquina é Macintosh ou Windows. Esses são exemplos de autoautenticação já embutidos no código da Rede (ou http).

Outro exemplo é o “endereço” de um usuário. Todo usuário da Rede tem, pelo tempo em que está usando a Rede, um endereço conhecido como Protocolo de Internet (IP)<sup>48</sup>. Esse endereço de IP é único: apenas uma máquina, em qualquer dado momento, pode ter um endereço específico. Dispositivos na Rede usam esse endereço para saber para onde enviar os pacotes de dados requisitados. Mas embora esses endereços sejam únicos, não há qualquer conexão necessária entre um endereço e uma pessoa. Apesar de algumas máquinas terem endereços de IP “estáticos” que são permanentemente atribuídos àquela máquina, muitas têm endereços de IP “dinâmicos”, que são atribuídos para apenas uma sessão e podem mudar quando a máquina reconecta à Internet. Assim, embora algumas informações sejam reveladas quando uma máquina está na Rede, a *Internet* atualmente não requer qualquer autenticação além de um endereço de IP.

Outras redes são diferentes. *Intranets*<sup>49</sup>, por exemplo, são redes que se conectam à Internet. Essas redes estão de acordo com os protocolos de Internet básicos, mas elas também sobrepõem a esses protocolos outros protocolos. Entre estes estão protocolos que permitem a identificação do perfil de um usuário pelo controlador da intranet. Tais protocolos, em outras palavras, possibilitam uma forma de autoautenticação que facilita a identificação. A extensão dessa identificação varia. Em um extremo estão técnicas biométricas que vinculariam uma característica física do usuário (impressão digital ou escaneamento ocular) a um registro de identidade, e assim identificariam especificamente o usuário; no outro extremo estão

---

<sup>48</sup> Um endereço de IP é “um número de 32 bits que identifica cada remetente ou destinatário de informações enviadas em pacotes pela Internet. Quando você solicita uma página HTML ou envia um e-mail, a parte de Protocolo de Internet do TCP/IP inclui seu endereço de IP na mensagem (na verdade, em cada um dos pacotes, se for necessário mais de um) e o envia para o endereço de IP que é obtido quando se busca o nome de domínio no URL que você solicitou ou no endereço de e-mail para o qual você está enviando uma mensagem. Na outra ponta, o destinatário pode ver o endereço de IP do solicitante da página da Web ou do remetente do e-mail e pode responder enviando outra mensagem usando o endereço de IP recebido” (IP ADDRESS (Internet Protocol address). In: **WhatIs**. Disponível atualmente, em versão atualizada, em <https://www.techtarget.com/whatis/definition/IP-address-Internet-Protocol-Address>).

<sup>49</sup> Intranets são a porção que cresce mais rapidamente na Internet hoje. Elas são um estranho híbrido de duas tradições na computação de redes — uma é o sistema aberto da Internet, e o outro é a capacidade de controle das redes privativas tradicionais. Uma intranet mescla valores de ambas para produzir uma rede que é interoperável, mas dá ao seu administrador uma grande parcela de controle sobre o comportamento do usuário. Uma “Internet” com controle é no que nossa intranet está se transformando. V., e.g., LOHR, Steve. Internet Future at IBM Looks Oddly Familiar. **The New York Times**, 2 set. 1996, p. 37 (“Nos Estados Unidos, o investimento em *software* de intranet para servidores, os poderosos computadores que armazenam dados de rede, deve aumentar para 6,1 bilhões de dólares em 2000, ante 400 milhões este ano. Em contraste, o investimento em *software* de servidores de Internet tem uma projeção de aumento para 2,2 bilhões de dólares, ante os atuais 550 milhões.”); LOHR, Steve. Netscape Taking on Lotus With New Corporate System. **The New York Times**, 16 out. 1996, p. D2 (“Executivos da Netscape apontaram estudos que projetam que o mercado de intranet deve aumentar para 10 bilhões de dólares em 2000”).

certificados que simplesmente identificariam características da pessoa — que ela é maior de dezoito anos, que ela é cidadã norte-americana etc.

Está além do escopo deste ensaio esboçar um panorama completo dessas tecnologias. Meu objetivo é muito mais limitado. É suficiente, aqui, mostrar que a identificação é possível, e depois explicar como o governo pode agir para facilitar o uso dessas tecnologias.

Minha alegação nesta seção é essa: se essas tecnologias de identificação estivessem em uso geral na Internet, a *regulabilidade* dos comportamentos no ciberespaço aumentaria. E o governo pode afetar o uso geral dessas tecnologias.

Então foquemos na questão individual da proteção de crianças contra conteúdos adultos na Rede<sup>50</sup>. O Congresso já tentou, por duas vezes, produzir uma legislação que regulasse a disponibilidade de tais conteúdos para “menores”<sup>51</sup>. À época deste escrito, ele falhara duas vezes<sup>52</sup>. No primeiro caso, o Congresso tentou regular de forma ampla demais; no segundo, ele corrigiu o problema, mas onerou a classe errada de usuários — os adultos<sup>53</sup>.

Consideremos uma terceira alternativa, que em minha visão não levantaria as mesmas preocupações constitucionais<sup>54</sup>. Imagine o seguinte estatuto:

1. *Navegação em modo infantil.* Fabricantes de navegadores possibilitarão a ativação de uma navegação em “modo infantil” [NMI]. Quando ativada, a NMI sinalizará aos servidores que o usuário é menor. O software do navegador deveria permitir uma proteção por senha para a navegação em modo não-infantil. O navegador também deveria desabilitar qualquer coleta de dados sobre o usuário de um navegador em modo infantil. Em especial, ele não transmitirá para os sites qualquer dado pessoal do usuário que permita identificá-lo.
2. *Responsabilidade do servidor.* Quando um servidor identificar um cliente em NMI, ele deverá (1) bloquear este cliente de qualquer material apropriadamente

<sup>50</sup> V. *Developments*, nota 10 *supra*, pp. 1637-1643 (sugerindo soluções de código para esse problema).

<sup>51</sup> V. Child Online Protection Act (COPA), Pub. L. No. 105-277, 112 Stat. 2681 (1998) (codificado em 47 U.S.C. § 231); Telecommunications Act de 1996 (Communications Decency Act, ou CDA), Pub. L. No. 104-104, §§ 501-502, 505, 508-509, 551-552, 110 Stat. 56, 133-43 (1996).

<sup>52</sup> V. *Reno v. ACLU*, 521 U.S. 844, 849 (1997) (derrubando parte do CDA); *ACLU v. Reno*, 31 F. Supp. 2d 473, 492-98 (E.D. Pa. 1999) (acolhendo o pedido da autora de antecipação de tutela em razão da probabilidade substancial de sucesso de sua pretensão, que considera o COPA presumidamente inválido e sujeito a estrito escrutínio).

<sup>53</sup> O CDA regulava conteúdo “indecente”, o que a Corte não reconheceu (fora do contexto de transmissão) como uma categoria de discurso sujeita ao poder de proibição do Congresso. O COPA regula as ações de adultos que desejam acessar conteúdo adulto. Como descrevo adiante, uma alternativa menos restritiva seria a de apenas atribuir um ligeiro ônus aos adultos.

<sup>54</sup> Embora essa ideia já esteja por aí há algum tempo, sou grato a Mark Lemley por me levar a reconhecê-la. Para uma análise mais formal da questão sobre a constitucionalidade dessa alternativa, v. LESSIG, Lawrence; RESNICK, Paul. The Constitutionality of Mandated Access Controls. *Michigan Law Review*, v. 98 (a ser publicado no outono de 1999). Um estatuto menos obrigatório também pode ser imaginado — um que simplesmente exigisse que servidores reconhecessem e bloqueassem navegadores com identificadores de crianças. Sob essa solução, algumas empresas de navegadores teriam um incentivo de mercado para fornecer NMI; outras não teriam. Mas, para criar esse incentivo, a sinalização deve ser reconhecida. Note que a Apple Computer chegou perto desse modelo com seu OS 9. O OS 9 permite que múltiplos usuários tenham acesso a uma única máquina. Quando a máquina está configurada para múltiplos usuários, cada usuário deve fornecer uma senha para obter acesso a seu perfil. Seria uma mudança pequena adicionar a esse sistema a capacidade de sinalizar que usuário é uma criança. Essa informação seria então reportada como parte da identificação da máquina.

considerado “prejudicial para menores”<sup>55</sup> e (2) abster-se de coletar qualquer dado pessoal do usuário que permita identificá-lo, com exceção dos necessários para processar suas requisições. Quaisquer dados dessa natureza coletados devem ser excluídos do sistema dentro de  $X$  dias.

Não obstante a retórica sobre a irregularidade do ciberespaço, perceba quão simplesmente essa regulação poderia ser implementada e aplicada. Num mundo onde noventa por cento dos navegadores são produzidos por duas empresas<sup>56</sup>, os desenvolvedores de código são proeminentes demais para se esconder. E por que se esconder de qualquer forma? — dada a simplicidade desse requisito, conformar-se a ele seria fácil. Em muito pouco tempo, um tal estatuto produziria navegadores com a funcionalidade da NMI, pelo menos para aqueles pais que quisessem ter um controle como esse nas máquinas da sua casa.

Da mesma forma, seria fácil para sites desenvolver softwares para bloquear o acesso se o usuário sinaliza que é uma criança. Um sistema assim não requereria uma identificação custosa, nem uma base de dados de registros de identidade, e nem cartões de crédito. Em vez disso, o servidor seria programado para aceitar usuários que não tivessem o modo infantil selecionados, mas rejeitar os que tivessem.

Minha posição não é a de endossar uma tal legislação: eu acho que a resposta ideal do Congresso é não fazer nada. Mas se o Congresso adotasse essa forma de regulação, minha visão é a de que ela seria ao mesmo tempo factível e constitucional. Netscape e Microsoft não teriam nenhuma objeção pela Primeira Emenda<sup>57</sup> viável a uma regulação de seu código<sup>58</sup>; e sites não teriam nenhuma objeção constitucional ao requisito de bloquear navegadores em modo infantil<sup>59</sup>. Nunca houve nenhum precedente jurisprudencial<sup>60</sup> que determinasse que, em razão

<sup>55</sup> V. *Ginsberg v. New York*, 390 U.S. 629, 641 (1968) (“Sustentar a competência estadual para excluir materiais definidos como obscenidade (...) requer apenas que possamos dizer que não foi irracional o fato de o Legislativo considerar que a exposição ao material condenado pela legislação é prejudicial a menores”).

<sup>56</sup> V. MECKBACH, Greg. Microsoft’s IE Tops in New Poll. Browser Gains Edge over its Netscape Competitor as Organizations Warm to Pre-Installed Software. **Computing Canada**, 9 jul. 1999, p. 25. (citando achados da Positive Support Review, Inc., de que que o Internet Explorer da Microsoft detém 60,5% de participação de mercado, comparada a 35,1% detidos pelo Navigator da Netscape). Eu faço uma importante qualificação a esse argumento mais adiante.

<sup>57</sup> Consagra o direito fundamental à liberdade de expressão e seus desdobramentos. (N. dos T.)

<sup>58</sup> Cf. *Junger v. Daley*, 8 F. Supp. 2d 708, 717-18 (N.D. Ohio 1998) (julgando que “o código-fonte é funcional por definição” e que, “em razão de os elementos expressivos de códigos-fonte de criptografia não são ‘inequívocos’ ou ‘substancialmente aparentes’, sua exportação não é protegida pela Primeira Emenda”). Em última análise, no entanto, a questão sobre se um código específico é expressivo ou puramente funcional é decidida caso a caso, e atualmente há divergência entre tribunais. Compare-se o caso citado com *Karn v. United States Dep’t of State*, 925 F. Supp. 1, 9 n.19 (D.D.C. 1996) (expressando que “códigos-fonte são meramente um meio de comandar um computador a desempenhar uma função”), com *Bernstein v. U.S. Dep’t of Justice*, 176 F.3d 1132, 1141 (9th Cir. 1999), reapreciação acolhida em 1999 WL 782073 (concluindo que “softwares de criptografia, em sua forma de código-fonte e empregados por pessoas do campo da criptografia, devem ser considerados expressivos para fins da Primeira Emenda”). Para um artigo útil que critica o alcance da decisão da corte distrital no caso *Bernstein*, v. ROSS, Patrick Ian. Computer Programming Language. **Berkeley Technology Law Journal**, v. 13, p. 405, 1998.

<sup>59</sup> Pelo menos enquanto o caso *Ginsberg* for o precedente vinculante. V. *Ginsberg*, 390 U.S., p. 633 (confirmando a condenação do operador de uma loja por vender a um menor material prejudicial para menores).

<sup>60</sup> No modelo de direito anglo-saxão de *common law*, e em específico nos EUA, o sintético texto constitucional é interpretado pelas cortes, que consagram direitos por meio de precedentes vinculantes. *Leading cases* célebres como *Marbury v. Madison* (que inaugurou o controle de constitucionalidade judicial), *Roe v. Wade* (que consagra o direito fundamental ao aborto, até ser superado pelo caso *Dobbs v. Jackson Womens’s Health Organization* em 2022) ou *Brown v. Board of Education of Topeka* (que julgou inconstitucional a segregação racial), todos da Suprema Corte dos EUA, completam o sentido do texto constitucional. Sobre o tema, v., e.g., CARDOZO, Benjamin N. The Judge as a Legislator. In: O’BRIEN, David M. (org.).

da liberdade de expressão, uma pessoa teria o direito de não ter sua expressão sujeita a absolutamente nenhuma limitação, se essa limitação fosse necessária para atender a uma necessidade de estado demonstrada; o único requisito posto pelo caso *Reno v. ACLU*<sup>61</sup> é o de que a limitação imposta seja a menos restritiva<sup>62</sup>. A limitação imposta pela NMI, sugiro eu, seria a menos restritiva.

O sistema de NMI também seria relativamente eficaz<sup>63</sup>. Imagine que o FBI tenha programado um bot para vasculhar a Rede por um navegador com o modo infantil ativado. O bot tentaria obter acesso a sites; se conseguisse, relataria ao investigador o máximo de conteúdo que pudesse extrair. Esse conteúdo seria então analisado, e o conteúdo que pudesse ser considerado adulto seria notificado a um investigador. Este investigador determinaria se esses sites eram de fato “sites adultos”; e se fossem, o inquérito procederia contra esses sites. O resultado seria um sistema extremamente eficaz no monitoramento do acesso a conteúdo adulto na rede. Esse sistema iria, em consequência, tornar o COPA inconstitucional, uma vez que representaria uma alternativa menos restritiva para o mesmo fim de regulação de conteúdo.

