

**UNIVERSIDADE ESTADUAL PAULISTA “JÚLIO DE MESQUITA FILHO”
FACULDADE DE CIÊNCIAS HUMANAS E SOCIAIS**

GUSTAVO ALARCON RODRIGUES

**ANÁLISE DAS *BLOCKCHAINS* E TECNOLOGIAS CORRELATAS
COMO FORMAS DE GARANTIA E EFETIVAÇÃO DOS DIREITOS À
PRIVACIDADE E À LIBERDADE NA *INTERNET***

**FRANCA
2021**

GUSTAVO ALARCON RODRIGUES

**ANÁLISE DAS *BLOCKCHAINS* E TECNOLOGIAS CORRELATAS
COMO FORMAS DE GARANTIA E EFETIVAÇÃO DOS DIREITOS À
PRIVACIDADE E À LIBERDADE NA *INTERNET***

Dissertação apresentada à Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, como pré-requisito para obtenção do Título de Mestre em Direito

Área de Concentração: Tutela e Efetividade dos Direitos da Cidadania

Orientadora: Prof.^a Dr.^a Patrícia Borba Marchetto

**FRANCA
2021**

R696a

Rodrigues, Gustavo Alarcon

Análise das Blockchains e tecnologias correlatas como formas de garantia e efetivação dos direitos à privacidade e à liberdade na internet / Gustavo Alarcon Rodrigues. -- Franca, 2021

214 p.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Faculdade de Ciências Humanas e Sociais, Franca
Orientadora: Patrícia Borba Marchetto

1. Blockchains. 2. Tecnologias descentralizadas. 3. Criptoativos. 4. Privacidade. 5. Liberdade. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca da Faculdade de Ciências Humanas e Sociais, Franca. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

GUSTAVO ALARCON RODRIGUES

**ANÁLISE DAS *BLOCKCHAINS* E TECNOLOGIAS CORRELATAS
COMO FORMAS DE GARANTIA E EFETIVAÇÃO DOS DIREITOS À
PRIVACIDADE E À LIBERDADE NA *INTERNET***

Dissertação apresentada à Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho” como pré-requisito para obtenção do Título de Mestre em Direito. Área de Concentração: Tutela e Efetividade dos Direitos da Cidadania.

BANCA EXAMINADORA

Presidente: _____
Prof.^a Dr.^a Patrícia Borba Marchetto

1º Examinador: _____
Prof. Dr. Gustavo Silveira Borges

2º Examinador: _____
Prof. Dr. Fernando Andrade Fernandes

Franca, 19 de novembro de 2021.

Dedico este trabalho ao meu pai, Edmilson, e à minha mãe, Luciana. Como não dedicar esse momento àqueles que são a minha rocha, a minha fortaleza, onde encontro forças todos os dias para continuar.

AGRADECIMENTOS

Agradeço, em primeiro lugar, a Deus, que iluminou o meu caminho durante esta caminhada.

Agradeço à minha Orientadora, Professora Dra. Patrícia Borba Marchetto, pela paciência na orientação e auxílio constante no desenvolvimento deste trabalho. Mais que isso, pelo carinho, apreço e constante ímpeto em auxiliar, mostrando-se sempre presente, seja para auxiliar na pesquisa ou para ter uma conversa amigável. Agradeço pelos ensinamentos que, com dedicação, foram a mim passados, orientando-me, não somente na vida acadêmica, mas também uma série de valores que levarei comigo.

Agradeço aos demais professores da casa, que me auxiliaram a alcançar a luz do conhecimento e adentrar, vigorosamente, no estudo do Direito, em especial, aos Professores Fernando e Jorge, pelos valorosos ensinamentos que contribuíram diretamente para a construção desse trabalho.

Agradeço, também, ao Professor Doutor Jefferson Bertolai, pelas excelentes discussões e indicações que contribuíram diretamente para a pesquisa aqui apresentada.

Agradeço a todos meus amigos, em especial, Giovanni, Gustavo, Leonardo, Octavio, Otávio, Isabela, Luísa. Obrigado pelas alegrias que passamos juntos e por todo o apoio durante as dificuldades. Aos meus colegas de orientação, agradeço pelo valoroso apoio em todos os momentos.

