DOS CÓDIGOS LEGAIS AOS CÓDIGOS DO CIBERESPAÇO: REFLEXÕES SOBRE DIREITO E *DEEP WEB*[1]

FROM LEGAL CODES TO CYBERSPACE CODES: THOUGHTS ON LAW AND DEEP WEB

Marcos Vinício Chein Feres[2]

Jordan Vinícius de Oliveira[3]

Resumo

O que são os códigos tecnológicos e como eles interferem nos códigos legais? Esse artigo visa analisar as interseções entre direito e ciberespaço. O plano de análise é composto pela teoria de viver plenamente a lei e pela técnica de pesquisa por traços de significação. Por meio do estudo de caso da rede Tor, verificou-se que os códigos tecnológicos são capazes de interferir na habilidade do sistema jurídico tradicional para regular o ciberespaço. Portanto, compreender esses elementos tecnológicos torna-se crucial para promover novas abordagens jurídicas adaptadas aos valores tecnológicos desse meio virtual.

Palavras-chave: Ciberespaço. Deep web. Propriedade intelectual. Software. Rede Tor.

Abstract

What are the so-called technological codes and how do they interfere with the traditional legal codes? This paper aims to analyze the intersections between law and cyberspace. The methodological tools consist of the intertwining with living lawfully theory and the unobtrusive research technique. Taking into account the case study of the Tor network, the main result is that the codes derived from technological environment make the traditional legal system less efficient to regulate cyberspace. Therefore, understanding these technological elements is essential to promote new legal approaches in accordance with the values of the cyberspace.

Keywords: Cyberspace. Deep web. Intellectual property. Software. Tor network.

INTRODUÇÃO

Discutir sobre a capacidade regulatória da rede e dos ciberespaços demanda uma abordagem analítica e crítica, não restrita a elementos dogmáticos puros. Essa temática

[1] A presente pesquisa conta com o financiamento do Conselho Nacional do Desenvolvimento Científico e Tecnológico, CNPq e da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior, CAPES.

[2] Bolsista de Produtividade PQ2 do CNPq. Mestre e Doutor em Direito pela UFMG. Professor associado da Universidade Federal de Juiz de Fora.

[3] Bolsista DS/CAPES. Bacharel em Direito e Mestrando em Direito e Inovação pela Universidade Federal de Juiz de Fora.

demanda do direito uma flexibilidade, de modo a comportar as nuances próprias das redes, programas e componentes físicos que compõem o ciberespaço.

De acordo com Lessig (2006, p. 09), pode-se dizer que o termo ciberespaço é mais específico do que a internet. Enquanto a internet é apenas o meio virtual de transferência de dados, o ciberespaço traz consigo uma conotação de pertença, um certo senso de comunidade e de participação. É o que pode ser presenciado, por exemplo, em grupos de discussão, redes sociais, ou em jogos online, que se tornam uma espécie de segunda vida para seus integrantes.

Ainda segundo Lessig (2006, p. 72), a compreensão de dois tipos de códigos, o legal e o tecnológico, revela-se importante para o ciberespaço. O código legal é o positivado, elaborado pelo Congresso, pelos governantes, entre outros, a exemplo das leis e decretos. O código tecnológico, contudo, é o desenvolvido por programadores: são as instruções contidas em softwares e hardwares que se incorporam às experiências de interação com o mundo virtual.

A presente pesquisa visa analisar o contexto dos ciberespaços como criações virtuais que replicam o agir humano em comunidade. Não se constitui como objetivo a análise direta sobre qualquer elemento legislativo, como a lei de direitos autorais ou o marco civil da internet. O que se propõe, entretanto, é uma análise sobre a interferência dos códigos tecnológicos que constituem esse ciberespaço no sistema jurídico vigente.

Metodologicamente, o referencial teórico consiste no conceito de viver plenamente a lei, de Zenon Bankowski (2008), para investigar a tensão entre o legalismo e a legalidade das normas jurídicas. A técnica de análise metodológica é a de traços de significação, segundo Babbie (2007), que incorpora os elementos da realidade fática para propor uma ressignificação dos conceitos teóricos que guiam as normas.

A questão de pesquisa tem por intuito verificar as implicações que os códigos tecnológicos trazem para a formulação e aplicação de normas jurídicas que atuem sobre o ciberespaço. Ancorada no marco teórico de viver plenamente a lei e no estudo de caso da rede Tor, afirma-se como hipótese que a complexidade dos novos códigos tecnológicos deve ser considerada no processo de regulação do ciberespaço, sob o risco de se adotar o mero legalismo desconectado da realidade digital.

A fim de fundamentar a reconstrução crítica sobre o papel de programas de computador e da rede propõe-se o seguinte percurso: primeiramente, serão estruturados os referenciais teóricos e metodológicos e a sua importância para a análise pretendida. Em um segundo momento, haverá uma análise de literatura crítica sobre o estado da arte

na temática de direito e regulação do ciberespaço e o papel dos programas de computador nesse contexto. Por fim, haverá uma abordagem do paradigma da *deep web* e de como essa rede comporta, ao mesmo tempo, ações legítimas e ilícitas que desafiam as regras e os institutos jurídicos tradicionalmente conhecidos.

2 NORTE METODOLÓGICO E TEÓRICO

A metodologia aplicada a esta pesquisa consiste em uma análise por traços de significação da prática interpretativa do direito. O objetivo é o de compreender o significado latente de alguns elementos tecnológicos que interferem na regulação jurídica do ciberespaço e quais são as suas implicâncias para a inovação e para a legalidade.

A técnica de análise segue a dinâmica da pesquisa qualitativa por traços de significação, de acordo com Babbie (2007, p. 318). Seguindo essa técnica, a investigação se inicia por uma análise geral sobre o conteúdo escrito e disponível sobre o objeto pesquisado, no caso, a regulação jurídica dos ciberespaços. Em seguida, emprega-se o marco teórico para o exame de alguns elementos constituintes da realidade fática, contrapondo-os às hipóteses iniciais. Por fim, realiza-se uma reinterpretação jurídica do papel do direito perante o âmbito normativo puro e a realidade fática dessas tecnologias, apontando novas definições ao assunto.