Para os propósitos de zoneamento do conteúdo adulto, essa mudança alteraria fundamentalmente a regulabilidade da Rede. E o faria não apenas regulando diretamente as crianças, mas alterando um único aspecto da “arquitetura”<sup>64</sup> da Rede — a capacidade de um navegador de fornecer certas informações sobre o usuário. Uma vez estando esta funcionalidade embutida nos navegadores em geral, a capacidade dos fornecedores de conteúdo adulto de discriminar entre adultos e crianças mudaria. Esta regulação do código tornaria então possível a regulação de comportamentos.

## 2. *Aumentando a regulabilidade individual: privacidade.* — O zoneamento de

---

**Judges on Judging: Views from the Bench.** 5. ed. Washington, D.C.: SAGE CQ Press, 2016; GINSBURG, Ruth Bader. Speaking in a Judicial Voice: Reflections on *Roe v. Wade*. In: Idem. *Ibidem*; SUNSTEIN, Cass R. **A Constitution of Many Minds.** Princeton: Princeton University Press, 2009. (N. dos T.)

<sup>61</sup> 521 U.S. 844 (1997).

<sup>62</sup> V. *idem*, p. 874. Nesse sentido, concordo com a leitura do caso *Reno* oferecida pelo professor Volokh. V. VOLOKH, Eugene. Freedom of Speech, Shielding Children, and Transcending Balancing. **Supreme Court Review**, v. 1997, p. 141, 1997, pp. 141-142 (“A liberdade de expressão para adultos pode ser restringida para servir ao imperativo interesse de proteger crianças, mas apenas se a restrição for o meio menos restritivo de fazê-lo”).

<sup>63</sup> A minha alegação não é a de que a regulação seria perfeitamente eficaz, porque, é claro, nenhuma regulação é perfeitamente eficaz. Crianças geralmente sabem mais sobre computadores do que seus pais e podem facilmente burlar controles que seus pais impõem. A questão relevante, no entanto, é se a capacidade de burlar o controle parental é mais fácil com o sistema de identificação de adultos do que com o sistema de identificação de crianças. Para burlar o sistema de identificação de adultos, as crianças precisariam apenas de um número de cartão de crédito válido — o que, em alguns casos, liberaria seu acesso sem cobrar o site do cartão de crédito. Mais importante ainda, o estado atual do conhecimento parental não é um parâmetro justo para julgar a potencial eficácia de um sistema. Pais teriam incentivo para aprender se as tecnologias de controle fossem apresentadas de forma mais simples.

A questão da eficácia também surge no contexto de sites estrangeiros, já que muitos sites estrangeiros dificilmente obedecerão a uma regulamentação do governo dos Estados Unidos. Mas, novamente, a questão relevante é se eles são mais propensos a respeitar uma lei de identificação de adultos ou uma lei de identificação de crianças. Minha impressão é a de que seria mais provável que eles respeitassem a lei menos restritiva.

<sup>64</sup> Meu uso do termo “arquitetura” é um tanto idiossincrático, mas não completamente. Eu uso o termo como é usado por Charles R. Morris e Charles H. Ferguson. V. MORRIS, Charles R.; FERGUSON, Charles H. How Architecture Wins Technology Wars. **Harvard Business Review**, Mar.-Abr. 1993, p. 86. Meu uso do termo não corresponde exatamente à maneira como ele é usado pelos cientistas da computação, exceto no sentido de “estrutura de um sistema”. V., *e.g.*, LOSHIN, Pete. *TCP/IP Clearly Explained*. 2nd ed. 1997, p. 394 (definindo “arquitetura”)

pornografia é um exemplo de regulação vertical<sup>65</sup>. O estado, presumidamente com apoio popular, impõe um juízo sobre quem deve ter acesso a quê. Ele impõe esse juízo obrigando desenvolvedores a desenvolver códigos em conformidade com as regras estatais. O estado precisa impor essas regras porque a arquitetura inicial da Rede impossibilita a regulação vertical. (A maioria pode pensar que esta é uma virtude, não um vício. Mas o estado provavelmente não faz parte dessa maioria.) Essa arquitetura interferia no controle vertical. A resposta foi modificar essa arquitetura.

O problema da privacidade no ciberespaço é diferente. A característica da Rede que cria o problema de privacidade (a coleta automática e invisível de dados) interfere na regulação vertical — regulação esta que é imposta por indivíduos por meio de escolhas individuais.

Diferentes arquiteturas podem possibilitar ou impossibilitar escolhas individuais fornecendo (ou deixando de fornecer) aos indivíduos tanto as informações de que eles precisam para tomar uma decisão quanto a opção de executar esta decisão. O exemplo da privacidade pressupõe uma arquitetura que não possibilita escolhas individuais, pois esconde fatos necessários para essas e, com isso, impossibilita o controle vertical. A autorregulação, assim como a regulação estatal, depende de arquiteturas de controle. Sem essas arquiteturas, nenhuma das formas de regulação é possível.

No entanto, repito, arquiteturas podem ser alteradas. Assim como no zoneamento da pornografia, arquiteturas que impossibilitam a autorregulação estão sujeitas a escolhas coletivas. O governo é capaz de agir no sentido de impor uma mudança no código, tornando a autorregulação menos custosa e facilitando, com isso, um aumento na autorregulação.

Aqui, a técnica para impor essa mudança, entretanto, é uma ferramenta tradicional de direito. O problema da proteção da privacidade no ciberespaço vem em parte de uma arquitetura que permite a coleta de dados sem o consentimento do usuário<sup>66</sup>. Mas o problema também vem de um regime implícito de direito subjetivo<sup>67</sup> que não requer que o coletor obtenha o consentimento do usuário. Como o usuário não tem direito real<sup>68</sup> sobre informações pessoais, as informações sobre o usuário são de livre apropriação. Assim, arquiteturas que possibilitam essa apropriação são eficientes para o coletor, e consistentes com o regime legal de base.

O truque seria mudar o regime legal de direito subjetivo de maneira suficiente para mudar os incentivos daqueles que arquitetam as tecnologias de consentimento. O estado

---

<sup>65</sup> *Top-down regulation*, no original. Optamos por traduzir “*top-down regulation*” e “*bottom-up regulation*”, respectivamente, como “regulação vertical” e “regulação horizontal”, em razão da tendência, em nossa tradição jurídica, de conceber o sistema jurídico com uma separação no mínimo esquemática entre direito público e direito privado. A partir dela, tendemos a visualizar as relações jurídicas de direito público como verticais, porque têm como fonte de regulação a lei, que é imposta pelo estado em face do particular, “de cima para baixo”. As relações privadas, por sua vez, têm como fonte de regulação primária o negócio jurídico e o contrato, *a priori* em pé de igualdade, sendo portanto descritas como horizontais — mas não “de baixo para cima”. (N. dos T.)

<sup>66</sup> Cf. REIDENBERG, Joel R.; SCHWARTZ, Paul M. **On-Line Services and Data Protection and Privacy — Regulatory Responses**. 1998, pp. 65-84. (“A transparência é um dos princípios fundamentais do direito europeu de proteção de dados. Este padrão exige que o processamento de informações pessoais seja estruturado de maneira aberta e compreensível para o indivíduo. Além disso, a transparência requer que os indivíduos tenham direitos de acesso e correção às informações pessoais armazenadas”).

<sup>67</sup> No original, “background regime of entitlement”. (N. dos T.)

<sup>68</sup> No original, “property interest”. (N. dos T.)

poderia (1) dar aos indivíduos o direito de propriedade dos dados sobre eles próprios, e assim (2) criar um incentivo para arquiteturas que facilitam o consentimento antes de entregar esses dados<sup>69</sup>.

O primeiro passo vem por meio de uma declaração estatal sobre quem é proprietário de quê<sup>70</sup>. O governo poderia declarar que informações sobre indivíduos obtidas por meio de uma rede de computadores é de propriedade dos indivíduos; outras pessoas só poderiam coletar estas informações e utilizá-las com o consentimento destes indivíduos. A declaração de direitos poderia então ser garantida por uma diversidade de possíveis meios tradicionais. O estado pode criminalizar o furto de tais informações, ou fornecer meios de reparação civil e incentivos para garantir direitos individuais se tais informações forem indevidamente apropriadas.

Esse primeiro passo, contudo, só seria útil se induzisse o segundo — dessa vez, uma mudança na própria arquitetura do espaço, e não apenas nas leis que o governam. Essa mudança na arquitetura teria o objetivo de reduzir os custos da escolha e de facilitar que os indivíduos expressassem suas preferências sobre o uso de dados pessoais e que pudessem ocorrer negociações sobre estes dados. Regimes de propriedade fazem pouco sentido se as transações envolvendo essa propriedade não forem fáceis. E um problema das arquiteturas existentes, repito, é a dificuldade de os indivíduos exercerem o direito de escolha sobre sua propriedade.

Mas há soluções. O Consórcio World Wide Web, por exemplo, desenvolveu um protocolo, chamado P3P<sup>71</sup>, para o controle de dados privados. O P3P permitiria que indivíduos selecionassem suas preferências sobre o intercâmbio de informações privadas, e então permitir que agentes negociassem a comercialização desses dados quando um indivíduo se conectasse a um dado site. Se, por exemplo, eu nunca quisesse visitar um site que registrasse meu endereço de IP e as páginas que eu tivesse visitado, o P3P poderia expressar essa preferência. Quando eu visitasse um site, um agente negociaria com ele sobre minhas preferências de acesso.

O P3P funciona como uma linguagem para expressar preferências sobre dados e como *framework* no interior do qual negociações sobre essas preferências poderiam ser facilitadas. Ele seria, em outras palavras, ser um *framework* dentro do qual indivíduos poderiam mais bem regular suas vidas no ciberespaço<sup>72</sup>.

Mas sem intervenção estatal, não é claro que um tal *framework* seria capaz de se desenvolver. O P3P cria ônus que os sites não assumirão em um mundo onde eles podem obter as mesmas informações de graça. Apenas mudando os incentivos desses sites — negando-lhes

---

<sup>69</sup> Cf. CALABRESI, Guido; MELAMED, A. Douglas. Property Rules, Liability Rules, and Inalienability: One View of the Cathedral. **Harvard Law Review**, v. 85, 1972, pp. 1089, 1092 (argumentando que, quando o estado protege um direito com uma regra de propriedade, “alguém que deseja remover o direito de seu titular deve comprá-lo dele em uma transação voluntária na qual o valor do direito é acordado com o vendedor”)

<sup>70</sup> Há uma questão constitucional importante que estou ignorando aqui — se o estado pode conceder um direito real [*property interest*] sobre “dados” privados.

<sup>71</sup> V. Platform for Privacy Preferences (P3P) Syntax Specification: WJC Working Draft. Disponível em <http://www.w3.org/TR/WD-P3P10-syntax/>.

<sup>72</sup> V. *Developments*, nota 10 *supra*, pp. 1645-1648 (descrevendo o P3P). Minha abordagem considera as soluções tanto do direito quanto do código como inseparavelmente vinculadas. A mudança no direito de propriedade é, na minha visão, necessária para criar os incentivos para a solução de código emergir.

acesso livre a essas informações — é que podemos esperar criar um incentivo suficiente para que eles adotem tecnologias que facilitem a compra. Estabelecer um direito real sobre dados privados criaria um tal incentivo; e seria o governo que então facilitaria esse direito.

Há muitos problemas com o P3P, e existem alternativas que podem funcionar muito melhor<sup>73</sup>. Mas o meu propósito não foi é o de endossar uma solução específica. Meu propósito é o de mostrar a possível necessidade de ação coletiva, até mesmo para simplesmente possibilitar o controle individual. As arquiteturas existentes impossibilitam os incentivos necessários para proteger a privacidade; as arquiteturas existentes beneficiam consumidores de informações privadas, ao passo que impossibilitam a escolha dos indivíduos que fornecem informações privadas. Logo, o sucesso de uma política que possibilite o exercício do direito de escolha requer ação coletiva.

\* \* \*

*3. Conclusões sobre arquitetura e regulabilidade.* — Regulações podem vir de qualquer direção — algumas de cima, outras de baixo. Meu argumento nesta seção foi o de que a regulabilidade de qualquer forma depende da arquitetura do espaço, e que esta arquitetura pode ser alterada.

O código do ciberespaço pode impossibilitar escolhas governamentais, mas o código pode impossibilitar escolhas individuais também. Não existe um alinhamento natural e geral entre regulação de baixo para cima e a arquitetura existente da Internet. Possibilitar escolhas *individuais* pode requerer uma modificação coletiva da arquitetura do ciberespaço, assim como possibilitar escolhas *coletivas* pode requerer modificação desta arquitetura. A arquitetura do ciberespaço é neutra: ela pode possibilitar ou impossibilitar qualquer tipo de escolhas. A escolha sobre qual delas possibilitar, entretanto, não é em nenhum sentido neutra.

#### *B. O código deslocando o direito.*

O argumento até agora é o de que o direito pode alterar as condicionantes do código, de modo que este possa regular comportamentos de maneira diferente. Nesta seção, eu considero a alegação oposta — a de que o código pode alterar as condicionantes do direito, de modo que

---

<sup>73</sup> O P3P tem sido alvo de diversas críticas e preocupações. Primeiramente, o P3P, por si só, não garante que os provedores de serviços de rede cumprirão com os acordos de privacidade alcançados por meio de negociações P3P. V. GREENLEAF, Graham. An Endnote on Regulating Cyberspace: Architecture vs. Law? **University of New South Wales Law Journal**, v. 21, p. 593, 1998, p. 615. Segundo, o P3P pode, na verdade, levar a um aumento na exploração de informações pessoais, permitindo que sites populares condicionem a entrada à revelação de informações altamente pessoais, dando assim aos usuários a opção menos desejável de desistir completamente dos sites ou a de ceder a solicitações de informação excessivamente intrusivos. V. GARFINKEL, Simson L. The Web's Unelected Government. **Technology Review**, Nov.-Dez. 1998, p. 38, 44. Terceiro, o P3P muito provavelmente acarretará o custo social de taxas de acesso aumentadas, uma vez que “muitas das informações pessoais coletadas online são utilizadas para direcionar a publicidade na Internet e, como a publicidade é uma importante fonte de receita para os provedores de sites, o ocultamento de informações pessoais pode limitar a capacidade dos provedores de atrair publicidade e, assim, prejudicar uma importante fonte de receita” (*Developments*, nota 10 *supra*, p. 1648 [notas de rodapé omitidas]). Quarto, “o ocultamento de identidades do espaço real (...) [possibilitadas pelo P3P] pode criar um desincentivo [para usuários da rede] à cooperação, e pode encorajar comportamentos socialmente inconsequentes” (*idem* [notas de rodapé omitidas]). Outra preocupação em relação ao P3P envolve a “questão crítica (...) de quais serão as configurações-padrão fornecidas aos usuários. Poucos usuários de computadores chegam a aprender a alterar as preferências de configurações em seu software. Logo, a forma como um navegador equipado com P3P se configura por padrão é a forma como a maioria da população da Internet vai usá-lo”. (Garfinkel, pp. 44, 46). Há também um número de soluções privadas para o problema da privacidade de dados. Para uma variedade de anonimizadores, infomediárias e servidores e navegadores seguros, v. ONLINE PRIVACY ALLIANCE. **Rules and Tools for Protecting Personal Privacy Online**.

o direito possa (de fato) regular de forma diferente. A chave está na locução adverbial “*de fato*”, pois nos meus exemplos o código não realiza uma mudança real de direito. O direito nos livros permanece o mesmo. Esses são, em vez disso, exemplos de o código alterando a efetividade de uma lei. Eles são, em outras palavras, exemplos de como efeitos indiretos do código podem alterar a regulação ou a política do direito.