Agradeço aos meus familiares, avós, padrinhos, tios e primos, que acreditaram em mim e permitiram, nos menores detalhes, que eu traçasse o caminho que me trouxe até aqui.

Agradeço, por fim, à Universidade Estadual Paulista “Júlio de Mesquita Filho”, tão gentil alma mater, que me acolhe em seus braços desde minha Graduação.

“Liberdade é liberdade de dizer que dois mais dois são quatro.”

ORWELL, 2021

RODRIGUES, Gustavo Alarcon Rodrigues. **Análise das *Blockchains* e tecnologias correlatas como formas de garantia e efetivação dos direitos à privacidade e à liberdade na *internet*.** 2021. 214 f. Dissertação (Mestrado em Direito) – Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Franca, 2021.

RESUMO

A pesquisa em questão trata de uma análise jurídica das *Blockchains*, criptoativos e tecnologias correlatas voltadas para a compreensão do seu potencial de serventia à dinâmica de tutela e efetividade de direitos humanos dentro dos ambientes virtuais, tendo como base, para os ensaios aqui pretendidos, a compreensão das referidas tecnologias como formas privadas de garantia de direitos nos ambientes virtuais, as novas roupagens presentes nos direitos humanos e, também, a crise de legalidade e legitimidade reinante no ambiente digital. Busca-se demonstrar como as *Blockchains* e tecnologias correlatas tutelam, por intermédio de estruturas descentralizadas, os direitos de liberdade e privacidade dos utilizadores da rede, de forma nativa ao ambiente digital. Parte-se, portanto, de um referencial geral acerca da técnica informacional, sua potencialidade e concretude lesiva à dinâmica de direitos fundamentais, visando demonstrar como a *Internet* instaura um ambiente juridicamente *sui generis*, com reduzida capacidade e aptidão para prover direitos no mundo dos átomos para aqueles ambientes digitais, pautando-se em uma remodelação do poder de fato. Posteriormente, fazendo uso de literatura especializada e geral, busca-se compreender a capacidade das *Blockchains* e tecnologias correlatas responderem a tal dinâmica supressiva de direitos, apresentando as características que marcam seu funcionamento e, dentro dessa análise, conduzindo para a correlação dessas novas tecnologias com a garantia do direito à liberdade, direito à privacidade na rede mundial de computadores. A pesquisa adota como base metodológica o método hipotético-dedutivo, partindo da questão problema para a composição da hipótese primária, visando o alcance dos objetivos pré-definidos. A hipótese será sujeita à avaliação por meio de imersão em robusto embasamento teórico para, dessa forma, comprovar sua possibilidade. A conclusão a que se chega é que a natureza algorítmica e automática das medidas empreendidas pelas referidas tecnologias teria potencial de tutela dos direitos de privacidade e liberdade no ambiente digital, ainda que haja pontos de fragilidades e pontos cuja alteração se faça necessária para a integração ao ordenamento jurídico.

Palavras-chave: *Blockchains*. Tecnologias descentralizadas. Criptoativos. Privacidade. Liberdade.

RODRIGUES, Gustavo Alarcon. **Analysis of Blockchains and related technologies as ways to guarantee and enforce privacy and liberty rights on the internet**. 2021. 214 f. Dissertação (Mestrado em Direito) – Faculdade de Ciências Humanas e Sociais, Universidade Estadual Paulista “Júlio de Mesquita Filho”, Franca, 2021.