Embora predominantemente teórica, a análise aqui desenvolvida é importante por estabelecer questionamentos sobre alguns aspectos relacionados à leitura jurídica das novas tecnologias. Como demonstrado por Feres e Oliveira (2016, pp. 17-8), a realidade tecnológica faz com que normas, como as de propriedade intelectual, estabeleçam regulações e definições sobre temas que constantemente evoluem, mas sem acompanhar esse ritmo de desenvolvimento. Assim, a análise por traços de significação possibilita uma abordagem crítica sobre o olhar do direito e sua capacidade evolutiva.

Para estabelecer essa investigação, o norte teórico utilizado é o de viver plenamente a lei de Zenon Bankowski (2008), especificamente pelo conceito de legalismo. Segundo o autor, o legalismo se estabelece quando as normas ganham uma

conotação objetiva e imutável, de maneira que as contingências da evolução da sociedade são colocadas em segundo plano (BANKOWSKI, 2008, pp. 40-5).

Assim, no legalismo, as regras são consideradas apenas em seu aspecto técnico puro e ganham um status praticamente inquestionável. Esse tom quase absoluto das regras faz com que, nos casos concretos, seja dada ênfase ao seu teor puro em vez do seu papel e contexto juntos à sociedade. É esse afastamento de seus pressupostos que faz com que a norma se interligue ao legalismo e não à legalidade (BANKOWSKI, 2008, p. 45).

Dessa maneira, viver plenamente o direito, de acordo com Bankowski (2008, pp. 71-81), significa um compromisso com a busca pela legalidade, ou adequação da norma às suas aspirações. A fim de atingir esse ideal, o direito não deve se reduzir à aplicação mecanicista da lei, mas sim se estender à análise de seu contexto real e das particularidades envolvidas para a sua efetivação. O processo de construção do direito exige uma compreensão profunda dos valores fundantes do sistema jurídico. Além disso, o sentido das normas jurídicas deve ser reconstruído a partir de fragmentos valorativos adequados ao contexto da comunidade.

Dessa forma, esse norte teórico se justifica pela sua capacidade reflexiva sobre o papel do direito junto à evolução da sociedade de tempos em tempos. Compreender os riscos atrelados ao legalismo permite enxergar o papel das instituições jurídicas para além da mera literalidade de suas expressões. Os ciberespaços e as novas tecnologias demandam, portanto, uma análise que comporte suas peculiaridades e não seja engessada a ponto de limitar o fluxo natural de evolução da sociedade por seus aparatos tecnológicos.

3 DEBATES SOBRE CIBERESPAÇO E INTERVENÇÃO JURÍDICA

Quando o tema é a capacidade de intervenção do direito sobre os espaços virtuais, existe uma dissonante discussão acerca do papel das normas e institutos jurídicos tradicionais.

Segundo Easterbook (1996, pp. 207-9), não se faz necessário criar um ramo do direito ou se preocupar com o caso específico do ciberespaço, já que as regras jurídicas gerais já são capazes de lidar com as circunstâncias particulares desse meio. Ele

estabelece uma analogia com um cavalo para explicar sua posição: não foi necessário criar uma doutrina ou legislação específica voltada apenas para lidar com esse tipo de animal (*law of the horse*), já que as normas gerais do direito – como as de compra e venda, indenização por acidente causado por cavalos, diretrizes para prêmios em competições de hipismo, entre outras – já foram capazes de atender às suas particularidades.

Para o autor, se o direito não conseguiu dirimir as divergências sobre tecnologias relativamente ultrapassadas, como as fotocópias e sua conciliação com o direito autoral, não haveria motivo para ele tentar se enveredar por mais uma seara em ascensão. Assim, Easterbrook argumenta que o esclarecimento e o reforço dos princípios de propriedade em vigência, aliados à criação de instituições próprias de negócios na internet, são medidas muito mais eficazes do que a criação de um novo direito cibernético (EASTERBROOK, 1996, pp. 210-6).

A visão de Johnson e Post (1996, pp. 1374-5) não segue essa linha de pensamento. De acordo com os autores, as medidas de regulação sobre os espaços virtuais não se adequam ao padrão próprio da rede, mas sim ao padrão físico tradicional. Dessa forma, o fenômeno da internet não poderia ser regulado por legislações baseadas em leis locais, já que sujeitos de várias partes do globo estão imediatamente envolvidos.

Eles argumentam que o mundo virtual alterou as relações de poder, os efeitos, a legitimidade e a capacidade de notificação (ou de ciência à observância de uma determinada jurisdição) que os governos têm sobre seus territórios locais. Se no mundo físico esses elementos seguem a força soberana de um Estado, no mundo virtual a rede de computadores subverteu essa lógica, por se tratar de uma dimensão global não circunscrita a uma localidade específica (JOHNSON; POST, 1996, pp. 1367-71).

Lessig (1999, pp. 501-3) concorda com Easterbrook no sentido de que as normas de regulação da internet devem ser capazes de se aplicar ao direito como um todo. Entretanto, ele destaca que se faz necessário considerar as particularidades do caso cibernético, já que esse fenômeno traz consigo consequências inéditas para a capacidade regulatória das normas jurídicas.

Conforme esse autor, o desenvolvimento do ciberespaço por meio de suas estruturas pode ocorrer de forma desregrada, de maneira que não comporte os valores tradicionais eleitos por uma determinada comunidade. Assim, esse espaço virtual e suas

particularidades próprias devem receber atenção especial do direito, já que o estabelecimento de uma mera regra não é capaz de atuar frente as complexidades da rede (LESSIG, 1999, pp. 548-9).