Em casos tais, legisladores se deparam com uma escolha. Onde as arquiteturas do código alteram as condicionantes do direito, elas, de fato, deslocam valores no direito. Legisladores deverão então decidir entre reforçar esses valores existentes ou permitir que a alteração ocorra. Nos exemplos que eu seleciono aqui, meu viés é em favor dos valores do direito, embora existam muitos exemplos que vão no outro sentido também. Meu argumento não é o de que o direito deve sempre reagir; frequentemente, o mercado será suficiente. Meu argumento apenas mostra por que pode ser necessário que ele reaja.

Meus exemplos são retirados do direito da propriedade intelectual e do direito dos contratos. Em ambos os exemplos, eu identifico valores de ordem pública que são deslocados pelas arquiteturas emergentes do ciberespaço. Essas arquiteturas, eu argumento, tornam possível um sistema que protege a propriedade individual de modo demasiado perfeito e anula a influência do direito público sobre os contratos de modo demasiado completo. O código, aqui, ameaça deslocar valores jurídicos de ordem pública, forçando uma escolha entre permitir ou não esse potencial deslocamento.

1. *O código deslocando o direito: propriedade intelectual.* — Nós temos leis específicas para nos proteger contra o furto de automóveis ou barcos<sup>74</sup>. Nós não temos leis específicas para nos proteger contra o furto de arranha-céus. Arranha-céus tomam conta deles próprios. A arquitetura do espaço real, ou, mais sugestivamente, seu código do espaço real, protege arranha-céus de modo mais eficiente que o direito. A arquitetura é aliada dos arranha-céus (tornando impossível movê-los); mas é inimiga dos carros e dos barcos (tornando bastante fácil movê-los).

Nesse espectro de carros a prédios muito grandes, a propriedade intelectual é de certa forma parecida com os carros, e bastante diferente de prédios grandes. Com efeito, no mundo atual, a propriedade intelectual se dá muito pior que carros e barcos. Se alguém furta meu carro, pelo menos eu fico sabendo; posso chamar a polícia, e eles podem tentar encontrá-lo. Mas se alguém faz uma cópia ilegal do meu artigo (copiando-o sem pagar por ele), eu não necessariamente fico sabendo. As vendas podem cair, minha reputação pode subir (ou cair), mas não há como rastrear o motivo da queda nas vendas como sendo esse furto individual, nem vincular a subida (ou queda) na fama a essa distribuição subsidiada.

Quando teóricos da Rede começaram a pensar sobre propriedade intelectual, argumentaram que as coisas estavam prestes a se tornar muito piores. “Tudo o que sabemos sobre propriedade intelectual”, nos disseram, “está errado”<sup>75</sup>. A propriedade não poderia ser

---

<sup>74</sup> De acordo com o Código Penal Modelo, no qual muitos códigos penais estaduais são baseados, o furto de automóveis, aviões, motocicletas, lanchas ou “outros veículos de propulsão motorizada” é crime (MODEL PENAL CODE § 223.1(2)(a) (1962)).

<sup>75</sup> BARLOW, John Perry. The Economy of Ideas. *Wired*, Mar. 1994, p. 84.

controlada na Rede; o *copyright* não faria sentido<sup>76</sup>. Autores teriam que encontrar novos meios de ganhar dinheiro no ciberespaço, porque a tecnologia tinha destruído a capacidade de ganhar dinheiro pelo controle de cópias<sup>77</sup>.

As razões disso eram simples: a Rede é um meio digital. Cópias digitais são perfeitas e gratuitas<sup>78</sup>. É possível copiar uma música de um CD em um formato chamado MP3. A música pode então ser postada no USENET para milhões de pessoas de graça. A natureza da Rede, nos disseram, tornariam os controles de *copyright* impossível. O *copyright* estava morto.

Havia algo estranho sobre esse argumento, desde seu nascimento. Ele carregava um certo determinismo tautológico<sup>79</sup>: “o modo como o ciberespaço é é o modo como ele tem que ser”. O ciberespaço era um lugar onde “infinitas cópias podiam ser feitas de graça”. Mas por quê, exatamente? Por causa do seu código. Infinitas cópias podiam ser feitas porque o código permitia sua produção. Então por que o código não poderia ser alterado? Por que não poderíamos imaginar um código diferente, que melhor protegesse a propriedade intelectual?

No começo desse debate, foi necessária verdadeira imaginação para visualizar esses códigos alternativos. Não estava óbvio como uma arquitetura diferente poderia possibilitar um melhor controle sobre objetos digitais. Mas, atualmente, nós já chegamos longe o suficiente para enxergarmos algo dessas alternativas<sup>80</sup>.

Consideremos as propostas de Mark Stefik do Xerox PARC. Numa série de artigos<sup>81</sup>, Stefik descreve o que ele chama de “sistemas de confiança”<sup>82</sup> para gerenciamento de *copyright*. Sistemas de confiança permite aos titulares de uma propriedade intelectual controlar o acesso a essa propriedade, e medir o uso dessa propriedade perfeitamente. Esse controle seria programado em um software que iria distribuir e, assim, regular o acesso a material protegido por *copyright*. Esse controle seria extremamente refinado, e possibilitaria ao detentor do

<sup>76</sup> V. e.g., DYSON, Esther. Intellectual Value. **Wired**, Jul. 1995, p. 136, 138–39. (“Controlar a produção de cópias (...) torna-se um desafio complexo. Ou você controla algo de forma muito rigorosa, limitando sua distribuição a um grupo pequeno e confiável, ou (...) seu produto vai acabar caindo nas mãos de uma grande audiência não pagante — isso se alguém se interessar em tê-lo para começo de conversa”); BARLOW, John Perry. **A Cyberspace Independence Declaration**. Feb. 9, 1996. Disponível em <http://www.eff.org/barlow> (“Seus conceitos jurídicos de propriedade, expressão, identidade, movimento e contexto não se aplicam a nós. Eles são baseados em matéria. Não há matéria aqui”).

<sup>77</sup> Cf. Dyson, nota 68 *supra*, p. 141 (sugerindo, por exemplo, que na era da Internet, “empresas de software bem-sucedidas estão adotando modelos de negócios em que são recompensadas por serviços, em vez de por código”; e que “o valor real criado pela maioria das empresas de software reside em suas redes de distribuição, bases de usuários treinadas e marcas — não em seu código”).

<sup>78</sup> V. NEGROPONTE, Nicholas. **Being Digital**. 1995, p. 58 (“No mundo digital, não apenas a facilidade [de fazer cópias] está em questão, mas também o fato de que a cópia digital é tão perfeita quanto o original e, com alguns cálculos sofisticados, até melhor”); Barlow, nota 67 *supra* (“No nosso mundo, qualquer coisa que a mente humana possa criar pode ser reproduzida e distribuída infinitamente sem custo”); Dyson, nota 68 *supra*, p. 137 (“[A Rede] nos permite copiar conteúdo essencialmente de graça...”); KHADDER, Nicholas. Project. **Annual Review of Law and Technology, Berkeley Technology Law Journal**, v. 13, p. 3, 1998, p. 3 (“Recentemente, por exemplo, a Internet permitiu aos usuários distribuir e vender informações de maneira muito ampla a um custo marginal desprezível para o distribuidor”).

<sup>79</sup> No original, “*is-ism*”. (N. dos T.)

<sup>80</sup> V. *Developments*, nota 10 *supra*, pp. 1650-1651 (descrevendo “containers de gerenciamento de direitos” como uma dessas alternativas).

<sup>81</sup> STEFIK, Mark. Letting Loose the Light: Igniting Commerce in Electronic Publication. In: **Internet Dreams: Archetypes, Myths, and Metaphors**, p. 219, 226–27. 1996; STEFIK, Mark. Shifting the Possible: How Trusted Systems and Digital Property Rights Challenge Us to Rethink Digital Publishing. **Berkeley Technology Law Journal**, v. 12, p. 137, 1997, pp. 139–407 (doravante, Stefik, “Shifting the Possible”); STEFIK, Mark. Trusted Systems. **Scientific American**, Mar. 1997, p. 78, 78–81.

<sup>82</sup> No original, “trusted systems”. (N. dos T.)

*copyright* um controle extraordinário sobre materiais protegidos.

Pense nele dessa forma: hoje, quando você compra um livro, você tem o “direito” de fazer uma série de coisas com esse livro. Você pode lê-lo uma vez, ou cem vezes. Você pode emprestá-lo a um amigo. Você pode tirar Xerox de algumas páginas dele, ou escaneá-lo e salvá-lo em seu computador. Você pode queimá-lo. Você pode usá-lo como peso de papel. Você pode vendê-lo. Você pode guardá-lo na sua estante e nunca o abrir nenhuma vez.

Algumas dessas coisas você pode fazer porque o direito lhe dá o direito de fazê-las — você pode vender o livro, por exemplo, porque o direito de *copyright* explicitamente lhe dá esse direito<sup>83</sup>. Algumas dessas coisas você pode fazer simplesmente porque ninguém pode impedi-lo. Um livreiro pode lhe vender um livro a um preço se você prometer lê-lo uma vez, e a um preço diferente se você quiser lê-lo cem vezes. Mas não existe nenhuma maneira de o livreiro saber se você obedeceu ao contrato. Em princípio, o livreiro poderia incluir um policial em cada livro, para que ele seguisse você por aí para se certificar de que você usou o livro como prometido. Mas os custos disso são simplesmente proibitivos. O livreiro está de mãos atadas.

Mas e se cada um desses direitos pudesse ser controlado, e cada um deles destacado e vendido separadamente? É dizer: e se um software pudesse regular se você pode ler o livro uma vez ou vem vezes; se você pode copiar e colar seu conteúdo ou apenas ler sem copiar; se você pode enviá-lo como documento anexo para um amigo, ou apenas mantê-lo na sua máquina; se você pode deletá-lo; se você pode usá-lo em outro trabalho, para outro propósito; ou se você pode simplesmente deixá-lo na sua estante?

Stefik descreve uma rede na qual esse destacamento de direitos é possível. Ele oferece uma arquitetura para a rede que permitiria aos proprietários de materiais protegidos por *copyright* vender acesso a esses materiais com condições estabelecidas por eles, e uma arquitetura que garantiria o cumprimento desses contratos.

Os detalhes do sistema não são importantes aqui<sup>84</sup>. A essência é simples o suficiente para entender. Objetos digitais seriam distribuídos dentro de protocolos que são sobrepostos sobre os protocolos básicos da Rede. Esse sistema mais sofisticado funcionaria interagindo seletivamente com outros sistemas. Assim, um sistema que controlasse acesso desse modo mais refinado só concederia acesso aos seus recursos a outro sistema que também controlasse acesso do mesmo modo refinado. Uma hierarquia de sistemas se desenvolveria; e materiais protegidos seriam comercializados apenas dentro desse sistema que controla acesso adequadamente.

Stefik transformou aviões em arranha-céus — ele descreveu uma forma de alterar o código do ciberespaço para tornar possível proteger propriedade intelectual de maneira muito mais eficaz do que é possível no espaço real.

Agora imagine por um momento que uma estrutura de sistemas de confiança emergisse. Como essa mudança no código alteraria a natureza do direito de *copyright*?

O direito de *copyright* é um bicho esquisito. Ele estabelece um tipo estranho de propriedade, pelo menos em relação a outras propriedades. A Cláusula de *Copyright* da Constituição dos Estados Unidos dá ao Congresso o poder de conceder aos “Autores” o direito

<sup>83</sup> V. 17 U.S.C. § 109 (1994).

<sup>84</sup> Para os detalhes técnicos, v. Stefik, “Shifting the Possible”, citado acima na nota 81, pp. 139-144.

sobre suas “Obras” por “Tempos limitados”<sup>85</sup>. No final desse tempo, o direito se torna não-exclusivo. A obra entra no domínio público. É como se o direito que você tem sobre seu carro fosse um arrendamento, que se estenderia por quatro anos, e depois expiraria, tornando seu carro disponível para quem quisesse pegar.

As razões dessa limitação da proteção por *copyright* são muitas, embora não se sobreponham completamente. Algumas razões são econômicas, e, em última análise, pragmáticas. Sistemas de propriedade (custosos e complexos) só são justificados se produzirem algum bem social. No caso de bens corpóreos, o bem social é óbvio. O direito protege o uso e o gozo de minha propriedade sobre bens corpóreos, como meu carro. Se você o usasse sem minha permissão, eu não poderia usá-lo. Se todo mundo pudesse usá-lo sem minha permissão, eu não teria muita razão para ser seu proprietário. Ao me dar o poder de controlar seu uso, o direito cria um benefício para meu domínio, e, por conseguinte, um incentivo para que eu busque o domínio.

Bens intangíveis são significativamente diferentes. Diferentemente do seu usufruto sobre meu carro, seu usufruto sobre meu poema não interferirá sobre o meu de maneira nenhuma. Bens intangíveis são não-rivais. Quando uma ideia é difundida, sua utilidade não diminui. Como escreveu Thomas Jefferson: “ninguém possui menos porque todos os outros possuem o todo. Aquele que recebe de mim uma ideia, recebe ele próprio instrução sem diminuir a minha; assim como aquele que acende sua vela na minha recebe luz sem me obscurecer”<sup>86</sup>. Assim, enquanto o direito precisa proteger a propriedade tangível tanto para que exista incentivo a sua produção, quanto para que o proprietário possa dela usufruir, ele precisa proteger a propriedade intangível apenas a fim de criar o incentivo a sua produção.

Mas a economia não é a única justificativa para limitar a proteção da propriedade intelectual “como se fosse propriedade”. O direito constitucional é outra<sup>87</sup>. Regulações de *copyright* são regulações de liberdade de expressão. O direito de *copyright* dá ao proprietário do *copyright* o poder de controlar não apenas cópias exatas, mas também obras derivadas e execuções de algumas obras. Essas regulações de expressão estão em tensão com a compreensão de que o direito deve manter a expressão livre. Um meio-termo é encontrado no conceito de *copyright* restrito — que protege uma obra até o limite necessário para induzir a criação, mas não mais que isso. Como a Suprema Corte disse no caso *Harper & Row, Publishers, Inc. v. Nation Enterprises*<sup>88</sup>, os Constituintes pretendiam que o *copyright* servisse como um “motor da livre expressão”<sup>89</sup>. Ele só é justificado conquanto sirva como tal motor.