ABSTRACT

The dissertation in question is a legal analysis of Blockchains, cryptoactives and related technologies aimed to understanding their potential to serve as a dynamic of protection and effectiveness of human rights within virtual environments. It is based on the essays aiming to understanding these technologies as private ways of guaranteeing rights in virtual environments, the new dresses of human rights and the crisis of legality and legitimacy that reigns in the digital environment. It seeks to demonstrate how Blockchains and related technologies protect, through decentralized structures, the rights of freedom and privacy of network users, natively to the digital environment. It starts, therefore, from a general reference about the informational technique, its potential and harmful concreteness to the dynamic of fundamental rights, aiming to demonstrate how the *Internet* establishes a legally sui generis environment, with reduced capacity and ability to provide rights in the world of atoms for those digital environments, based on a remodeling of de facto power. Subsequently, using specialized and general literature, we seek to understand the capacity of Blockchains and related technologies to respond to such suppressive dynamics of rights, presenting the characteristics that mark their operation and, within this analysis, leading to the correlation of these new technologies with the guarantee of the right to freedom, right to privacy on the world wide web. The research adopts as methodological basis the hypothetical-deductive method, starting from the problem question to the composition of the primary hypothesis, aiming to reach the pre-defined objectives. The hypothesis will be subject to evaluation by means of immersion in a solid theoretical foundation, in order to prove its possibility. The conclusion reached is that the algorithmic and automatic nature of the measures undertaken by these technologies would have the potential to protect the rights of privacy and freedom in the digital environment, even though there are weak points whose alteration is necessary for integration to the legal framework.

Key words: Blockchains. Decentralized technologies. Cryptoactives. Privacy. Liberty.

LISTA DE ABREVIATURAS E SIGLAS

CEPI	Centro de Ensino e Pesquisa em Inovação
DLT	Distributed Ledger Technology, tecnologia de registro distribuído
EU	União Europeia
EUA	Estados Unidos da América
FBI	Federal Bureau Investigation
FISA	United States Foreign Intelligence Surveillance Court
GDPR	General Data Protection Regulation
INC	Instituto Nacional de Criminalística
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº13.709/2018)
NSA	National Security Agency
OCDE	Organização para o Comércio e Desenvolvimento
OEA	Organização dos Estados Americanos
ONU	Organização das Nações Unidas
OUA	Organização da Unidade Africana
TCP/IP	Transmission Control Protocol / Internet Protocol, Protocolo de Controle de Transmissão / Protocolo de Internet
UNESP	Universidade Estadual Paulista “Júlio de Mesquita Filho”

SUMÁRIO

INTRODUÇÃO	10
CAPÍTULO 1 A TÉCNICA INFORMACIONAL E O DIREITO	14
1.1 A técnica e seus paradigmas filosóficos	14
1.2 Técnica informacional	20
<i>1.2.1 Técnica informacional, imagens técnicas e a vivência humana: olhar filosófico</i>	22
<i>1.2.2 A emergência da técnica informacional</i>	27
1.3 A Manifestação Digital do Direito	35
<i>1.3.1 Conflito de perspectivas acerca da Internet</i>	36
1.3.1.1 Perspectiva Externa e o Isotopismo Jurídico	38
1.3.1.2 Perspectiva Interna e o Utopismo Jurídico	42
1.4 A Dicotomia Átomo-Bit (?)	47
CAPÍTULO 2 O AMBIENTE DA INTERNET E SUAS DINÂMICAS DE PODER	60
2.1 Dinâmicas violatórias e protetivas dos direitos na internet	72
2.2 Tutela e Garantia da liberdade e da privacidade	85
<i>2.2.1 Liberdade no ambiente virtual</i>	88
2.2.1.1 Liberdade de navegação	92
2.2.1.2 Liberdade de Pensamento	99
2.2.1.3 Liberdade Econômica	104
2.3 Privacidade no ambiente virtual	107
2.4 Conclusões Parciais	123
CAPÍTULO 3 BLOCKCHAINS, CRIPTOATIVOS E TECNOLOGIAS CORRELATAS E SEU PAPEL NA TUTELA E GARANTIA DE DIREITOS	126
3.1 Respostas do mundo dos bits antes da ascensão das tecnologias descentralizadas ligadas à Blockchain e mecanismos DLT	129
3.2 Características e funcionamento das Blockchains, criptoativos e tecnologias correlatas¹	40
3.3 Criptoativos e Tecnologias correlatas enquanto mecanismos privados de tutela e garantia de Direitos Humanos	155
<i>3.3.1 Privacidade</i>	161
<i>3.3.2 Liberdade</i>	168
CONCLUSÃO	177
REFERÊNCIAS	186