Já Goldsmith (1999, pp. 01-5) compreende as particularidades do ciberespaço, mas argumenta que as ferramentas tradicionais disponíveis para o universo jurídico são capazes de lidar com essas especificidades. O autor chama de céticos os que argumentam em sentido contrário e aponta que eles se fundam basicamente em dois argumentos: um sobre legitimidade e outro sobre a arquitetura própria da rede, utilizados para descredenciar posições em favor da capacidade interventiva do direito sobre a internet.

Ocorre, contudo, que para o autor esses argumentos não procederiam. As normas e soluções já existentes para conflitos e transações internacionais, aliadas à capacidade evolutiva da própria tecnologia, tornam possível regular os efeitos que uma conduta virtual gera sobre determinada jurisdição. Em sua essência, Goldsmith aponta que as transações virtuais não seriam diferentes das transações do mundo físico, já que ambas envolvem agentes existentes no espaço real e suas respectivas jurisdições. Logo, os efeitos de uma conduta oriunda do espaço virtual sobre uma nação seriam capazes de legitimar o seu interesse e sua capacidade de intervenção sobre esse espaço digital (GOLDSMITH, 1999, pp. 31-7).

Em resposta a esse pensamento, Post (2002, pp. 1365-9) estabelece dois tipos abordagens sobre direito e ciberespaço: a excepcional e a não-excepcional. Consoante sua classificação, Goldsmith e outros autores seriam não-excepcionalistas, por crerem na capacidade das normas tradicionais aliadas ao desenvolvimento da tecnologia para regular o ciberespaço, de modo que a internet não seria um fenômeno extraordinário para o direito. Já a posição contrária, da qual faz parte, seria de que a internet e as implicações por ela erigidas são tão inusitadas ao ponto de demandarem uma nova consideração do direito.

O principal argumento defendido por este autor é o de que a internet e as novas tecnologias constituem um fenômeno emergente, cujas normas e ferramentas tradicionais do direito não conseguirão atender de maneira satisfatória. Ele aponta que as leis e os princípios usuais devem ser respeitados em sua essência, mas que as tecnologias e a nova era digital clamam por uma reconsideração de suas diretrizes (POST, 2002, pp. 1386-7).

Já em outra obra, Lessig (2006, pp. 122-5) desenvolve, em mais detalhes, sua teoria sobre as particularidades do ciberespaço, asseverando que não somente a lei é capaz de intervir em comportamentos no mundo real e virtual, mas também outros três elementos: as normas, o mercado e a arquitetura própria do ciberespaço. As normas são elementos regulatórios na medida em que são consagradas no âmbito social e, embora não codificadas, são seguidas pelos indivíduos. No mercado, as estruturas de preço possuem um importante papel para moldar comportamentos coletivos e individuais. Já a arquitetura própria do ciberespaço, formada por softwares e hardwares que o constituem, é capaz de condicionar a maneira de acesso e de comportamento dos sujeitos na rede. Assim, o ambiente virtual correlaciona estes quatro âmbitos, tornando incompleta qualquer compreensão baseada em apenas um deles.

Como o objetivo da presente pesquisa é o de avaliar pormenorizadamente a quarta camada de regulação, a da arquitetura, e sua correlação com as demais, sobretudo a do direito, cumpre uma menção ao caso dos códigos (hardwares e principalmente softwares) que formam o ciberespaço e como a relação entre propriedade e regime jurídico são importantes para a discussão sobre a regulação dele.

Nesse sentido, Pressman (2010, p. 04-7) conceitua o software de computador como um sistema composto não por elementos físicos, mas lógicos, dotado de características peculiares. Assim, o software se difere de um componente físico, ou hardware, na medida em que é fruto de um característico processo de desenvolvimento, não se desgasta e é feito sob medida. Pela primeira característica, entende-se que o software não é manufaturado em sentido clássico. Quanto a não se desgastar, isto significa que o software não está sujeito às decomposições ambientais a que o hardware se expõe. Todavia, acaba por se deteriorar a cada falha, a qual indica um erro no processo de design ou na etapa de transmutação para um código a ser executável em uma máquina física. No que tange à terceira característica, ser feito sob medida, entende-se que o software não se baseia comumente em componentes já existentes, como nas indústrias em que peças são pré-moldadas. Aqui, ressalta o autor que a reutilização de um componente de software em larga escala para programas diferentes começou a se estender, contudo, ainda é incipiente.

Feita a conceituação, faz-se necessário entender qual o contexto real de aplicação do software na rede para, a partir deste ponto, compreender quais as

implicações geradas por esse elemento no ciberespaço. Ainda conforme Pressman (2010, p. 07-8), existem inúmeras maneiras de aplicação do software, como para a construção de sistemas, aplicações científicas, algoritmos de inteligência artificial, softwares embutidos para a indústria, aplicações para a internet, entre outros. Observa-se, desse modo, o enorme impacto que os programas de computador exercem sobre o meio digital.

Para as normas de propriedade intelectual, a proteção jurídica do software se desenvolve a partir da opção do programador por liberar ou restringir o acesso ao código-fonte de sua criação. Conforme Lee (2006, p. 49), o código-fonte é o formato de linguagem de programação utilizado pelos desenvolvedores de software, que permite a compreensão, modificação e adaptação de suas funcionalidades. Sua importância é essencial para a computação, pois ele é a principal via para alavancar o conhecimento contido em um programa.

O mesmo autor afirma se o criador do programa optar por restringir o acesso ao código-fonte, ele estará protegido pela via tradicional do copyright. Mas se a opção for por liberar o código-fonte, o programa será primeiramente protegido por copyright para, então, ter flexibilizadas as suas restrições para permitir o acesso e a edição de sua tecnologia. Neste caso, o regime jurídico seria o do *copyleft*, adotado nos softwares abertos e de código-fonte livre (LEE, 2006, pp. 49-51).

Esses regimes de proteção geram reflexos variados, desde a capacidade de aprendizado de informação básica dos programas de computador até a capacidade da regulação de seus efeitos por entes estatais. Segundo Ghaleb (2016, pp. 05), a disponibilidade do código-fonte é vital para o que se chama de engenharia reversa dos programas de computador. A engenharia reversa é o caminho de obtenção das funcionalidades do programa, sendo o processo basilar utilizado para o seu aprendizado.