Finalmente, e de modo relacionado, os limites sobre a propriedade intelectual refletem um compromisso com um domínio comum intelectual<sup>90 91</sup>. É verdade que alguns bens de

<sup>85</sup> Art. I, § 8, cl. 8, da Constituição dos EUA.

<sup>86</sup> Carta de Thomas Jefferson para Isaac M’Pherson (13 ago. 1813), in JEFFERSON, Thomas. **The Writings of Thomas Jefferson**. H.A. Washington ed., 1854, pp. 175, 180.

<sup>87</sup> Para fins de transparência, estou atualmente representando um cliente *pro bono* em uma causa que levanta a questão das limitações da Primeira Emenda sobre a Cláusula de Copyright. V. *Eldred v. Reno*, No. 1:99CV00065 (D.D.C. 1999).

<sup>88</sup> 471 U.S. 539 (1985).

<sup>89</sup> *Idem*, p. 558.

<sup>90</sup> No original, “*intellectual commons*”. (N. dos T.)

<sup>91</sup> V. BENKLER, Yochai. Free as the Air to Common Use: First Amendment Constraints on Enclosure of the Public Domain. **New York University Law Review**, v. 74, p. 354, 1999, pp. 360–63; LANGE, David. Recognizing the Public Domain.

domínio comum enfrentam tragédias<sup>92</sup>. Mas uma vez que o problema do incentivo é solucionado, o domínio comum intelectual não precisa mais enfrentá-las. As limitações ao escopo do direito da propriedade intelectual servem para fomentar esse domínio comum intelectual — gerando um recurso que possa ser colhido por outros como insumo<sup>93</sup>.

A natureza essencial de um domínio comum é a de que qualquer indivíduo é livre para usá-lo sem a permissão de mais ninguém<sup>94</sup>. Ou, mais especificamente, um bem é de domínio comum se um indivíduo está livre de qualquer julgamento, seja ele discricionário, baseado em conteúdo ou em perspectiva, sobre se o bem pode ou não ser usado. Eu posso ter que pagar uma pequena taxa para entrar num parque, mas, se eu pago a taxa, tenho o direito de entrar. O parque é um recurso aberto a todos. É um espaço que os indivíduos podem ocupar sem pedir a permissão subjetiva de mais ninguém<sup>95</sup>.

Essas três justificativas para os limites sobre a propriedade intelectual se sobrepõem, mas não são coextensivas. Todas elas, por exemplo, justificariam alguma forma de “*fair use*” — uma defesa que o direito de *copyright* dá aos usuários de material protegido<sup>96</sup>.

De uma perspectiva econômica, o *fair use* pode ser justificado seja porque o uso é pequeno em relação aos custos de transação de cobrar por ele, seja porque certos usos tendem a aumentar a demanda em geral por trabalhos protegidos. O direito de usar excertos na resenha de um livro beneficia a classe dos autores de livros em geral, uma vez que possibilita resenhas de livros, que, por sua vez, aumentam a demanda total por livros<sup>97</sup>.

De uma perspectiva de liberdade de expressão, o alcance de uma justificação para o *fair use* dependeria do conteúdo em questão. Melville Nimmer, por exemplo, levantou um caso hipotético no qual os interesses protegidos pela Primeira Emenda justificariam o *fair use* além

---

**Law and Contemporary Problems**, v. 44, Autumn 1981, p. 157, pp. 175–76, 178 (comparando a propriedade intelectual a um terreno que pode ser prejudicado pela colonização); LITMAN, Jessica. The Public Domain. *Emory Law Journal*, v. 39, 1990, pp. 965, 967, 1023 (observando que o “domínio público é a principal salvaguarda da matéria-prima que torna a autoria possível” e, assim, “permite que a lei de direitos autorais evite um confronto com a pobreza de algumas das premissas sobre as quais se baseia”).

<sup>92</sup> V. HARDIN, Garrett. The Tragedy of the Commons. *Science*, v. 162, p. 1243, 1968. Republicado em ELLICKSON, Robert C.; ROSE, Carol M.; ACKERMAN, Bruce A. (eds.). **Perspectives on Property Law**. 2. ed., 1995, p. 132, 133.

<sup>93</sup> V. LEMLEY, Mark A. The Economics of Improvement in Intellectual Property Law. *Texas Law Review*, v. 75, p. 989, 1997, pp. 1083–1084 (argumentando que “a propriedade intelectual representa um ‘equilíbrio delicado’ entre os direitos dos titulares de propriedade intelectual e os direitos dos usuários, incluindo a próxima geração de titulares”, e que certas limitações aos direitos dos titulares de propriedade intelectual são, portanto, necessárias para incentivar melhorias); Litman, nota 91 *supra*, p. 968 (“O domínio público deve ser compreendido não como o domínio de materiais que não merecem proteção, mas como um dispositivo que permite que o restante do sistema funcione deixando a matéria-prima da autoria disponível para os autores usarem”); McJOHN, Stephen M. Fair Use and Privatization in Copyright. *San Diego Law Review*, v. 35, n. 32, 1998, pp. 61, 66 (“O domínio público é, por si só, um recurso fundamental para a produção adicional de obras criativas”).

<sup>94</sup> V., *e.g.*, Hardin, nota 92 *supra*, pp. 133–134.

<sup>95</sup> V. Benkler, nota 91 *supra*, pp. 360–364.

<sup>96</sup> V. 17 U.S.C. § 107 (1994). O *fair use* garante que os usuários de material protegido por *copyright* tenham o direito de utilizar esse material de forma limitada, independentemente da vontade do titular do *copyright*. Assim, por exemplo, posso fazer uma paródia de uma obra protegida por *copyright*, mesmo que o autor discorde. Para uma discussão sobre os limites da paródia como *fair use*, v. KAPLAN, Lisa Moloff. Parody and the Fair Use Defense to Copyright Infringement: Appropriate Purpose and Object of Humor. *Arizona State Law Journal*, v. 26, 1994, p. 857, 864–82. V. também McJohn, nota 93 *supra*, pp. 86–87, 94–95 (usando a aplicação pela corte da tese da paródia como *fair use* para embasar um argumento de que o escopo do *fair use* é mais amplo do que apenas o de uma solução para o alto custo de transação para o licenciamento).

<sup>97</sup> V. POSNER, Richard A. **Law and Literature**. 2. ed., 1998, p. 407; LANDES, William M.; POSNER, Richard A. An Economic Analysis of Copyright Law. *Journal of Legal Studies*, v. 18, 1989, pp. 325, 358–59.

do escopo fornecido pelo direito de *copyright*<sup>98</sup>.

Porém, da perspectiva do domínio comum, o que é importante sobre o *fair use* não é tanto o valor do *fair use*, ou sua relação com questões de interesse público. O que é importante é o direito de usar sem permissão. Esta é uma concepção de autonomia. O direito garantido é o direito de usar esses recursos sem a aprovação de outra pessoa.

O "*fair use*", assim, sopesa os direitos de um autor individual contra os direitos de um usuário sob qualquer das justificativas para o direito de *copyright*. Mas está claro, repito, independentemente da justificativa, que o desenvolvimento de sistemas de confiança ameaça alterar esse sopesamento. Da perspectiva econômica, ele ameaça empoderar autores individuais contra os interesses da classe; da perspectiva constitucional, ele ameaça limitar a livre expressão independentemente de sua relação com questões de interesse público; e, da perspectiva do domínio comum, ele fundamentalmente altera a natureza do acesso. No interior de uma estrutura de sistemas de confiança, o acesso se dá sempre e apenas mediante permissão. O parâmetro de base é o controle, independentemente de até que ponto esse controle seja exercido.

Este é um problema específico do ciberespaço. No espaço real, o direito pode me garantir o direito ao *fair use*, ou de fazer uso de uma obra em domínio público. Ele me garante esse direito me dando uma defesa se o proprietário de uma obra protegida por *copyright* tentar me processar por apropriação de sua propriedade. O direito, nesse caso, produz o efeito de negar ao proprietário qualquer ganho de causa; o direito retira sua proteção, e deixa a propriedade no domínio comum.

Mas não há garantia similar quanto a propriedade protegida por sistemas de confiança<sup>99</sup>. Não há nenhum motivo para acreditar que o código que Stefik descreve garantiria o *fair use*, ou um termo limitado para a proteção. No lugar disso, o código dos sistemas de confiança poderia muito bem proteger materiais de modo absoluto, ou protegê-los por termo ilimitado<sup>100</sup>. O código não precisa ser ponderado do modo que o direito de *copyright* é. O código pode ser projetado como seu programador quiser, e programadores têm pouco incentivo para tornar seu produto imperfeito<sup>101</sup>.

Sistemas de confiança, então, são formas de direito privatizado. Eles são arquiteturas de controle que deslocam as arquiteturas de controle vigorantes pelo direito estatal. E, na medida em que arquiteturas de direito sopesam valores privados e públicos, equilibrando-os, deveríamos nos preocupar se arquiteturas de código desequilibram esse sopesamento, respeitando valores privados em detrimento dos públicos.

---

<sup>98</sup> V. NIMMER, Melville B. Does Copyright Abridge the First Amendment Guarantees of Free Speech and Press? **UCLA Law Review**, v. 17, 1970, pp. 1180, 1197-98 (argumentando que a Primeira Emenda protegeria a reprodução de fotografias do massacre de My Lai, mesmo que proibida pela lei de *copyright*); v. também *Triangle Publications, Inc. v. Knight-Ridder Newspapers, Inc.*, 626 F.2d 1171, 1184 (5th Cir. 1980) (argumentando que "sob circunstâncias limitadas, um privilégio da Primeira Emenda pode e deve existir quando a utilização da expressão protegida por *copyright* é necessária para transmitir pensamentos ou expressões").

<sup>99</sup> V. Stefik, *Shifting the Possible*, nota 72 *supra*, pp. 139-141.

<sup>100</sup> *Idem*, p. 147.

<sup>101</sup> V. *Developments*, nota 10 *supra*, pp. 1649-1656 (descrevendo possíveis problemas com uma solução de código para a violação de *copyright* e argumentando que, embora o governo não deva intervir em tais soluções até que os problemas se tornem evidentes, ações legislativas são apropriadas se as soluções de código efetivamente perturbarem o equilíbrio da lei de *copyright*).

É impossível prever em abstrato se esse será o resultado dos sistemas de confiança. Há bons motivos para crer que sim, e pouco que sugira o contrário. Mas meu objetivo aqui não é prever; meu objetivo é isolar uma resposta. Se o direito privatizado deslocar valores públicos, o público deveria fazer alguma coisa?

2. *O código deslocando o direito: “contratos”*. — Sistemas de confiança são um exemplo de deslocamento do direito pelo código. Um segundo é o direito dos contratos. Tem havido bastantes discussões na literatura sobre o ciberespaço acerca de como, em essência, o ciberespaço é um lugar onde o “contrato”, em vez da “lei”, vai governar o comportamento das pessoas<sup>102</sup>. A AOL, por exemplo, requer que você informe seu nome para entrar no sistema. Isso é “como” um contrato, dizem esses teóricos<sup>103</sup>, uma vez que você está limitado por um conjunto de condicionantes com as quais concordou quando assinou o serviço da AOL. É como se você simplesmente promettesse se identificar quando entrasse na AOL, e quando não se identificasse, a AOL então teria pretensão pela quebra do contrato. É um “como se”, só que melhor: a obrigação é imposta e exigida mais eficientemente do que se fosse imposta e exigida por meio do direito contratual.

Como professor de contratos, eu acho essas alegações estranhas. Pois condicionantes de código sozinhas *não* são “contratos”. Claro elas são “como” contratos, no sentido de que ambos são condicionantes autoimpostas, mas “ser como” não é “ser”. Um “leão” é como um “gato”, mas seria tolice deixar seu filho brincar com um leão. Então, seria igualmente tolo presumir que os contratos-código são igualmente benignos.

A diferença é a seguinte: para cada contrato executado — para cada acordo que subseqüentemente requer que um terceiro obrigue ao cumprimento dos termos desse acordo —, existe um juízo, feito por um terceiro, sobre se o cumprimento daquela obrigação deve ser exigido. Em geral<sup>104</sup>, esses juízos são feitos pelo Judiciário. E quando um órgão judicial faz um desses juízos, ele considera não apenas as regras privadas contraídas pelo negócio jurídico, mas também questões de ordem pública, que podem, em alguns contextos, derrogar essas regras privadas. Quando o Judiciário processa a execução de um contrato, ele decide até onde seu poder pode ser usado para forçar o cumprimento do acordado. Às vezes, o contrato será cumprido integralmente; mas, frequentemente, os acordos não poderão ser totalmente efetivados. Questões como impossibilidade ou erro poderão exonerar certas obrigações. Regras sobre meios executivos limitarão os meios que as partes poderão empregar. Exceções de ordem pública condicionarão os tipos de negócios jurídicos que poderão ser executados. “Contratos” incorporam todas essas regulações, e é a mescla desse conjunto de valores de ordem pública e obrigações privadas que, juntos, produzem o que chamamos de “um contrato”.

Quando o código executa um acordo, contudo, ou quando o código efetiva uma

---

<sup>102</sup> V. HARDY, Trotter. Property (and Copyright) in Cyberspace. **University of Chicago Legal Forum**, 1996, p. 217, 237 (concluindo que “o ciberespaço deveria ser pelo menos tão, se não mais, propício para a transação de direitos reais quanto o espaço ‘real’”); NIMMER, Raymond T. Article 2B: An Introduction. **Marshall Journal of Computer and Information Law**, v. 16, 1997, p. 211, 220 (argumentando que contratos devem reger transações sobre informações digitais porque “a regulação [legislativa ou judicial] de termos é norma de direito contratual contratual inaceitável na era da informação”).

<sup>103</sup> Cf. Nimmer, *op. cit.*, p. 228-231, 234-235 (1997) (recomendando alterações na lei de contratos que tornariam esses tipos de acordos contratos exequíveis).

<sup>104</sup> Claro, existem duas exceções importantes aqui que ainda não analisei — acordos de arbitragem e práticas alternativas de resolução de disputas.

condicionante autoimposta, esses valores de ordem pública não necessariamente entram nessa mescla <sup>105</sup>. Consequências às quais o Judiciário pode oferecer resistência (medidas expropriatórias, por exemplo <sup>106</sup>) podem ser impostas pelo código sem hesitação. O programador do código opera livre das limitações implícitas do direito contratual. Ele pode construir um regime alternativo para exigir o cumprimento de condicionantes voluntárias. E nada requer ou garante que esse regime alternativo será compatível com os valores do regime geral de fundo a que chamamos “contrato”.