INTRODUÇÃO

A transição entre uma realidade técnica industrial e uma realidade técnica informacional mostra-se como um fenômeno amplo e, ao mesmo tempo, súbito, capaz de impor novas realidades que, muitas vezes, não conseguem ser devidamente acompanhadas pelos poderes institucionalizados e por estruturas com menores percepções valorativas da realidade. Trata-se de um fenômeno rápido que, em menos de uma década, conforme denota Klaus Schwab (SCHWAB, 2016), foi capaz de se expandir muito mais que a revolução tecnoindustrial, foi capaz de se projetar em um século. Sua dinâmica rápida e fluida permitiu que a realidade informacional circundasse grande parte das ambiências humanas e, por sua vez, das próprias estruturas de poder e regulação social, indicando uma dimensão valorativa que, no decorrer dos anos, passaria a incidir diretamente sobre a realidade jurídica, demandando novas práticas regulatórias, indicando novas formas institucionais e normativas que seriam tecnicamente adequadas.

Assim, demarca-se a era da informação como uma realidade técnica capaz de projetar reflexos marcantes sobre o direito, que, apesar da paulatina percepção e reação dessa ciência, passa a demandar novas formas de exercício da regulação social sobre a esfera digital. Surge a necessidade de o direito incidir sobre as largas vias informacionais da *Internet* e demais redes por onde “existem”, digitalmente, milhares de pessoas, visando estabelecer padrões concretos e dignos de regulação para toda aquela palheta de relações, condutas e direitos, que, agora, tomam forma em *bits*¹ projetados sobre telas.

Confrontando a realidade informacional e sua essência polarizada com relação aos institutos e relações típicas da era industrial, observa-se a existência de reiteradas dificuldades de os mecanismos usuais de regulação conceberem a manifestação ou a existência digital de direitos e, além, disso, estruturarem respostas aptas a promoverem reflexos dentro da própria esfera virtual, portanto, sem a necessidade de se socorrer ao mundo dos átomos. Nesse intermédio, insere-se o objetivo central da pesquisa, que seria a hipótese da utilização de criptomoedas, *Blockchains* e mecanismos correlatos², enquanto estruturas natas à rede informacional, como mecanismos de tutela dos direitos digitalmente existentes (ou manifestados).

¹ *Bit* é a menor unidade informacional usada na computação para armazenar ou comunicar.

² Tecnologias pautadas em padrões descentralizados de gestão de dados, inexistindo formas de controle ou estruturas centrais, responsáveis pela gestão e manejo do fluxo de informações.

A análise em questão busca alcançar, especificamente, os direitos no ambiente digital, virtual ou informacional, qual seja o conceito utilizado, referindo-se à vivência dentro da *Internet*, uma estrutura em rede que comunga quase a totalidade da realidade humana virtualizada.

Enquanto construção do trabalho, lançam-se duas hipóteses primárias, como forma de culminar, mediante testagem dedutiva, em conclusões acerca da questão preliminar: a existência de uma realidade digital, que se distingue da realidade física, com projeção dessa questão sobre a incidência do direito e demais formas regulatórias; e a existência de direitos ou meras manifestações de direitos no ambiente digital, e a fragilidade de respostas institucionalizadas e nativas à rede aptas à realidade técnica da informação.

Os objetivos específicos do trabalho circundam as hipóteses primárias levantadas, enquanto etapas para a construção e testagem da hipótese final, aquela que tem como base o objetivo geral da pesquisa. Por meio da abordagem multidisciplinar acerca da técnica, da sociedade da informação e das suas projeções sobre o direito, busca-se compreender as dinâmicas de poder da rede, a manifestação de direitos na *Internet* e as fragilidades das estruturas institucionalizadas e não ortodoxas de regulação do ambiente virtual. Por meio desses objetivos, busca-se testar a hipótese da utilização das *Blockchains*, criptoativos e demais tecnologias correlatas, enquanto constructos tecnicamente adequados, capazes de tutelar, por intermédio de estruturas privadas descentralizadas, os direitos de liberdade e privacidade, dos utilizadores da rede, de forma nativa e sem recursos necessários ao mundo dos átomos.