Essa engenharia pode se dar por três caminhos: análise estática, análise dinâmica e análise híbrida. No primeiro caso, o programa é compreendido basicamente pelo seu código-fonte, enquanto no segundo, mesmo sem o código-fonte, é possível compreender alguns traços de funcionamento do software durante sua execução. A análise híbrida, por sua vez, é a que combina o código puro do programa com sua execução. Embora seja possível a análise dinâmica sem o código-fonte, algumas técnicas desse tipo de análise necessitam da sua obtenção para fornecer funcionalidades mais completas. Logo, o aprendizado de um software passa, em muito, por seu código-fonte (GHALEB, 2016, pp. 01-4).

É nesse ponto em que Lessig (2006, pp. 148-9) chamam a atenção para os desdobramentos que o tipo de código empregado nos softwares gera para a capacidade de intervenção e regulação jurídica. Para esse autor, embora os softwares fechados não sejam passíveis de compreensão de suas tecnologias por qualquer interessado, a capacidade de regulá-los é maior do que no caso dos softwares abertos. Como o software fechado é geralmente pertencente a grandes empresas do ramo de tecnologia, os Estados e órgãos de regulação conseguiriam controlá-las para que se adéquem aos seus desejos, sob pena de represálias econômicas ou políticas[4].

Já no caso dos softwares abertos, o caráter público de seu processo de desenvolvimento e de utilização faz com que não seja possível a apropriação exclusiva de suas funcionalidades por agentes privados. Ainda assim, mesmo que ocorra alguma ação de controle desse tipo de programa, a comunidade de desenvolvedores e usuários que o governam poderia migrar para outros projetos similares, de maneira que não é possível controlar seu dinamismo (LESSIG, 2006, p. 150).

Para compreender a diferença entre esses tipos de códigos e a capacidade de intervenção do direito, Lessig (2006, p. 150) estabelece a analogia do controle de conteúdo sobre um certo livro em um regime totalitário, como o da antiga União Soviética. Imagine que o Estado desejasse que todas as produções literárias possuíssem um capítulo sobre o então líder máximo, Stalin. No software aberto, essa obrigação seria plenamente contornável, pois essa menção obrigatória seria como um capítulo que pode ser ignorado sem prejuízo ao enredo da história, já que o software é adaptável. Já no software fechado, como o conteúdo do código não é disponibilizado, essa menção estaria atada de maneira persistente a toda a história, sobre a integralidade do software.

Nesse sentido, Grimmelmann (2005, pp. 1724-32) ressalta que o software tem natureza institucional regulatória, o que faz com que ele condicione as atividades realizadas no âmbito virtual. Seus códigos são capazes de intervir no mundo digital ao estabelecerem regras observáveis para os sistemas de operação, de transmissão e de armazenamento de informação. Dessa maneira, o programa de computador desempenha uma essencial função na demarcação do ciberespaço.

[4] Exemplo é o do governo totalitarista chinês, que condicionou as empresas do ramo de tecnologia, como a Microsoft, Yahoo e Google a se adequarem ao regime de controle ou filtragem de certas informações consideradas como indevidas pelo Estado (LESSIG, 2006, p. 79).

Estabelecidas essas discussões iniciais, faz-se necessário aplicar a óptica teórica de Bankowski (2008) para o papel das normas jurídicas no ciberespaço. Como demonstra o autor, o legalismo é observável quando se estabelece uma aceitação cega das regras por si mesmas, sem atenção ao contexto que as envolve.

A crença na capacidade das normas tradicionais do direito para lidarem com o fenômeno complexo do ciberespaço, como visto em Easterbrook (1996) e Goldsmith (1999), pode revelar mais do que um otimismo com a eficiência das leis atualmente em vigência. Essa crença dá indícios de um apego às normas tradicionais, incapaz de reconhecer o elemento pulsante da evolução tecnológica como transformador da realidade humana.

Assim, a teoria de viver plenamente a lei (BANKOWSKI, 2008) se torna relevante para analisar a necessidade de evolução das normas frente aos novos contextos. Os códigos tecnológicos e a complexidade envolvida em seu desenvolvimento e regulação demonstram que o direito precisa ter maior atenção com a arquitetura do ciberespaço, para incorporá-la no seu escopo regulatório. Caso contrário, a lei será apenas uma norma literal, sem conexão com o meio tecnológico que a envolve.

Verifica-se, assim, que, embora existam algumas divergências sobre a capacidade de intervenção das normas jurídicas sobre o ciberespaço, os componentes de sua arquitetura são importantes elementos para se alcançar uma compreensão integrada de seu funcionamento. Dessa maneira, o regime de propriedade intelectual adotado pode interferir na capacidade regulatória de Estados e agentes que busquem estabelecer limites a esse espaço.

Partindo-se desses pressupostos, a análise sobre o fenômeno da rede Tor na *deep web* serve para reforçar o caráter complexo da regulação no contexto do ciberespaço.

4 SOFTWARE, CÓDIGO E REGULAÇÃO: O CASO DA REDE TOR

Uma vez estabelecida a conexão entre a forma de propriedade intelectual pretendida para um software e a capacidade de regulação sobre o mesmo, cumpre abordar a *deep web* a partir de desdobramentos da rede Tor. A investigação dessa rede é

paradigmática, por revelar como os códigos que compõem o ciberespaço condicionam a capacidade de intervenção do direito.

A primeira tarefa dessa abordagem é conceitual: o que seria *deep web*? De acordo com He at al. (2007, p. 95), a *deep web* (ou internet profunda) é basicamente uma rede invisível para os mecanismos de busca de internet comuns, como o Google, o Yahoo ou o Bing. Enquanto na internet comumente conhecida (*surface web* ou internet superficial) uma informação é encontrada graças a links estáticos, na internet profunda as páginas são listadas como respostas pertencentes a um banco de dados oculto. Assim, na internet superficial esses navegadores comuns não possuem a expertise técnica necessária para retornar de forma eficiente os resultados contidos nessas bases de dados e esse conteúdo permanece fora de seu alcance.