Isto não é necessariamente uma crítica às condicionantes autoimpostas do código. A maioria delas é, sem dúvida, inofensiva; e provavelmente seria exequível se fosse traduzida para contratos reais.

No entanto, é, sim, resistir à implicação oposta — de que, se essas obrigações são “como” contratos”, então elas são tão imunes a questionamentos quanto as obrigações equivalentes no espaço real, constituídas por contratos.

Pois, mais uma vez, no espaço real, alguém poderia muito bem acreditar que um conjunto de obrigações impostas por contrato não seria controvertido. Condiçoadas pelo direito concorrencial, limitadas por princípios de equidade, balizadas pelas normas de validade e eficácia — as obrigações seriam checadas por um órgão judicial antes de suas condicionantes serem efetivadas. Há uma checagem de segurança estrutural em obrigações desse tipo, o que garante que elas não irão longe demais. Quando intervém para forçar o cumprimento dessas obrigações, o Judiciário empregaria a coleção de ferramentas que o direito contratual desenvolveu para modificar ou abrandar obrigações que, em outras circunstâncias, o direito contratual poderia efetivar.

O análogo do ciberespaço não tem uma caixa de ferramentas equivalente. Suas obrigações não são condicionadas pelos valores de ordem pública que o direito contratual abarca. Em vez disso, suas obrigações fluem automaticamente das estruturas impostas no código. Essas estruturas servem os fins privados do programador do código; são uma versão privada de direito contratual. Porém, segundo os realistas jurídicos passaram uma geração ensinando, e costumamos esquecer: direito contratual é direito *público*. “Direito público privado” é paradoxal<sup>107</sup>.

Em certa medida, esse argumento sobre contratos é o mesmo que o argumento sobre *copyright*. Em ambos os contextos, o *direito* atende a valores de ordem pública; em ambos os contextos, um regime privatizado para estabelecer uma proteção relacionada é efetivado; em ambos os contextos, devemos questionar se esse substituto deveria ser autorizado a deslocar

---

<sup>105</sup> Minha alegação não é a de que cumprir compromissos semelhantes a contratos sempre envolve valores devidamente considerados públicos. Não acredito que seja levantada uma questão constitucional toda vez que meu filho troca a tarefa de lavar a louça com minha filha. Mas, dada a extensão do comércio afetado por transações na Internet, o fato de alguns contratos serem realmente “privados” não significa que os contratos no ciberespaço sejam geralmente “privados”.

<sup>106</sup> V. RESTATEMENT (SECOND) OF CONTRACTS: EXCUSE OF A CONDITION TO AVOID FORFEITURE § 229 (1979).

<sup>107</sup> Esta é uma visão comum. Para uma amostra desses argumentos, v. COHEN, Morris R. The Basis of Contract. **Harvard Law Review**, v. 46, 1933, p. 553, 585–92; COHEN, Morris R. Property and Sovereignty. **Cornell Law Quarterly**, v. 13, 1927, p. 8, 21–30; HALE, Robert L. Bargaining, Duress, and Economic Liberty. **Columbia Law Review**, v. 43, 1943, p. 603, 626–28; HALE, Robert L. Coercion and Distribution in a Supposedly Non-Coercive State. **Political Science Quarterly**, v. 38, 1923, p. 470, 488–91.

esses valores de ordem pública.

Minha resposta em ambos os casos é não. Na medida em que essas estruturas de código deslocam valores de direito público, o direito público tem uma razão para intervir no sentido de restaurar esses valores de ordem pública. Se e como deve fazê-lo é outra questão. Meu argumento até aqui é apenas sobre identificar uma razão para fazê-lo.

### C. O direito regulando o código

Meus exemplos da última seção foram de situações nas quais o código deslocaria valores intrínsecos ao direito. Os exemplos desta seção são de situações familiares nas quais o direito pode deslocar valores no código. Esses dois conjuntos de exemplos sugerem um argumento mais geral: modalidades competem. Os valores implícitos numa dada modalidade de condicionantes, ou numa dada instância dessa modalidade, pode competir com os valores de uma modalidade de condicionantes diferente. Essa competição pode induzir uma resposta. À medida que o código desloca o direito, o direito pode reagir no sentido de recuperar os valores deslocados. À medida que o direito regula o código, programadores podem reagir no sentido de neutralizado o efeito do direito<sup>108</sup>. Cada modalidade funciona como uma espécie de soberania. Cada soberania compete com as outras.

Eu já esbocei alguns exemplos dessa competição. Existem mais exemplos do direito regulando o código.

*Telefone digital:* Quando as redes de telefone se tornaram digitais, os governos perderam uma importante capacidade de interceptar telefones; a arquitetura da rede digital dificultou as interceptações, mas o governo simplesmente reagiu tornando obrigatória uma arquitetura diferente, com um *design* diferente<sup>109</sup>.

*Tecnologia de áudio digital:* DAT é um código que faz cópias digitais de áudio digital. Essas cópias digitais são, em princípio, perfeitas e ilimitadas. Assim, o código dificulta o controle de cópias. O Congresso respondeu com regulações que requeriam que o código limitasse o número de cópias seriais que poderia fazer e reduzir a qualidade se o número de cópias excedesse determinado limite<sup>110</sup>.

*Anti-evasão:* Sistemas de confiança, como já descrevi, são sistemas que possibilitam o controle sobre a distribuição de objetos digitais por meio de tecnologias de criptografia que dificultam o uso não autorizado. Essas tecnologias, contudo, não são perfeitas; existem códigos capazes de “crackear-las”<sup>111</sup>. Assim, a ameaça desses códigos é uma ameaça a esses sistemas de controle. Ano passado, o Congresso reagiu a essa ameaça incluindo dispositivo antievasão no

<sup>108</sup> Por exemplo, os escritores de código podem disponibilizar seu código como código aberto, consulte infra nota 105, ou podem publicar as interfaces de programação de aplicativos (APIs) relevantes que facilitam a evasão à regulamentação estatal.

<sup>109</sup> V. Communications Assistance of Law Enforcement Act (CALEA), Pub. L. No. 103-414, 108 Stat. 4279 (codificada em 47 U.S.C. §§ 1001–1010) (exigindo que empresas de telefonia selecionem uma arquitetura de rede que facilite a interceptação telefônica).

<sup>110</sup> V. Audio Home Recording Act, 17 U.S.C. § 1002 (1994) (descrevendo a exigência de conformidade com um sistema que limita a produção de cópias em série); v. também U.S. DEPARTMENT OF COMMERCE, **Intellectual Property and the National Information Infrastructure: The Report of the Working Group on Intellectual Property Rights**. 1995, pp. 189–190.

<sup>111</sup> Um *crack* é um software que “quebra” um regime de proteção embutido em um programa. No Brasil, tornou-se comum o verbo “crackear” para se referir ao uso de um *crack*. (N. dos T.)

*Digital Millenium Copyright Act*<sup>112</sup>. Esse dispositivo torna crime “crackear” um regime de proteção, mesmo se o uso do material subjacente não seja, em si, uma violação de *copyright*<sup>113</sup>.

*V-Chip*: O V-Chip modifica o código de transmissões de televisão para facilitar discriminação *ex ante* nos programas disponíveis para exibição. Antes do V-Chip, o código de televisão era incapaz de discriminar automaticamente com base no conteúdo do programa. Esse código dificultava que pais exercessem controle sobre o que seus filhos assistiam. O Congresso reagiu requerendo o uso de um código de televisão que possa reconhecer e bloquear conteúdo com base nas classificações indicativas geradas pelo mercado<sup>114</sup>.

*Criptografia*: O governo conduziu uma longa campanha para limitar o acesso a tecnologias de criptografia por medo de que elas tornassem fácil demais a ocultação de provas de crime. Para tratar do problema de mensagens indescritografáveis, o Congresso flertou com a ideia de regular códigos de criptografia diretamente. Em setembro de 1997, a Comissão de Comércio da Câmara de Representantes ficou a um voto de recomendar uma legislação que teria requerido que as tecnologias de criptografia permitissem às autoridades interceptar e descriptografar informações protegidas pela tecnologia<sup>115</sup>.

Esses exemplos mostram que as arquiteturas do ciberespaço podem efetivar ou tornar sem efeito os valores implícitos ao direito; o direito, ao atuar sobre as arquiteturas do ciberespaço, pode efetivar ou tornar sem efeito os valores implícitos no código. A medida que um desloca o outro, uma competição poderia se desenvolver. Programadores podem desenvolver códigos que desloquem o direito; legisladores podem reagir com normas que desloquem códigos.

O Código da Costa Leste (escrito em Washington, publicado no Código de Leis dos Estados Unidos) pode, assim, competir com o Código da Costa Oeste (escrito no Vale do Silício, ou em Redmond, publicado em bits gravados em plástico). Da mesma forma, os autores do Código da Costa Leste podem cooperar com os autores do Código da Costa Oeste. Não está claro qual dos códigos devemos temer mais<sup>116</sup>. O conflito desloca valores em ambas as esferas, mas a cooperação também ameaça valores.

Meu objetivo neste ensaio não é o de esgotar todo o espectro dessas interações<sup>117</sup>. Tampouco é o de prever qual dos lados prevalecerá. Em vez disso, meu objetivo aqui é usar o cenário descrito até aqui para sugerir as lições que devem ser aprendidas a partir de um cenário

<sup>112</sup> Digital Millennium Copyright Act § 1201, Pub. L. No. 105-304, 112 Stat. 2860, 2863–72 (1998).

<sup>113</sup> Idem.

<sup>114</sup> V. Implementação da Seção 551 do Telecommunications Act de 1996, 6, Video Programming Ratings, Federal Communications Commission, 13 F.C.C.R. 8232 (1998); Technical Requirements to Enable Blocking of Video Programming Based on Program Ratings, Federal Communications Commission, 13 F.C.C.R. 11248 (1998).

<sup>115</sup> V. Security and Freedom Through Encryption (SAFE) Act, H.R. 695, 105th Cong. (1997).

<sup>116</sup> Fiz uma importante simplificação nesta análise, que não faço em outros escritos. V. LESSIG, Lawrence. The Limits in Open Code: Regulatory Standards and the Future of the Net. *Berkeley Technology Law Journal*, v. 14, p. 759, 1999. Minha suposição é a de que esses programadores — os alvos dessa regulamentação estatal — estão escrevendo código fechado, em oposição a código aberto. O código fechado é um código que não viaja com seu código-fonte, e não é facilmente modificado. Se um padrão ou protocolo estiver incorporado a este código fechado, é improvável que os usuários ou adotantes desse código consigam desfazer esse padrão. O código aberto é diferente. Se o governo determinasse um determinado padrão ou protocolo dentro de um design de software de código aberto, os usuários ou adotantes sempre estariam livres para aceitar ou rejeitar a porção do design do governo. Assim, se o espaço de aplicação é primariamente software de código aberto, o poder regulatório do estado é diminuído.

<sup>117</sup> V. idem, p. 767-768 (detalhando o conflito).

mais completo.

Esse conflito entre código e direito deve nos compelir a considerar princípios. Deveríamos pensar melhor sobre os valores que devem guiar, ou balizar, esse conflito entre autoridades. Na última parte a seguir, pretendo esboçar dois princípios. Estes não são, de maneira nenhuma, os únicos princípios que nos devem concernir; eles simplesmente são os dois cujos remédios parecem menos óbvios. E eles são dois princípios que podem nos mostrar algo sobre o que um direito do ciberespaço pode ensinar de maneira mais geral.

### III. Lições

Até aqui, esbocei a história de uma inevitável competição entre um conjunto de valores almejados pelo direito, e um conjunto de valores vigente no interior de uma arquitetura específica do código. Minha alegação não é a de que os valores de qualquer um dos dois sejam totalmente pretendidos por qualquer pessoa ou instituição, nem de que eles sejam consistentemente compreendidos. Porém, independentemente de que esses valores serem pretendidos e de quão incompletamente sejam compreendidos, eles inevitavelmente entrarão em conflito. Esse conflito frequentemente induzirá uma resposta — frequentemente pelo direito, pelo menos, e às vezes por arquitetos de código. Minha alegação é a de que podemos aprender algo dessa resposta.

Nesta seção final, quero sugerir três lições que emergem dessa competição. A primeira é uma lição sobre limites ao poder do direito de regular o código. Não apenas comportamento são mais reguláveis sob algumas arquiteturas do que sob outras, mas as próprias arquiteturas podem ser mais ou menos reguláveis. A diferença é menos uma função do código do que de *design* organizacional. Como irei argumentar, o modo como o código é *possuído* vai afetar a capacidade de regulá-lo.

Essa lição ecoa um argumento conhecido de filosofia política, com sinal invertido. Na filosofia política, o argumento é o de que a propriedade é um freio para a ação do estado; no contexto do ciberespaço, meu argumento é o oposto.

A segunda lição é sobre transparência. Faz muito tempo que é um valor de regimes constitucionais liberais o de que a regulação seja transparente. A escolha entre regular por meio do direito e regular por meio de código põe uma pressão extraordinária sobre esse valor. Como outros já anotaram, mas o ciberespaço tornará sistematicamente mais aparente, a não transparência pode ser um aliado efetivo para a regulação. O ciberespaço tornará a não transparência uma opção constante.

Por fim, a terceira lição é sobre ajuste. Há apenas alguns poucos contextos no direito constitucional em que o estado deve fazer ajustes finos em sua regulação para um dado fim estatal. Leis envolvendo liberdade de expressão e direitos da personalidade são dois exemplos primários. Mas o ciberespaço tornará muito mais saliente a preocupação sobre o escopo de uma regulação que em outro contexto seria legítima. A regulação de arquiteturas é sensível e fundamental, muito como a regulação de engenharia genética. Mexer com essas questões é algo que ramifica.

#### A. Os limites da regulabilidade

Eu argumentei que o ciberespaço não é inerentemente irregular; que sua regulabilidade se dá em função de seu *design*. Alguns *designs* tornam comportamentos mais reguláveis; outros tornam comportamentos menos reguláveis. O estado, aleguei, pode influenciar o *design* do ciberespaço de maneiras que aumentam a capacidade estatal de regular.

Há um limite cada vez mais significativo ao poder regulatório do estado. De maneira peculiar, o poder depende de quem tem o domínio sobre o código. Na medida em que o “espaço de aplicação” do código do ciberespaço é privado — no sentido que descreverei adiante — o poder do estado é aumentado. Na medida em que o “espaço de aplicação” do código do ciberespaço não é privado, mas sujeito a um “domínio comum”, o poder do estado é reduzido.