O trabalho tem uma dinâmica exploratória, orientando-se pelo relacionamento de fenômenos não evidentes, possuindo uma abordagem qualitativa centrada à abordagem teórica da temática proposta. Conforme já antecipado, há a adoção do modelo hipotético-dedutivo como metodologia de manejo e gestão dos dados captados através de pesquisas e revisões bibliográficas. São lançadas hipóteses primárias, que serão testadas por meio de uma aproximação dedutiva, imergindo a hipótese em robusta discussão teórica fundada em autores para, assim, chegar a um resultado. Obtidos os resultados preliminares, enquanto respostas das hipóteses primárias, forma-se um substrato base para a testagem da hipótese central, que culminará no objetivo principal desse trabalho.

Em um primeiro momento, busca-se compreender a realidade filosófica que rege a técnica, visto que o trabalho que tem sua base fundada nas dinâmicas da técnica, em especial, a informacional, lançando bases, também, com o apoio da ciência da informação, para compreender, axiologicamente, o que foi a ascensão da sociedade informacional e seu impacto sobre as ciências culturais. Dada a alternância da técnica, muito bem constatada com o apoio

basilar da filosofia e sociologia da técnica e as compreensões da ciência da informação, surge a necessidade de antever como o direito, uma instituição social tipicamente apegada ao mundo dos átomos, é capaz de reger as relações ali nascentes, apresentando o conflito entre as formas de regulação incidentes sobre essa nova realidade e o contraposto entre a legalidade estatal e a legalidade das demais formas de regulação. Partindo dessa dinâmica, será possível confirmar ou não a primeira das hipóteses, tendo como paradigma os padrões jurídicos das redes, em especial, a *Internet*, assim como uma abordagem acerca das regulações extra-estatais diante da vivência virtualizada.

Feito isso, parte-se à abordagem da segunda hipótese, buscando-se construir uma visão acerca dos problemas da *Internet* com relação aos direitos ali existentes ou manifestos, haja vista que as suas bases filosóficas, valorativas e concepcionais estarão já estabilizadas. Dentro da vida virtualizada, busca-se demonstrar o potencial de lesividade aos direitos digitalmente manifestos, em especial, a liberdade e a privacidade, como provável decorrência de uma tutela pouco eficiente, de uma inadequação técnica das vias jurídicas usuais e uma fragilidade dos meios nativos à rede. Apesar da incidência jurídica e do rompimento, no campo teórico, com a dita dualidade “átomo-bit”, projeta-se uma sombra sobre os direitos dos utilizadores, no qual a já frágil garantia e efetivação dos direitos fundamentais é ampliada diante de contextos alegais e com uma legalidade sem amparos legítimos, focado em interesses de grupos e em que há a subversão da ordem constitucional.

Ainda nessa hipótese, busca-se demonstrar que é provável uma suplantação da visão jurídica positivista, estritamente focada na atuação do Estado, em nome de uma realidade jurídica múltipla natural do meio virtual. No entanto, como se busca demonstrar, uma visão romantizada também seria totalmente incoerente com a realidade fática da rede, em que a atuação de agentes reguladores privados (mercado, comunidades regidas pelo costume ou mesmo codificadores) mostra-se, também, capaz de violar direitos fundamentais dos utilizadores da *Internet*. Diante desse impasse entre as tutelas de direitos despendidas sobre os utilizadores da rede, busca-se construir uma teorização acerca da crise de legalidade e de legitimidade que se instaura na *Internet*, suplantando padrões mínimos de dignidade humana e rompendo com a ordem constitucional, abrindo caminho para o objeto central da pesquisa, que é a atuação das *Blockchains*, criptoativos e tecnologias correlatas para garantir os direitos fundamentais dos utilizadores da rede.