Da mesma forma, Bright Planet (2013, pp. 01-3), empresa especializada em exploração de conteúdo da *deep web*, afirma que os mecanismos comuns de busca podem direcionar o usuário a um site com conteúdo da rede profunda, mas não conseguem retornar resultados específicos desse conteúdo.

A rede Tor é uma das mais populares para acessar a *deep web*. Conteúdos alocados dentro dessa rede são acessados basicamente por meio de um navegador específico, o Tor Browser. O Tor é um software de código aberto, a saber, a compreensão e o desenvolvimento dele estão disponíveis para quaisquer interessados no projeto (TOR PROJECT, 2017a). Como explicam Feres e Oliveira (2016, pp. 14-5), a grande particularidade da rede e do software Tor em relação aos navegadores e às redes comuns é que eles garantem dois atributos para o uso da internet: a privacidade, representada pela proteção dos dados do usuário, e o anonimato, representado pela proteção da identidade do usuário.

Assim, enquanto na web comum é possível identificar e rastrear o usuário pelo seu número de IP[5], na internet profunda essa informação fica oculta por criptografia[6], onde a conexão do usuário é feita mediante várias retransmissões (TOR PROJECT, 2017a). A principal ferramenta responsável por resguardar os dados do usuário e da

[5] *Internet Protocol* é um protocolo de rede formado por números e seu funcionamento é similar ao de um endereço, indicando a origem da conexão dos computadores que acessam a rede (LESSIG, 2006, p. 43).

[6] Soares e Veronese (2007, p. 12) explicam que a criptografia é uma aplicação da criptologia, ciência matemática, que equilibra comunicação e segredo. Ela viabiliza a segurança na troca de mensagens na internet em geral, sendo que seus algoritmos possibilitam controle na transmissão de mensagens e conteúdo.

página alocada nessa rede é a dos chamados *hidden services* (serviços ocultos). Essa ferramenta possibilita que o criador de uma página ou serviço alocado na rede Tor, como serviços de mensagem ou websites, esconda sua posição geográfica, de maneira que se torne difícil rastreá-lo (TOR PROJECT, 2017b).

Como todas as informações acima possuem certa complexidade, estabelece-se a seguinte analogia para esclarecer a diferença entre a rede Tor, contida na internet profunda, e a rede comum superficial. Imagine, primeiramente, que os destinos contidos na internet superficial e na rede Tor são como endereços físicos e que os navegadores são como formas para o transporte desses usuários aos endereços desejados.

Na rede comum, o usuário utiliza-se de seu navegador identificado pelo número de IP e trafega pela rede com o auxílio de links para atingir o website desejado. Por analogia, o navegador é uma espécie de automóvel, o número de IP é a placa de seu carro, os links são placas de direção na estrada e o website é o destino final. Dessa forma, durante todo o seu percurso o usuário pode ser facilmente identificado pela placa de seu automóvel e responsabilizado por suas condutas no trânsito.

Já para acessar a rede Tor, contida na *deep web*, o usuário se utiliza de um navegador específico, o *Tor Browser*, que criptografa seu número de IP. Ele estabelece seu acesso por meio de várias conexões interligadas, a rede Tor, para atingir seu destino final sem o auxílio necessário de links do buscador. Pela mesma analogia, o usuário seria um passageiro de metrô e, portanto, não identificável pelos transeuntes como no caso da placa de automóvel. Além disso, o seu trajeto se interconecta e é redistribuído em várias linhas subterrâneas até atingir seu destino final, um site da rede Tor. Logo, o rastreamento desse usuário e de suas condutas é muito difícil, senão impossível.

Por possibilitar a privacidade e o anonimato de seus usuários a partir dos *hidden services*, a rede Tor é usualmente associada às atividades ilícitas. Bright Planet[7] (2013, p. 03) destaca que a rede Tor atrai usuários para fins como pornografia infantil, venda de substâncias ilícitas, lavagem de dinheiro, entre outras condutas ilegais.

[7] Ainda de acordo com a empresa, a rede Tor estaria inserida dentro da chamada *dark web* ou internet escura, cujo conteúdo foi intencionalmente ocultado. Assim, a rede Tor seria uma componente da *dark web*, uma parte perigosa da *deep web* (BRIGHT PLANET, 2013, pp. 01-3). O nome internet escura ou *dark web* traz, portanto, uma conotação negativa para redes como a Tor. Ele deixa a impressão de que apenas atividades ilícitas são desenvolvidas em seu meio. É nesse ponto, contudo, que o presente estudo diverge: como será visto, essa concepção de uso único para fins criminosos não procede. Dessa maneira, preferiu-se por não empregar o conceito *dark web* no artigo.

No Brasil, a partir de uma busca[8] direcionada aos sites das instâncias máximas do poder judiciário, o Superior Tribunal de Justiça e o Supremo Tribunal Federal, verificou-se um caso público identificado ao uso indevido da *deep web*.