Por privado, quero dizer que o “espaço de aplicação” é desenvolvido da forma como a maioria dos códigos comerciais é atualmente projetada. Empresas de *software* projetam esses códigos e os vendem num pacote completo. O produto que elas licenciam não contém o código-fonte. A licença não dá ao usuário o direito de modificar o código-fonte; o produto é vendido no estado em que se encontra, e espera-se que seja utilizado no estado em que se encontra. O conteúdo e a função do aplicativo são definidos pelo vendedor; não se pretende que o usuário tenha qualquer ingerência no seu *design*. Embora seja distribuído por meio de contratos (licenças), esse código é efetivamente de propriedade do vendedor. O vendedor mantém direitos exclusivos sobre seu *design* e seu desenvolvimento.

A alternativa a esse modelo “comercial” é o modelo de desenvolvimento de *software* inicialmente promovido pela Free Software Foundation e, mais recentemente, pelo movimento “Open Source”<sup>118</sup>. Nesse modelo, o software é distribuído com seu código-fonte. Usuários têm o direito de modificar esse código. A depender da licença, eles podem ter o direito de usar esse código modificado em outros empreendimentos comerciais. Se uma característica específica de um aplicativo popular é indesejável, usuários desse modelo têm o direito — e, porque ele vem com seu código fonte, a capacidade — de removê-la.

Essa forma de organização produz “códigos de domínio comum” — códigos que não são de domínio privado nem de domínio estatal, mas, em vez disso, estão sujeitos a um domínio comum<sup>119</sup>. A essência de um domínio comum é a de que nenhuma pessoa exerce individualmente um direito exclusivo sobre o código. Nos termos estabelecidos por uma gama de licenças, qualquer um é livre para se apropriar desse código e desenvolvê-lo como queira.

Há uma quantidade extraordinária de literatura sobre esse movimento de *Software Livre*

---

<sup>118</sup> V. GOMULKIEWICZ, Robert W. How Copyleft Uses License Rights to Succeed in the Open Source Software Revolution and the Implications for Article 2B. *Houston Law Review*, v. 36, 1999, pp. 179, 182–85; STALLMAN, Richard. The GNU Operating System and the Free Software Movement. In: DI BONA, Chris; OCKMAN, Sam; STONE, Mark (eds.). **Open Sources: Voices from the Open Source Revolution**. 1999, pp. 53, 56–57, 60–61, 69–70 (doravante *Open Sources*).

<sup>119</sup> Isso não é tecnicamente preciso, mas o espírito da metáfora está correto. Para proteger códigos de apropriação, licenças de software impõem muitas condições para o uso de código aberto. Algumas condições podem parecer tecnicamente inconsistentes com a ideia de um domínio comum. Talvez uma descrição melhor envolva um domínio comum autoaplicável. V. DI BONA, Chris; OCKMAN, Sam; STONE, Mark. Introduction. **Open Sources: Voices from the Open Source Revolution** (*op. cit.*), p. 1-3 (descrevendo a Licença Pública Geral (GPL) emitida para consumidores de código aberto). De acordo com esta descrição, a GPL “basicamente diz que você pode copiar e distribuir um software licenciado sob a GPL à vontade, desde que não iniba outros de fazer o mesmo, seja cobrando pelo próprio software ou restringindo-o por meio de um licenciamento adicional. A GPL também exige que trabalhos derivados de trabalhos licenciados sob a GPL sejam também licenciados sob a GPL” (*idem*).

ou Open Source<sup>120</sup>. Meu objetivo aqui é apenas o de tecer um pequeno argumento: quando o código de um “espaço de aplicação” é de domínio comum, o poder regulatório do estado é fraco; quando o código de um “espaço de aplicação” é privado, o poder regulatório do estado é forte. O poder do estado, nesse sentido, depende da *organização* do código que constitui o ciberespaço — não apenas de sua arquitetura, mas também de quem controla essa arquitetura.

O motivo é simples. O estado regula fazendo com que as pessoas se comportem de determinadas maneiras. Quando regula “códigos”, ele o faz obrigando programadores a escrever códigos de maneira diferente. Quando eu descrevi uma regulação que pode zonestar de maneira mais eficiente conteúdos “prejudiciais para menores”, aquele esquema dependia significativamente do fato de que uma grande porção do mercado de navegadores é controlado por um pequeno número de empresas. Como Netscape e Microsoft são grandes empresas, com patrimônios reais, elas são alvos fáceis para a regulação.

Porém, quando não há uma única organização ou um pequeno número de organizações que controle o código, ou quando o código, ainda que inicialmente controlado por uma empresa, é aberto e, portanto, modificável, então o governo tem menos capacidade de regulá-lo. Um requisito impopular imposto a um código de domínio comum será simplesmente removido por pessoas que não podem ser facilmente reguladas pelo estado. Expandir o número de pessoas capazes de controlar o código, assim, contrai o poder do estado de regulá-lo. Um código de domínio comum é controlado menos facilmente que um código privado.

Nada nessa alegação é absoluto. Não estou argumentando que a organização do código é o único fator que importa. Tampouco estou argumentando que o estado é incapaz de ter qualquer efeito em códigos de domínio comum<sup>121</sup>. Mas o fato é que existe um efeito, ainda que marginal.

Esse argumento, contudo, sugere algo importante sobre o valor de um domínio comum, ao menos para aqueles que limitariam o poder regulatório do estado. Se um código é concebido como propriedade privada, e se são conferidos amplos direitos aos proprietários daquele código, então esse regime aumentará o poder regulatório do estado. O poder regulatório seria ainda maior se o estado controlasse o código, pois um código estatal seria mais regulável que um código privado. Mas um código estatal seria também menos eficiente. Já se foram os dias em que burocratas produziam algo; mais vale deixar a produção para o mercado.

Em relação a um código de domínio comum, entretanto, um código privado é mais regulável. Se o direito de propriedade confere o poder de disposição, então o domínio privado torna esse poder exclusivo; o domínio comum torna esse direito não exclusivo. O domínio comum não identifica uma pessoa única que detenha o poder exclusivo de dispor do código. Assim, códigos de domínio produzem diversas fontes de disposição, e limitam o poder

---

<sup>120</sup> V. idem; DYSON, Esther. Open Mind, Open Source. **Release 1.0**, Nov. 1998, p. 1; Gomulkiewicz *op. cit.*; Lessig (1999); MOODY, Glyn. The Wild Bunch. **New Scientist**, Dez. 12, 1998, p. 42; O'REILLY, Tim. Lessons from Open-Source Software Development. **Communications of the ACM**, Abr. 1999, p. 33; SELTZER, Larry. Software Returns to Its Source. **PC Magazine**, Mar. 23, 1999, p. 166; UBOIS, Jeff. Open-Source Tools Gain Credibility. **InformationWeek**, Mar. 22, 1999, p. 1A; SHAH, Rawan. Open Source Software for Windows NT: Developers of the World, Unite! You Have Nothing to Lose But Proprietary Control. **Windows TechEdge**, Fev. 1999; TURNER, Brough. Open Source Software Infuses CTI. **CTI Magazine**, Mar. 1999.

<sup>121</sup> V. Lessig (1999, p. 767-768).

regulatório do estado.

O domínio privado é comumente considerado um freio ao poder estatal. Ele é criticado por criar seu próprio problema de concentração de poder, mas muitos acreditam que este seja um poder menos perigoso. Seja isso verdade ou não, compreender o papel que o código pode desempenhar na regulação de comportamentos no ciberespaço põe em relevo uma observação sobre domínio que, sem isso, pode ser ignorada. Direitos exclusivos podem ser necessários para criar incentivos à atividade criativa no âmbito do ciberespaço; esses direitos podem ser justificados por um aumento na eficiência. Mas eles também ajudam a racionalizar o poder de disposição. Se uma constituição visa limitar esse poder ao estado, ela deve levar em conta o aumento nesse poder que direitos exclusivos no ciberespaço gerarão.

## B. Questões sobre a regulação do código pelo direito

Considerando que a organização do código permaneça sujeita à influência do estado, há duas questões que o ciberespaço tornara mais salientes. Uma é o alcance de tal regulação — se ela é finamente ajustada a um fim legítimo. A outra é a transparência dessa regulação — se as condicionantes impostas pelo estado são reconhecidas como condicionantes, e como condicionantes impostas pelo estado.

Minha alegação não foi a de que essa forma de regulação (por meio tanto da arquitetura quanto do direito) é nova no ciberespaço; minha alegação, no máximo, é a de que sua relevância é nova. Embora no passado, em contextos limitados, o estado tenha tido uma oportunidade de regular de uma maneira que iria, ela própria, aumentar a regulabilidade<sup>122</sup>, ele não teve essa oportunidade de uma maneira tão fundamental.

1. *Superinclusividade*. — A primeira questão que a regulação do código levanta é uma questão geral de superinclusividade. Para um dado objetivo, há qualquer número de maneiras de construir uma solução por meio de um código. Algumas serão mais restritas que outras. Com restritas, quero dizer menos generalizáveis — soluções que resolvem um problema, mas não possibilitam a regulação de muitos outros. E uma questão “constitucional” é se existe valor em restringir o escopo de regulações que possibilitam a regulação.

Dois exemplos expressam o argumento. No *Digital Millennium Copyright Act*, o Congresso incluiu um dispositivo antievasão<sup>123</sup>. Esse dispositivo regula esforços para contornar tecnologias projetadas para proteger materiais sujeitos a *copyright*. Se você tentar evadir-se dessas tecnologias, terá cometido um crime. Ou, de forma análoga, se você tentar arrombar a fechadura, terá cometido invasão.

<sup>122</sup> V. e.g., STERN, Robert L. The Commerce Clause Revisited — The Federalization of Intrastate Crime. **Arizona Law Review**, v. 15, 1973, pp. 271, 274–76 (discutindo o caso *United States v. Five Gambling Devices*, 346 U.S. 441 (1953), no qual o Tribunal derrubou a seção 3 do Johnson Act, 64 Stat. 1135 (1951), que exigia que fabricantes e revendedores apresentassem registros mensais de vendas e entregas e se registrassem anualmente junto ao Procurador-Geral. A autoridade para a “doutrina dos registros exigidos”, que isenta “registros exigidos” da proteção da Quinta Emenda [que consagra o devido processo legal e a proteção contra autoincriminação], é *Shapiro v. United States*, 335 U.S. 1, 7–15 (1948); mas a doutrina foi limitada por *Albertson v. Subversive Activities Control Board*, 382 U.S. 70, 77–78 (1965), que restringiu a aplicação da doutrina dos registros exigidos/autodeclaração a propósitos regulatórios genuínos. Ver também *Haynes v. United States*, 390 U.S. 85, 95–100 (1968) (encontrando requisitos de relatórios em violação à Quinta Emenda porque não eram de natureza regulatória); *Grosso v. United States*, 390 U.S. 62, 66–69 (1968) (idem); *Marchetti v. United States*, 390 U.S. 39, 54–57 (1968) (idem).

<sup>123</sup> V. Digital Millennium Copyright Act § 1201, Pub. L. No. 105-304, 112 Stat. 2860, 2863–72 (1998)

O problema com essa estrutura, no entanto, é o de que ela confere mais proteção do que conferiria o direito de *copyright* subjacente. Como críticos da norma antievasão apontaram<sup>124</sup>, o direito criminaliza a evasão a essas mesmo quando o uso feito do material não teria configurado uma violação de *copyright*.

Ainda assim, o dispositivo antievasão pune uma evasão que simplesmente possibilita um *fair use*. O direito, assim, protege mais o código do que o material sujeito a *copyright* subjacente.

Teria sido simples construir uma norma antievasão que não fosse assim tão excessivamente ampla. A lei poderia, por exemplo, ter considerado a evasão uma circunstância agravante em qualquer persecução por violação de *copyright*. Porém, ao proteger o código mais que o *copyright*, a lei cria um incentivo ao *copyright* privatizado que eu descrevi na Parte II. Isto é, a lei protege esquemas cujo efeito último pode muito bem ser a quebra do equilíbrio visado pelo direito de *copyright*.

Alguns podem justificar essa forma de regulação como uma espécie de norma contra invasão de propriedade. Por essa concepção, o dispositivo antievasão simplesmente protege proprietários contra o acesso não autorizado a sua propriedade. Mas a metáfora aqui é perigosa. Se o dispositivo antievasão alcançasse apenas tentativas de “hackear” o sistema de um computador, então “invasão de propriedade” seria uma metáfora útil. Mas na medida em que o dispositivo visa considerar a propriedade intelectual mais como uma propriedade real, protegendo-a do acesso à informação, em vez do acesso a computadores, então a metáfora da “invasão de propriedade” não é útil. Eu não invado sua ideia simplesmente porque penso nela.

Um segundo exemplo de ajuste fino é ainda mais problemático. Eu descrevi na Parte II um esquema para facilitar o zoneamento de conteúdos no ciberespaço. Na minha visão, o direito poderia direcionar a arquitetura do ciberespaço no sentido de um espaço acessado mediante identificação. Ao criar um incentivo para que os indivíduos portem identidades digitais, ou ao obrigar os sistemas a verificar identidades digitais, o direito poderia induzir o fornecimento de identidades, aumentando assim a regulabilidade.

Há muitos *designs* possíveis para um ciberespaço acessado mediante identificação, todavia. Esses variados *designs* geralmente têm diferentes consequências para a regulabilidade do ciberespaço. Eu descrevi na Parte II uma versão de uma identidade infantil. Ela seria um navegador que oculta informações pessoais sobre o usuário, mas indica que o usuário é menor. O *design* possibilitaria a servidores com conteúdo adulto identificar o cliente como criança, e assim negar-lhe acesso; também possibilitaria a sites que coletam dados atender a normas que proibissem a coleta de dados de crianças.

Um ciberespaço alternativo acessado mediante identificação criaria incentivos para que os usuários portassem identidades digitais<sup>125</sup>. Esses certificados digitais verificariam alguns dados sobre seu portador — por exemplo, nome, idade, cidadania e sexo.

---

<sup>124</sup> SAMUELSON, Pamela. The Digital Rights War. **Wilson Quarterly**, outono de 1998, p. 48, pp. 52–53; SAMUELSON, Pamela. A Look at... Whose Ideas, Anyway? Facing a Pay-Per-Use Future. **The Washington Post**, 1 Nov., 1998, p. C3.

<sup>125</sup> O governo já está explorando essa ideia, mas a meu ver não muito bem. V. *GSA's Federal Technology Service Issues ACES RFP* (“ACES [Certificados de Acesso para Serviços Eletrônicos] destinam-se a fornecer identificação, autenticação e não-repúdio por meio do uso de tecnologia de assinatura digital como meio para que indivíduos e entidades comerciais sejam autenticados ao acessar, recuperar e enviar informações ao governo”).

A fim de controlar conteúdos adultos, o único dado essencial do certificado seria a idade. E, assim como a identidade infantil pode possibilitar outras regulações relacionadas com o fato de ser criança, uma identidade etária em geral possibilitaria outras regulações relacionadas com o fato de ser adulto, como regulações de apostas ou de eleições.