Testadas as hipóteses primárias, parte-se à hipótese central, visando articular os resultados preliminares para, de forma dedutiva, constatar ou não a possibilidade dos criptoativos e mecanismos correlatos servirem como instrumentos de tutela e garantia de

direitos no ambiente virtual da *Internet*. Inicia-se a secção com uma abordagem técnica dos criptoativos e suas estruturas correlatas, especificando sua base de funcionamento e estruturação ideológica, indicando seus princípios basilares, dinâmicas e seus efeitos indiretos, por meio do conhecimento multidisciplinar. Apontadas suas bases, parte-se para a comprovação da utilidade desses mecanismos à tutela dos direitos humanos, especificando como esses constructos digitais conseguem efetivar e garantir direitos, pormenorizando sua protetiva sobre a liberdade, privacidade e os direitos socioeconômicos, concluindo as discussões e, assim, já obtendo resultados acerca da hipótese levantada e sua possível adequação aos objetivos já traçados.

CAPÍTULO 1 A TÉCNICA INFORMACIONAL E O DIREITO

A abordagem da técnica em sua dinâmica informacional passa por uma visão geral acerca da manifestação desse fenômeno inerentemente humano, esta, abordada com afincamento e delimitação por diversos filósofos desde o século XIX. Etimologicamente, trata-se de uma compreensão tecnológica³, que envolve a percepção da técnica e a discussão acerca de suas bases, de forma a conceber os impactos diretos desse fenômeno sobre as relações humanas, especialmente socioculturais e jurídicas. Conforme apresenta Hermínio Martins (2012), é impossível compreender uma sociedade e suas dinâmicas sem antes analisar suas técnicas e impactos.

Sendo o Direito uma ciência cultural, eminentemente vinculada à sociedade e suas projeções, torna-se impossível contextualizá-lo senão enquanto um produto da técnica e também uma técnica em si, enquanto mecanismo humano de rompimento com a naturalidade. O Direito enquanto produto da técnica dá indícios da sua vinculação à toda dinâmica que envolve a humanidade e suas bases culturais, sendo aportado, sobre o Direito, um conjunto de valores que tem origem na técnica ou é, ao menos, influenciado por estruturas técnicas. Faz-se, aqui, a ressalva do Direito enquanto uma ciência imersa na técnica e o direito, objeto de estudo do Direito, enquanto estrutura circundada pela técnica e, assim, axiologicamente influenciada.

1.1 A técnica e seus paradigmas filosóficos

A técnica figura nas discussões filosóficas desde o período clássico, apontada como um desuso da inteligência, uma atividade responsiva às dinâmicas ontológicas que cercavam os seres humanos e, por sua vez, indignas de assumirem posição junto às ciências, que possuíam uma conotação unicamente contemplativa. *Techné* figurava como “conhecimento empírico de um objeto ou ação que servia ao homem” (VARGAS, 1994, p.18), distante da contemplação, em razão do necessário apego à aplicação prática. A oposição da *Techné* à *epistémé*, pensar filosófico, dava-se, logo, em razão da sua aplicação ao domínio físico, sua projeção sobre o mundo das coisas na forma de soluções efetivas para problemas e, por atenderem às necessidades materiais, mostravam-se desprezadas (ELLUL, 1968, p.28). Sejam os sofistas, técnicos e não epistêmicos, tão criticados na antiguidade helênica por Platão, ou a oposição ferrenha, até mesmo destrutiva, de Arquimedes (ELLUL, 1968, p.29), há a manifestação da

³ Trata-se de uma abordagem teórico-analítica da técnica, portanto, tecnológica, assumindo a noção primária de tecnologia trazida por Vieira Pinto (2008, p. 219).

técnica enquanto o “saber-fazer”, opondo-se diretamente à *epistème*, que figurava enquanto o saber da razão das coisas.