No recurso ordinário em habeas corpus, RHC 56005/SP, julgado em 2015, cujo provimento do acórdão do Superior Tribunal de Justiça foi denegatório, analisou-se o uso da rede profunda para fins de pornografia infantil. Nesse caso, o emprego da *deep web* foi considerado como elemento potencializador da multinacionalidade do delito, como se pode verificar:

> RECURSO ORDINÁRIO EM HABEAS CORPUS. PRODUÇÃO E FOTOGRAFIA DE CENA PORNOGRÁFICA ENVOLVENDO CRIANÇA, DIVULGAÇÃO DE IMAGENS OU FOTOGRAFIAS COM CONTEÚDO PORNOGRÁFICO INFANTIL E ARMAZENAMENTO DE ARQUIVOS CONTENDO CENAS OU IMAGENS PORNOGRÁFICAS OU DE SEXO EXPLÍCITO ENVOLVENDO CRIANÇAS OU ADOLESCENTES. UTILIZAÇÃO DE FÓRUNS NA INTERNET E SITE EM REDE OCULTA NA INTERNET. TRANSNACIONALIDADE DO DELITO. COMPETÊNCIA DA JUSTIÇA FEDERAL.
>
> (...)
>
> 4. Na hipótese em apreço, a forma como o recorrente disponibilizaria, transmitiria, publicaria e divulgaria arquivos contendo pornografia ou cenas de sexo explícito envolvendo crianças ou adolescentes permitira o seu acesso por pessoas em qualquer local do mundo, bastando que também participassem dos mesmos fóruns que ele, **ou que também acessassem sites na rede oculta chamada *deep web***, circunstância que revela a transnacionalidade da conduta narrada na exordial acusatória e justifica a competência da Justiça Federal para processar e julgar o feito (BRASIL, 2015, grifo próprio).

O julgado não revela se o infrator se utilizava da rede Tor ou qual a maneira de persecução que os órgãos legais utilizaram para identificá-lo. Entretanto, como visto em

[8] Os termos "*deep web*" e "navegador Tor" foram pesquisados em 01 de junho de 2017 diretamente nos serviços de busca de jurisprudência dos respectivos tribunais. O link <http://www.stj.jus.br/SCON> foi acessado para a pesquisa de jurisprudência do STJ e o link <http://www.stf.jus.br/portal/jurisprudencia/pesquisarJurisprudencia.asp> para o STF.

Bright Planet (2013), o uso de fóruns ou páginas nessa rede são plenamente possíveis para esse fim, com o auxílio do anonimato e da privacidade.

Sem entrar no mérito do delito, a citação dessa jurisprudência serve para iniciar o debate sobre a potencialidade da rede Tor e sobre como os seus códigos interferem na capacidade de regulação do direito. As perguntas que se estabelecem a partir desse ponto são as seguintes: seriam a *deep web* e a rede Tor utilizadas somente para fins ilícitos? Para quais fins se justificaria o desenvolvimento colaborativo de um software livre que provê privacidade e anonimato para o uso da internet? Para responder a essas perguntas, cumpre abordar o segundo exemplo de uso da *deep web*, o site wEYE.

O wEYE[9] é uma plataforma de defesa de direitos humanos na internet, que se utiliza do anonimato e privacidade da rede Tor para o recebimento de vídeos que denunciem violações à dignidade humana ao redor do mundo. Como a censura em regimes ditatoriais se torna um dos grandes obstáculos para a luta por direitos humanos, a plataforma disponibiliza um link[10] na *deep web*, por meio da rede Tor, para a postagem de vídeos colaborativos oriundos de todas as partes do mundo (WEYE, 2017).

Nesse caso em específico, os atributos de anonimato e privacidade da rede e do navegador Tor são utilizados para a promoção dos direitos humanos, principalmente em países onde há regimes totalitários, assim como censura e controle do acesso dos cidadãos à internet (TOR, 2017c). No caso do wEYE, é possível identificar vídeos enviados de países como Uganda, Filipinas e Paquistão. Além do anonimato garantido pela arquitetura da rede Tor, o serviço conta com um processo de dois passos de envio e de verificação do conteúdo dos vídeos que recebe. Esse processo envolve especialistas do mundo todo que trabalham em busca da autenticidade tanto do material recebido quanto do fato denunciado (WEYE, 2017).

O exemplo da plataforma é apenas um entre outros vários usos justos e lícitos da arquitetura da rede Tor. Outros exemplos são pessoas normais em busca de privacidade online, ativistas das mais variadas causas, militares, jornalistas e profissionais de tecnologia da informação (TOR, 2017c).

De acordo com a análise empírica de Biryukov et al (2014, p. 06), o número de atividades que utilizam os serviços ocultos da rede Tor para fins ilícitos (como mercados de drogas, pornografia infantil ou compra de armas) e lícitos (como atividades em prol dos direitos humanos, pesquisa, liberdade de expressão) é equiparado. Esses

[9] Website: <http://www.weye.info/about>.
[10] Endereço (disponível apenas via Tor): <ydtjl5cn3smvsork.onion>.

autores constatam que o uso dos serviços da rede é variado, de maneira que não é possível fixar um perfil único de "subversivo" aos usuários do serviço.

Trabalhados esses dois exemplos de uso da *deep web* e da rede Tor, a última etapa de análise se desenvolve pela conjunção dos códigos próprios da rede Tor e a capacidade de sua regulação jurídica frente ao marco teórico adotado.

De acordo com Lessig (2006, pp. 122-5), existem quatro camadas constituintes do ciberespaço, capazes de interferir nos comportamentos dos sujeitos. O autor, contudo, não se dedica ao fenômeno da *deep web*, de maneira que se torna pertinente conceituá-la frente a sua classificação para entender como essas camadas se articulam. Trabalhadas comparativamente para o caso da rede Tor, tem-se a seguinte ilustração na Tabela 1:

Tabela 1: Elementos de regulação de comportamento na rede superficial e profunda

Rede	Lei	Norma	Mercado	Arquitetura
Internet Superficial	✓	✓	✓	✓
Rede Tor	✗	✓	✓	✓

Fonte: Elaboração própria dos autores

Dos quatro elementos estabelecidos por Lessig, a rede Tor afeta diretamente na constituição de um elemento: a lei. Isso não significa que seja impossível às autoridades processarem ou irem em busca de um usuário dessa rede que cometa uma infração[11]. Significa, entretanto, que sua arquitetura própria é moldada de maneira a ocultar a identidade do usuário da rede, o que dificulta ou inviabiliza por completo a intervenção do direito.

Dessa forma, imagine a dificuldade em aplicar, a partir de uma interação entre indivíduos que utilizem a rede Tor, a tradicional classificação dos elementos da relação jurídica, conforme os estudos de introdução ao direito.