Porém, uma vez que identidades tais certificam mais dados que apenas a idade, elas facilitam um escopo regulatório vastamente aumentado. Se certificarem dados de cidadania ou de residência, elas permitirão regulações que condicionem o acesso ao preenchimento desses requisitos. Quanto mais dados as identidades certificarem, mais zoneamento o sistema possibilitará.

Se a finalidade estrita de uma regulação por parte do Congresso fosse a de proteger crianças, então o meio menos restritivo de fazê-lo seria o navegador em modo infantil. Mas, se o Congresso discordar, então a superinclusividade pode se tornar um problema. Isso porque, ao criar os incentivos para identidades mais abrangentes, o estado poderia criar os incentivos necessários para facilitar regulações muito mais abrangentes de comportamentos no ciberespaço. Uma tal regulação se estenderia para além do legítimo interesse regulatório do estado, e facilitaria a regulação para muito além de esforços para limitar o acesso a material adulto.

Nos exemplos do dispositivo antievasão e do NMI, a estrutura da potencial regulação é a mesma. Em ambos, ao menos duas mudanças na arquitetura podem atingir o fim estatal. Uma das mudanças facilita esse fim por si só; a outra facilita esse fim e, como subproduto, cria a oportunidade de regulação para além desse fim. No caso do dispositivo antievasão, essa regulação adicional é uma regulação privada; no caso das identidades, ela é pública.

A questão, em cada caso, é se algo pende em favor da regulação mais restrita ou da mais ampla. No contexto da regulação de conteúdo, o princípio da liberdade de expressão obviamente o faz. Mas a regulação por identificação se relaciona de forma ambígua com a livre expressão. Uma regulação de identidades poderia ser extrapolada para motivos alheios à liberdade de expressão. E se isso ocorresse — por exemplo, para facilitar atividades bancárias ou o uso de cartões de crédito on-line —, então a mesma questão acerca dos subprodutos persistiria. O estado pode ter uma necessidade legítima de regular no sentido de encorajar a identificação, mas a consequência do aumento de identificação pode ser uma virada na irregularidade do espaço de modo geral.

2. *Transparência.* — Um segundo problema com a regulação do código pelo direito é a falta de transparência. Quando o estado demanda que indivíduos se comportem de uma determinada maneira, eles reconhecem que é o estado quem está regulando. Se não gostarem dessa regulação, eles podem eleger representantes que a rejeitem. A regulação, desse modo, é contrabalanceada pelo processo político<sup>126</sup>.

A transparência também é tradicionalmente um valor que condiciona a promulgação de

---

<sup>126</sup> Cf. RAWLS, John. *A Theory of Justice*. 1971, p. 133 (“Uma terceira condição [para um conceito de direito] é a da publicidade (...). O ponto da condição de publicidade é fazer com que as partes avaliem concepções de justiça como constituições morais de vida social publicamente reconhecidas e totalmente eficazes”); DAN-COHEN, Meir. *Decision Rules and Conduct Rules: On Acoustic Separation in Criminal Law*. *Harvard Law Review*, v. 97, 1984, pp. 625, 667–73 (avaliando argumentos em favor da transparência ao passo que conclui que a transparência também acarreta custos significativos).

regulações. Embora os Constituintes<sup>127</sup> tenham mantido secretas suas deliberações, e embora o Senado tenha preservado esse sigilo até 1795<sup>128</sup>, o estado de direito sempre requereu que uma lei se tornasse pública antes de produzir efeito. O *Administrative Procedure Act* (APA)<sup>129</sup> levou esse valor ainda mais adiante — em resposta ao emergente estado regulador<sup>130</sup>, o APA estabeleceu procedimento que demandam abertura no processo administrativo<sup>131</sup>.

Mas, e se a regulação pudesse ser secreta — ou, mais precisamente, e se o fato de que o governo está regulando de uma certa maneira pudesse ser mantido em sigilo? Nesse caso, essa condicionante de *accountability* política desapareceria. Uma vez que não estaria claro que a fonte da regulação é o governo, ele poderia atingir seu objetivo sem pagar o preço político ou diminuir a eficácia da regulação.

O caso *Rust v. Sullivan*<sup>132</sup> é um exemplo do poder da não-transparência. O Governo Reagan se opunha ao aborto. Um grupo de mulheres que poderiam ser dissuadidas de abortar era o daquelas que visitavam clínicas de planejamento familiar. Obviamente, por força do precedente *Roe v. Wade*<sup>133 134</sup>, o governo está limitado quanto aos meios que pode selecionar para impedir abortos. Embora não seja obrigado a financiar abortos, o estado não pode proibi-los completamente. Embora possa argumentar contra o aborto — por exemplo, pregando cartazes com os dizeres “o Governo acredita que optar pela vida é melhor que optar pelo aborto” em qualquer clínica de planejamento familiar com financiamento estatal —, essas campanhas seriam provavelmente ineficazes. Advertências do governo seriam tratadas meramente como advertências do governo — um produto da política, entenderiam muitos, e pouco mais que isso.

Em razão disso, o Governo Reagan optou por uma técnica diferente e mais eficaz. Proibiu que médicos em clínicas de planejamento familiar recomendassem ou discutissem o aborto como um método de planejamento familiar. Em vez disso, se perguntados, esses médicos deveriam dizer que o programa “não considerava o aborto um método apropriado de planejamento familiar e, por isso, não aconselhava ou encaminhava para aborto”<sup>135</sup>.

Ora, o que esse método de regulação tem de genial é que ele efetivamente esconde o dedo do governo. Como Laurence Tribe sustentou ante a Suprema Corte<sup>136</sup>, ele permite ao governo transmitir sua mensagem sem ligar a mensagem ao governo. Muitas mulheres provavelmente chegarão à conclusão de que é o seu médico que está lhes dissuadindo da ideia do aborto — já que é o médico que está dizendo ou deixando de dizer alguma coisa sobre o aborto. O governo

<sup>127</sup> No original, “*Framers*”. (N. dos T.)

<sup>128</sup> V. BAKER, Richard Allan. *The Senate of the United States: A Bicentennial History*. 1988, pp. 24–25.

<sup>129</sup> Lei de Processo Administrativo. (N. dos T.)

<sup>130</sup> No original, “administrative state”.

<sup>131</sup> V. *Administrative Procedure Act*, 5 U.S.C. § 553 (1994) (exigindo que regras vinculantes sejam promulgadas após um procedimento de audiências públicas [*notice and comment procedure*]).

<sup>132</sup> 500 U.S. 173 (1991).

<sup>133</sup> 410 U.S. 113 (1973).

<sup>134</sup> Emblemático *leading case* da Suprema Corte dos EUA, que, em janeiro de 1973, julgou ser o aborto um direito constitucional. Foi superado em junho de 2022 pelo caso *Dobbs v. Jackson Women’s Health Organization*, considerando a regulação sobre o direito ao aborto como matéria de competência estadual, sem proteção específica da Constituição dos EUA. (N. dos T.)

<sup>135</sup> *Rust*, 500 U.S., p. 180 (citando 42 C.F.R. § 59.8(b)(5) (1989))

<sup>136</sup> V. a transcrição dos debates orais do caso *Rust*, 500 U.S., p. 173 (Nos. 89-1391, 89-1392), disponível em 1990 WL 601355, at \*3–\*27 (Oct. 30, 1990).

atinge seu objetivo minando a transparência. O sucesso do programa está em derrotar a transparência.

O ciberespaço apresenta uma oportunidade patente para o que aconteceu no caso *Rust*. Isso porque é uma característica da experiência das pessoas no ciberespaço a de que é improvável que elas associem qualquer condicionante específica a uma opção de um programador. Quando uma pessoa entra em uma sala de bate-papo na AOL com capacidade para apenas vinte e três pessoas, é provável que ela acredite que essa limitação é de alguma forma determinada pela natureza do espaço. Porém, é claro, vinte e três é um número arbitrário; poderia muito bem ter sido 230. A diferença seria uma escolha, e as razões para a escolha não estão dadas.

Isso cria uma extraordinária oportunidade para o governo. Pois, uma vez que o governo possa ocultar suas escolhas no código do espaço, ele pode, como o Governo Reagan no caso *Rust*, evitar as consequências políticas de suas escolhas. Uma vez que ele possa usar a arquitetura para dar efetividade a suas escolhas, ele pode atingir seus objetivos mais rápida e facilmente do que se os perseguisse abertamente.

Minha alegação não é a de que essa oportunidade é nova, nem de que toda regulação por meio da arquitetura é não transparente. Quando Robert Moses construiu pontes em Long Island que bloqueavam ônibus, impedindo o acesso dos motoristas — e com isso dos menos afortunados — às praias públicas<sup>137</sup>, tratava-se de uma regulação por meio da arquitetura, e essa regulação escondia bem seus motivos. Mas, quando o estado constrói um quebra-molas na rampa de acesso a um terminal aéreo, também se trata de uma regulação por meio de arquitetura. Essa regulação de maneira alguma esconde a política por trás dela — ninguém acredita que foi a natureza ou o acaso que colocou o quebra-molas no meio da rua.

A diferença entre o ciberespaço e o espaço real é, novamente, uma diferença de grau. As oportunidades para uma regulação não transparente são multiplicadas no ciberespaço, e a questão fundamental, ou constitucional, é se deveríamos nos preocupar. Nossa crença no valor da transparência deveria nos afastar de regulações por meio de código que escondam suas motivações? Deveríamos exigir que o estado anuncie seu propósito, ou deixe evidente sua atuação?

O ciberespaço levanta a questão da transparência em um novo contexto. Quando regula indiretamente, por meio da regulação do espaço do ciberespaço, o governo deveria ser obrigado a deixar a regulação transparente?<sup>138</sup> Tenho a forte impressão, consistente com nossa tradição, de que a resposta deveria ser sim<sup>139</sup>. Mas também tenho a forte opinião de que não há nada no nosso atual rol de princípios constitucionais que realmente obrigue o governo a fazê-lo. Se a constituição quiser estar em dia com os problemas do ciberespaço, ela deve ser capaz de abordar

---

<sup>137</sup> V. CARO, Robert A. *The Power Broker: Robert Moses and the Fall of New York*. 1974, p. 318.

<sup>138</sup> Para um ataque poderoso à falha do governo em manter transparência em sua regulamentação, v. FROOMKIN, Michael. *It Came from Planet Clipper: The Battle Over Cryptographic Key "Escrow"*. **University of Chicago Legal Forum**, 1996, p. 15.

<sup>139</sup> Quão afirmativamente o estado deve fazer isso é uma questão mais difícil. Pelo menos podemos ser claros sobre o que não deve fazer. Por exemplo, em uma proposta recente de relaxar os controles de criptografia, a administração ainda estava clara sobre o desejo de manter o sigilo das técnicas de investigação usadas para rastrear o comportamento online. V. a transcrição da coletiva de imprensa da Casa Branca de 16 de setembro de 1999. Embora algumas técnicas sem dúvida devam ser confidenciais, a extensão e a natureza do controle do estado sobre a arquitetura da criptografia não deveriam ser.

essas questões.

### C. Questões sobre a regulação do direito pelo código

O direito, como argumentei, é vulnerável à soberania concorrente do código. Programadores podem escrever códigos que desloquem os valores que o direito tem abraçado. E, se os valores jurídicos quiserem sobreviver, o direito pode muito bem ter que reagir.

Meus exemplos da Parte II descrevem dois casos específicos nos quais os valores de um regime jurídico são deslocados. Mas podemos descrever esse deslocamento de forma mais geral. Geralmente, os valores que a atual arquitetura possibilita são valores de controle horizontal<sup>140</sup> — exceto, como anotei, no caso da privacidade. Eles possibilitam um controle a partir de estruturas horizontais, como as que se assemelham a contratos ou à propriedade. Eles interferem na imposição vertical<sup>141</sup> de regras que os usuários não escolheriam para si próprios.

Isso não significa que o estado não possa regular, pois, como descrevi, ele pode usar técnicas indiretas para criar incentivos que afetem comportamentos horizontais. No entanto, essa constatação evidencia uma fragilidade no potencial da Internet para a autorregulação.

Existe uma economia política para a autorregulação da Rede, assim como existe uma economia política para a regulação em geral. Como acontece com qualquer economia política, alguns interesses têm maiores ganhos individualmente do que outros a partir de uma arquitetura específica. Esses interesses financiam uma dada evolução do *design* horizontal da Rede, e pode-se esperar que eles prevaleçam nessa evolução ainda que o ganho líquido a partir do seu *design* seja menor que o ganho líquido a partir de outro *design*.

Este óbvio argumento sugere um segundo. Usuários precisam de um meio de ação coletiva no relativamente pequeno número de casos nos quais a regulação horizontal deixa desprotegidos alguns valores jurídicos importantes, ou nos quais a evolução desse *design* horizontal ameaça algum valor jurídico importante. Na conjuntura atual, essa regulação coletiva é resistida por muitos na Rede<sup>142</sup>. Mas deveríamos rejeitar distinções simplistas — a escolha nunca foi entre anarquia e totalitarismo, ou entre liberdade e controle. Algumas regulações podem aumentar a liberdade individual, ainda que outras condicionem essa liberdade a um objetivo coletivo.

Há duas ilustrações óbvias desse argumento. A primeira, privacidade, eu já apresentei, e vou abordar em mais detalhes agora. A segunda, *spam*, eu descrevo adiante.

*1. Privacidade.* — Anteriormente, eu descrevi uma maneira pela qual o estado poderia efetivamente subsidiar arquiteturas para garantir privacidade. Deve ficar claro, não obstante a retórica sobre autorregulação, que sem esse subsídio, a proteção à privacidade do consumidor é improvável. Existem organizações, claro, que estão tentando estabelecer proteção à privacidade. Todavia, sua efetividade é mínima em comparação aos interesses e ao poder de

<sup>140</sup> No original, “values of bottom-up control”. (N. dos T.)

<sup>141</sup> No original, “top-down imposition”. (N. dos T.)

<sup>142</sup> V. *e.g.*, FREZZA, Bill. Cyberspace Jurisprudence: Who Shall Punish Evil? **InternetWeek**, 1 fev. 1999, p. 25.

mercado do comércio no ciberespaço. Como a FTC<sup>143</sup> descreveu<sup>144</sup>, os esforços dessas entidades autorreguladas têm sido totalmente ineficazes para provocar uma mudança nas proteções do espaço. E não há nada no horizonte que sugira que o futuro da privacidade do consumidor vá ser diferente do passado.

Para valores como privacidade, é improvável que uma regulação horizontal seja capaz de alterar uma arquitetura — aqui, a arquitetura do comércio — que beneficia tão significativamente uma poderosa classe específica de usuários. O desafio é o de sobrepor a esse *design* horizontal estruturas e incentivos que possibilitarão alguma liberdade de escolha coletiva além do efeito cumulativo desorganizado da expressão de preferências individuais.