Conforme Pinto (1985, p. 181), toda a relação jurídica possui quatro elementos: sujeito, objeto, fato jurídico e garantia. Os sujeitos integram os polos ativo e passivo da relação e são condições mínimas para a sua intercorrência. O objeto é o fim sobre o qual

[11] Vide o exemplo do mercado de drogas e produtos ilícitos Silk Road. O site, que funcionava na rede Tor, atingiu a marca de dezenas de milhões de dólares em vendas e foi acompanhado pela inteligência do serviço secreto americano e fechado em 2013 pelo FBI (ALDRIDGE; DÉCARY-HÉTU, 2014, p. 01-6).

a relação se estabelece. Já o fato que decorre dessa interação e é relevante ao direito é chamado de fato jurídico. Por fim, a garantia apresenta-se como um conjunto de providências coercitivas do sujeito ativo a fim de evitar a violação do direito (PINTO, 1984, p. 183).

Analisados sob a perspectiva das relações ocorridas na rede Tor na *deep web*, essa clássica definição de relação jurídica fica prejudicada, no mínimo, quanto aos sujeitos (cuja identidade é criptografada) e à garantia (uma vez que pela localidade oculta, os serviços ocultos da rede Tor inviabilizam o sujeito ativo de obrigar uma prestação do sujeito passivo). Isso não significa que sujeitos, seu objeto, fato jurídico e até mesmo a garantia jurídica de um contrato lícito cessem de existir no espaço real, mas simplesmente que é muito difícil identifica-los ou imputar-lhes a responsabilidade sobre certa conduta.

Desse modo, devido à criptografia do navegador e aos serviços ocultos da conexão, a rede Tor impede ou dificulta que alguns elementos da relação jurídica, que é a manifestação dos efeitos concretos da lei, possam ser efetivados em seu âmbito.

Entretanto, como expõem Aldridge e Décary-Hétu (2014) e Biryukov et al. (2014), a arquitetura própria dessa rede comporta outras dimensões à exceção da legal: ela possibilita a criação de mercados e não veda o estabelecimento de normas próprias de conduta dentro de seus sites e serviços.

Nesse sentido, verifica-se que o ciberespaço comporta inúmeras particularidades e é constituído por um jogo próprio de códigos, como softwares e conexões, que interferem ou até inviabilizam atividades de regulação ou intervenção do direito.

Tudo isso se inicia pela simples escolha da forma de proteção do código-fonte de um programa, que pode interferir em inúmeros aspectos do ciberespaço. Os regimes de propriedade intelectual, como o copyright ou o *copyleft*, são ferramentas jurídicas que interferem diretamente na disseminação de um programa e na sua capacidade de intervenção e repercussão na sociedade tecnológica.

Como abordado por Lessig (2006, 148-9), os softwares de código aberto são mais difíceis de serem regulados, uma vez que não são centralizados ou governados por agentes com fins unilaterais. Esses softwares, como o navegador de código aberto Tor, podem ser desenvolvidos por uma comunidade global e multifacetada, de caráter flexível e heterogêneo em sua constituição. Portanto, o exemplo da rede Tor demonstra que é impossível falar em regulação jurídica do ciberespaço sem levar em consideração os aspectos técnicos dos códigos que o compõem.

A rede Tor nada mais é do que um veículo poderoso de comunicação. Como todo veículo ou toda criação humana, é possível identificar usos devidos e indevidos de seus atributos. Porém, seja para coibir condutas ilegais ou seja para incentivar espaços de autonomia moral e luta por direitos mínimos, essa ferramenta precisa antes de mais nada ser incorporada pelo direito e pelo Estado democrático como um elemento constituinte da sociedade tecnológica.

Aplicando-se a perspectiva teórica de Bankowski (2008, pp. 40-5) para o caso do ciberespaço, constata-se que viver plenamente a lei significa muito mais do que a mera defesa de institutos jurídicos tradicionais. Viver plenamente a lei em tempos digitais é uma tarefa que demanda o questionamento constante dos dogmas e das regras jurídicas, sejam elas relativas à propriedade intelectual ou a outras especialidades do direito, de modo a verificar se os seus conteúdos estão em conformidade com os valores consagrados na atual sociedade digital.

Dessa forma, a estrutura legal que atribui aos programas de computador uma natureza jurídica de propriedade exclusivista ou aberta gera reflexos imediatos na lógica de controle regulatório da rede. Essa estrutura é capaz de interferir em fenômenos variados, desde o compartilhamento e acesso ao conhecimento até o controle de Estados sobre as novas tecnologias.

Sabendo que a sociedade da informação e as novas tecnologias são, hoje, componentes estruturais da complexidade do real, é essencial se rever a tradicional dinâmica legalista. O fenômeno cibernético é capaz de extrapolar as escalas e os limites tradicionais das relações jurídicas, de modo que, se o direito insistir no legalismo da aplicação de tradicionais institutos e regras consagrados em outros tempos, acaba por ser superado pela complexidade do real advinda dos novos valores sociais refletidos nos ciberespaços.

O que a *deep web* e a rede Tor demonstram é que o descredenciamento ou a criminalização de sua existência em nada irão cooperar para um direito mais coerente e contextualizado para os novos tempos.

CONSIDERAÇÕES FINAIS

Esta pesquisa se dedicou a uma investigação sobre o ciberespaço e as implicações que esse ambiente virtual traz para o direito. O plano teórico empregado foi o de viver plenamente a lei, de Zenon Bankowski e a técnica de análise foi a de traços de significação. Procurou-se estruturar um sistema analítico de conceitos para se reconstruir o sentido do fundamento, da função e da finalidade dos institutos jurídicos frente às novas tecnologias.

Os casos analisados guardam relação com a rede Tor e a maneira incomum como esse canal de interação opera sobre as estruturas de mercado, normas sociais e a lei. Constatou-se que, como qualquer criação humana, essa rede pode ser usada tanto para fins ilícitos quanto para objetivos legítimos, sem uma necessária prevalência de um lado ou de outro.