2. *Spam*. — *Spam*<sup>145</sup> é o envio de e-mails comerciais não solicitados, geralmente em massa, a listas de contas de e-mail ao redor da Internet. Essas listas são extremamente baratas — 500 dólares por 500 mil nomes de uma única fonte<sup>146</sup>; como o preço é tão baixo, é possível enviar 10 milhões de e-mails usando uma dessas listas e ter lucro mesmo se o retorno por destinatário for muito pequeno.

A lucratividade do *spam* se dá em função do *design* dos e-mails. A arquitetura inicial do sistema de e-mail fazia pouca coisa para autenticar usuários de *relays* de e-mail. O SMTP (*Simple Mail Transport Protocol*), por exemplo, que ainda é o protocolo de e-mail dominante, permite *relays* de e-mail de terceiros sem conta no sistema de e-mail primário<sup>147</sup>. Com sistemas de SMTP configurados para aceitar *relays* de terceiros, eu posso direcionar meu e-mail para ser enviado através desses sistemas, mesmo que eu não tenha conta nesses sistemas. Assim, *spammers* podem usar sistemas de *relay* de terceiros para inundar a Rede de e-mails<sup>148</sup>.

*Relays* de terceiros não são a única técnica que os *spammers* usam. Mas são assunto de um importante debate sobre *spam* na Internet. Isso porque, embora muitos não empreguem um sistema de *relay* de terceiros, alguns administradores de sistemas querem que o canal de *relay* seja mantido aberto, e tomam outras providências para garantir que o canal não seja abusado por *spammers*<sup>149</sup>.

Outros, encarando os *relays* de terceiros como a maior causa de *spam*, querem esses

<sup>143</sup> *Federal Trade Commission*, agência federal de comércio dos EUA. (N. dos T.)

<sup>144</sup> V. *Privacy Online*, p. 41 (“Uma autorregulação eficaz continua sendo desejável porque permite que as empresas respondam rapidamente às mudanças tecnológicas e empreguem novas tecnologias para proteger a privacidade do consumidor [...] Até o momento, no entanto, a Comissão não viu surgir um sistema autorregulatório eficaz”). No entanto, em julho de 1999, a FTC enviou um novo relatório ao Congresso, concluindo que “as iniciativas autorregulatórias descritas [pelo relatório] refletem o esforço substancial e o compromisso dos líderes da indústria com práticas justas de informações” (1999).

<sup>145</sup> V. *Developments*, p. 1601-1603 (descrevendo o problema do spam, as várias soluções legais que foram propostas e as implicações dessas soluções quanto a direitos da Primeira Emenda).

<sup>146</sup> SORKIN, David E. Unsolicited Commercial E-Mail and the Telephone Consumer Protection Act of 1991. *Buffalo Law Review*, v. 45, n. 47, 1997, p. 1010.

<sup>147</sup> V. SCHWARTZ, Alan; GARFINKEL, Simson. **Stopping Spam: Stamping Out Unwanted Email and News Postings**. 1998, pp. 90-91; Cukier, Kenneth. ISPs and Corporates Overcome by Spam. *CommunicationsWeek International*, 19 jan. 1998, p. 26.

<sup>148</sup> V. Schwartz; Garfinkel, 1998, p. 90 (advertindo que um servidor “não deve permitir que computadores desconhecidos [retransmitam e-mails], para que um *spammer* não aproveite o servidor para ocultar seus rastros”); NEWS BRIEFS: Spammers Still Find Too Many Open Doors. *Network World*, 12 jul. 1999, p. 6 (citando um relatório que constatou que aproximadamente 17% dos servidores de e-mail permanecem abertos para o tráfego de *relay*).

<sup>149</sup> FONTANA, John. Slam the Spam Door. *InternetWeek*, 17 ago. 1998, p. 1 (observando que “há aqueles que não têm escolha a não ser deixar seus relays abertos” e citando um administrador de e-mail universitário que explica que sua solução é “monitorar pra caramba os logs”).

canais fechados. E alguns desses outros organizaram *blacklists*<sup>150</sup> para sistemas de *open relay*; assinantes usam essas *blacklists* para determinar quais remetentes terão seus e-mails rejeitados<sup>151</sup>. Se o administrador do seu e-mail tiver deixado seu *relay* aberto, é provável que o seu *site* seja adicionado a essas listas; se o seu *site* for adicionado a essas listas, o seu e-mail, quando enviado a *sites* administrados por assinantes dessas listas, em muitos casos simplesmente desaparecerá.

Essa produção de *blacklists* é uma espécie de justificação — é um exemplo de particulares fazendo direito com suas próprias mãos<sup>152</sup>. Chamar de justificação não é criticar os justiceiros. Justiceiros, em uma natureza sem estado, podem ser as únicas pessoas combatendo o crime, e eu certamente acredito que, em relação às normas da Rede, *spam* é crime.

Porém, à parte a virtude, o justificação tem seus custos. Essas *blacklists* criam conflitos que se estendem para muito além da simples listagem de um site. Consideremos um exemplo de uma batalha potencialmente explosiva<sup>153</sup>.

Em 1998, Jeff Schiller, administrador de rede do MIT, começou a receber e-mails de usuários do sistema do MIT reclamando que seus e-mails para outras pessoas fora do domínio do MIT haviam sido bloqueados. Os e-mails estavam sendo boqueados porque um justiceiro de *spam*, o Open Relay Behavior-modification System<sup>154</sup> (ORBS), havia decidido que a rede do MIT tinha “más práticas de e-mail”. Sem aviso, o MIT foi colocado na *blacklist* do ORBS, e assinantes do ORBS começaram a excluir automaticamente e-mails do MIT. Uma empresa em específico confirmou sua política de bloqueio de acordo com a lista do ORBS — a Hewlett Packard (HP). E-mails do MIT para a HP não chegariam, disseram ao MIT, até que o MIT mudasse sua política de rede.

O MIT não se deixaria coagir. Sua decisão de não bloquear automaticamente todos os e-mails de *relays* de terceiros (e-mails que o servidor do MIT envia sem autenticar que o remetente é associado ao MIT) fazia sentido para sua rede e para a comunidade do MIT. O MIT tomava medidas para limitar *spam* fiscalizando o uso de sua função de *relay* de terceiros. Mas seus métodos não eram os métodos do ORBS, o que tornava o MIT um inimigo do ORBS.

Em vez de ceder à pressão do ORBS, o MIT decidiu brigar. E, como uma coisa leva a outra, decidiu entrar na briga com o MIT.

<sup>150</sup> Em português, listas negras. No contexto dessas tecnologias, contudo, é mais comum o emprego do termo em inglês, motivo pelo qual optamos por não o traduzir. (N. dos T.)

<sup>151</sup> V. DENNIS, Roger. Xtra's E-mail Problems Continue. **Christchurch Press**, 9 mai. 1998, p. 27.

<sup>152</sup> Outros exemplos de justificação antispam abundam. V. POST, Daniel G. Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace. **University of Chicago Legal Forum**, 1996, p. 139-163 (descrevendo o Cancelmoose, “um ser fictício operando pseudonimamente no ciberespaço que liderou a emissão de ‘cancelbots’ — comandos que cancelam postagens em grupos de notícias Usenet — em resposta a casos relatados de ‘spam’”); LEE, Richard C. Cyber Promotions, Inc. v. America Online, Inc. Comment. **Berkeley Technology Law Journal**, v. 13, n. 5, 1998, p. 417 (“Muitas entidades relacionadas com e-mails indesejados têm recebido ataques paralisadores de sistema, vírus e até ameaças físicas”); MARCUS, Joshua A. Commercial Speech on the Internet: Spam and the First Amendment. **Cardozo Arts & Entertainment Law Journal**, v. 16, p. 245, 1998, p. 248 (contando a história de dois advogados de Scottsdale, Arizona, cuja imensa disseminação de *spam* provocou “e-mails de ódio, ameaças de morte e comentários antissemitas”).

<sup>153</sup> V. LESSIG, Lawrence. The Spam Wars. **The Industry Standard**, 31 dez. 1998.

<sup>154</sup> Em português, Sistema de Modificação de Comportamento quanto ao *Open Relay*, ou *Relay Aberto*. (N. dos T.)

Até que veio uma espécie de intervenção divina. Em resposta às queixas de outros ISPs, o provedor de serviços de rede do ORBS, BC Tel, decidiu que seus “testes de *relay* não autorizados” eram uma violação de sua própria política de rede. Em razão disso, a BC Tel chutou o ORBS para fora da rede, e os e-mail do MIT voltaram a fluir para a HP. Uma guerra do *spam* fora evitada.

Essas *blacklists* são uma espécie de regulação horizontal. Assim como as soluções para o problema da privacidade, elas são uma regulação horizontal imperfeita. Isso porque não são capazes de lidar diretamente com o problema real que está afetando a Rede — a saber, o *spam*. Para combater o *spam*, *blacklists* adotam técnicas que são, ao mesmo tempo, sub e superinclusivas, e, para usuários sugados pelo buraco negro dessas técnicas, essas *blacklists* atraem conflitos reais<sup>155</sup>.

Um meio mais simples e mais direto de lidar com esse problema seria uma espécie de regulação governamental. Normas contra invasão de privacidade são um primeiro exemplo<sup>156</sup>; uma lei tornando obrigatório o etiquetamento de *spam* seria um segundo<sup>157</sup>. Ambas as leis poderiam mudar os incentivos dos *spammers*, elevando o custo do *spam* a um nível no qual os benefícios não superassem os custos<sup>158</sup>.

Por essa visão, o *spam* foi “causado” pelo efeito que o código produziu no mercado — facilitar publicidade de baixo custo. A resposta é um direito que aumenta os custos no mercado — diminuindo assim a incidência de publicidade de baixo-custo. Em outras palavras, o direito, nesse caso, ofereceria compensação para a mudança no código<sup>159</sup>. A comunicação consensual (não *spam*) ainda seria barata; a comunicação não consensual (*spam*) ainda seria mais barata do que no espaço real.

3. *Valores em evidência.* — Meu objetivo nesta seção foi o de pôr em evidência um conjunto de valores que não deveríamos perder de vista enquanto tratamos do conflito entre as regulações do direito e as regulações do código. Esses valores deveriam restringir tanto o efeito do direito no código quanto o efeito do código no direito. Considerando que o direito use código, mas de forma não transparente, nós temos razão de questionar a técnica do direito. E, considerando que o direito pode atingir seus fins por meio de código, nós temos razões para requerer que o código seja finamente ajustado para servir apenas a fins estatais legítimos.

E também vice-versa. Quando uma estrutura de código afeta valores implícitos no direito, há bons motivos para garantir que esses valores não sejam deslocados. Na categoria

<sup>155</sup> V. GENTILE, Kimberly. U. Texas-Austin’s Junk E-mail Service Nixed, Problems Cited. **U. Wire**, 20 nov. 1998 (relatando que funcionários de computação da Universidade do Texas recuaram do ORBS após receberem reclamações de que e-mails legítimos estavam sendo bloqueados, e citando um funcionário que afirmou que o ORBS é “uma medida rigorosa demais para ser implementada neste momento”); HALL, Rob. Here’s the Dumbest Idea to Hit the Net. **Ottawa Sun**, 2 out. 1998, p. 51 (descrevendo o ORBS como “um método drástico demais para ser adotado”).

<sup>156</sup> V. *Developments*, p. 1602 (descrevendo uma causa em que uma tese de invasão de propriedade de um ISP foi acatada).

<sup>157</sup> V. idem (descrevendo alguns projetos legislativos).

<sup>158</sup> Para comentários sobre a regulação da prática de spam, v., em geral, HAWLEY, Anne E. Taking Spam out of Your Cyberspace Diet: Common Law Applied to Bulk Unsolicited Advertising via Electronic Mail. **UMKC Law Review**, v. 66, 1997, p. 381; Sorkin, *op. cit.*; Lee, *op. cit.*; MILLER, Steven. Washington’s “Spam Killing” Statute: Does It Slaughter Privacy in the Process? **Washington Law Review**, v. 74, 1999 p. 453.

<sup>159</sup> GOLDSMITH, Jack L. Against Cyberanarchy. **University of Chicago Law Review**, v. 65, 1998, p. 1201 (observando que “mudanças [nas regulamentações estatais] são esperadas quando a velocidade da comunicação aumenta dramaticamente e o custo da comunicação diminui dramaticamente”).

geral dos casos em que a agregação horizontal de preferências não seja capaz de produzir a mescla ideal de regulações, deveríamos limitar a agregação feita por meio do *design* horizontal do código.

## Conclusão

No centro de qualquer lição sobre o ciberespaço está uma compreensão sobre o papel do direito. Devemos fazer uma escolha sobre a vida no ciberespaço — sobre se os valores nele inseridos serão os valores que queremos<sup>160</sup>. O código do ciberespaço constitui esses valores; ele pode ser moldado a fim de constituir valores que ressoem com nossa tradição, assim como pode ser construído de modo a refletir valores inconsistentes com nossa tradição.

À medida que a Rede cresce, que seu poder regulatório aumenta, que sua força como fonte de valores se torna estabelecida, os valores dos soberanos do espaço real vão inicialmente sair perdendo. Em muitos casos, sem dúvida, isto é algo muito bom. Mas não há razão para acreditar que será algo bom de modo geral ou indefinido. Não há nada que garanta que o regime de valores constituído por código será um regime liberal; e há pouca razão para esperar que uma mão invisível de programadores vai conduzi-lo nessa direção. Com efeito, na medida em que programadores atendam aos desejos do comércio, um poder de controle pode muito bem ser a inclinação que esse código começará a ter<sup>161</sup>. Compreender essa inclinação será um projeto contínuo do “direito do ciberespaço”.

Entretanto, o juiz Easterbrook argumentou que não há razão para ensinar o “direito do ciberespaço” mais do que há razão para ensinar o “direito do cavalo”, porque nenhum dos dois, sugeriu ele, iria “iluminar todo o direito”<sup>162</sup>. Este ensaio foi uma respeitosa discordância. As ameaças a valores implícitos no direito — ameaças aumentadas por mudanças na arquitetura do código — são apenas exemplos específicos de uma constatação mais geral: de que não é só o direito que possibilita os valores jurídicos e que os valores jurídicos, e que o direito sozinho não é capaz de garanti-los. Se nosso objetivo for um mundo constituído por esses valores, então são esses outros reguladores — o código, mas também as normas sociais e o mercado — que devem ser abordados tanto quanto o direito. O ciberespaço evidencia não apenas como essa interação acontece, mas também a urgência em compreender como afetá-la. •

---

<sup>160</sup> V. FANO, Robert. On the Social Role of Computer Communications. *Proceedings of the IEEE*, v. 60, 1972, p. 1249-1253.

<sup>161</sup> Este é o argumento central em Lessig (1999), nota 2 *supra*.

<sup>162</sup> Easterbrook (1996), nota 1 *supra*.