Verificou-se ainda que, embora haja o debate sobre a capacidade das normas jurídicas de intervir no ciberespaço, a camada conhecida como *deep web* demonstra o quão poderosa pode ser a arquitetura dos códigos que compõem a internet, limitando até o potencial de identificação dos envolvidos e, consequentemente, de intervenção do direito nas condutas humanas.

Assim, cumpre apontar como caminho não uma lei específica e direcionada estritamente para conter abusos no ciberespaço, mas sim uma necessária atualização do sistema jurídico para as novas tecnologias. Ao compreender a capacidade e a complexidade envolvida nos códigos tecnológicos, as medidas regulatórias podem trazer novas perspectivas para que as legislações se atualizem aos novos tempos.

REFERÊNCIAS

ALDRIDGE, Judith. DÉCARY-HÉTU, David. Not an 'Ebay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. *Social Science Research Network*, maio de 2014. Disponível em: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2436643>. Acesso em: 03 maio 2017.

BABBIE, Earl. *The Practice of Social Research.* Eleventh Edition. Belmont: Thomson Wadsworth, 2007.

BANKOWSKI, Zenon. *Vivendo Plenamente a Lei.* Rio de Janeiro: Elsevier Brasil, 2008. 289 p.

BIRYUKOV, Alex. PUSTOGAROV, Ivan. THILL, Fabrice. WEINMANN, Ralf-Philipp. *Content and popularity analysis of Tor hidden services*. arXiv:1308.6768v2 [cs.CR], 17 Nov 2014. Disponível em: <https://arxiv.org/pdf/1308.6768.pdf>. Acesso em 04 jun. 2017.

BRASIL. Superior Tribunal de Justiça. *Recurso Ordinário em Habeas Corpus, RHC 56005/SP*. Min. Rel. Jorge Mussi, Quinta Turma. Data do Julgamento: 21 de maio de 2015.

BRIGHT PLANET. *Understanding the Deep Web in 10 Minutes*. Whitepaper disponível em: <http://bigdata.brightplanet.com/hs-fs/hub/179268/file-22990148-pdf/docs/deep_web_whitepaper_v3_for_approval.pdf>. Acesso em 05 mar. 2017.

EASTERBROOK, Frank H. Cyberspace and the Law of the Horse. *University of Chicago Legal Forum*, n. 208, 1996.

FERES, Marcos Vinício Chein; OLIVEIRA, Jordan Vinícius de. Precisamos Falar sobre Copyright: o que Creative Commons, Open Access e Deep Web têm em Comum? *Revista de Propriedade Intelectual, Direito Contemporâneo e Constituição,* vol. 10, ed. 03, pp. 01-20. DOI: < http://dx.doi.org/10.16928/2316-8080.V10N03p.001-020>.

FREITAS, Christiana Soares de. VERONESE, Alexandre. Segredo e Democracia: certificação digital e software livre. *IP. Informática Pública*, v. 8/2, p. 09-26, 2007.

GHALEB. Taher Ahmed. The role of open source software in program analysis for reverse engineering. *2nd International Conference on Open Source Software Computing (OSSCOM)*, Beirut, 2016, pp. 1-6. DOI: <10.1109/OSSCOM.2016.7863684>. Acesso em 24 maio 2017.

GOLDSMITH, Jack L. Against Cyberanarchy. *University of Chicago Law Occasional Paper*, n. 40, 1999.

GRIMMELMANN, James (2005). Regulation by Software. *The Yale Law Journal*, Vol. 114, No. 7, pp. 1719-1758. Recuperado em 5 de maio de 2017, de <http://www.jstor.org/stable/4135763>.

JOHNSON, David R. POST, David G. Law And Borders: The Rise of Law in Cyberspace. *Stanford Law Review*, n. 48, 1996. Disponível em: <http://www.cli.org/X0025_LBFIN.html>. Acesso em 17 abril 2017.

LEE, Jyh-An. New Perspectives on Public Goods Production: Policy Implications of Open Source Software. *Vanderbilt Journal of Entertainment and Technology Law* [Vol. 9:1:45], 2006. Disponível em: <http://ssrn.com/abstract=963491>. Acesso em: 15 maio 2017.

LESSIG, Lawrence. The Law of the Horse: What Cyberlaw Might Teach. *Harvard Law Review*, Vol. 113, No. 2, pp. 501-549. Recuperado em 30 de setembro, 2012, de <http://www.jstor.org/stable/1342331>.

_____. *Code (version 2.0)*. Nova Iorque: Basic Books, 2006. 411p. ISBN-10: 0–465–03914–6. ISBN-13: 978–0–465–03914–2.

PINTO, Carlos Alberto da Mota. *Teoria Geral do Direito Civil*. Coimbra: Coimbra Editora, 3ª ed, 1985.

POST, David G. Against 'Against Cyberanarchy'. *Berkeley Technology Law Journal, Vol. 17, p. 1365, 2002*. Disponível em Social Science Research Network: <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=334581>. Acesso em 23 abril 2017.

PRESSMAN, Roger. *Software Engineering*: a Practitioner's Approach. Seventh Edition. New York: McGraw-Hill, 2010.

TOR PROJECT. *Frequently Asked Questions*. (2017a). Disponível em: <https://www.torproject.org/docs/faq.html.en>. Acesso em: 02 jun. 2017.

_____. *Tor: Hidden Service Protocol*. (2017b). Disponível em: <https://www.torproject.org/docs/hidden-services.html.en>. Aceso em: 01 jun. 2017.

_____. *Users of Tor*. (2017c). Disponível em: <https://www.torproject.org/about/torusers.html.en>. Acesso em 30 maio 2017.

WEYE. *About.* wEYE - The Video Platform For Human Rights. Disponível em: <http://www.weye.info/about>. Acesso em 30 mar 2017.

RECEBIBO 05/06/2017
APROVADO 15/06/2017
PUBLICADO 01/07/2017