Por sua vez, a *techné* mostrava-se não como mera prática ontológica, simplesmente mecânica e associada às essencialidades naturais humanas, figurando como um saber, uma base teórica, associada a uma atividade (PARRY, 2003), portanto, uma interseção entre o mundo das ideias e o mundo das coisas. Kant (1995, p. 32) parte da compreensão da técnica enquanto uma complexidade de normas voltadas à aplicação de conhecimentos teorizados, assim, separando-se de um conhecimento teórico simplesmente pela sua forma de apresentação. A visão de Kant concatena a ideia de que a técnica seria o engendramento intermediado pelos humanos, daquelas teorias que regem a natureza das coisas, portanto, um conjunto de diretivas para a construção da realidade humana.

O materialismo fenomenológico existencialista de Ortega y Gasset analisa a técnica e sua essência sob uma ótica instrumentalista, compreendendo-a enquanto uma manifestação coletiva de diversos atos técnicos. A técnica, sob a visão Ortegiana, rege-se por uma dinâmica sobrenatural, assim, ultrapassando a naturalidade e adentrando na artificialidade enquanto manifestação antropológica, capaz de inserir o ser humano além das trivialidades do meio natural. Assim, entende o autor que são atos técnicos e a técnica (ORTEGA Y GASSET, 1963, p.14).

Os atos técnicos são, portanto, atos que modificam ou reformam a circunstância ou natureza, conseguindo que nela haja o que não há, seja, o que não existe. O conjunto de atos técnicos é a técnica, tida como a reforma que o homem impõe à natureza em vista da satisfação das suas necessidades.

O autor compreende a técnica dentro da dinâmica humana de vivência, articulando essa como uma forma de reação ao meio natural, que oprime o homem e impõe sérias limitações à vivência humana plena (ORTEGA Y GASSET, 1963, p. 17). As necessidades, enquanto condições supérfluas, necessárias ao bem-estar, condicionam o ser humano a produzir métodos mediatos e eficientes de poupar esforços, limitando os imperativos primários em nome daquelas urgências não-biológicas. A técnica, assim, figuraria como uma tendência humana de garantir, por formas mais simples e seguras, aquilo que surgia nas suas necessidades através de procedimentos mediados, inicialmente tendentes a reduzir recursos e esforços despendidos na realização imediata.

A realização mediata necessitaria de uma prévia abstração humana, que se contrapõe às dinâmicas biológicas da natureza, para suspender suas atividades e dedicar-se à projeção de

novos caminhos-guia à sua vivência. A abstração necessária conduz a imersão nos âmbitos da técnica, induzindo à supressão das influências presentes em nome da projeção imaginativa de técnicas superiores, questão essa que fornece, a tal fenômeno, uma expansão além da realidade, conduzindo a instrumentalização em graus ainda mais robustos (MARÍAS, 1947, p. 265-266). A técnica, na visão de Ortega Y Gasset (1963, p. 39) toma uma conotação prometeica, libertadora, livrando-nos dos males hodiernos e dos “grilhões do espaço-tempo que nos limitam.”

O autor parte de uma visão gnóstica, em rompimento com a vida em sua faceta biológica, concebendo-a como um atributo que se vincula à essencialidade humana. A existência humana apresenta-se como uma porção que não coincide com a natureza, uma esfera heterogênea com relação à naturalidade do mundo, exigindo que os seres humanos, enquanto condição para existirem, reajam ao meio e promovam mecanismos técnicos que garantam a possibilidade de se dedicarem a si mesmos (ORTEGA Y GASSET, 1968, p. 38-47). Por meio de uma base antrópica da técnica, sobre a qual é inerente o seu desenvolvimento, busca-se alcançar um status “antinatural” (ORTEGA Y GASSET, 1963, p. 30), que coloque o ser humano em um patamar superior à simples existência biológica, no patamar da “sobrenatureza”, capaz de satisfazer, de forma mediata e cooperativa, todas as suas necessidades. Não se trata de um rompimento total com a manifestação física da existência, aos moldes do que propuseram autores transhumanistas, mas sim uma melhor adaptação da existência humana e suas complexidades ao ambiente, de forma a facilitar a vivência e garantir o necessário e o supérfluo.

Toda a instrumentalidade atribuída à técnica sofre forte oposição do pensamento de Heidegger, que, partindo de sua fenomenologia-existencialista, busca compreender a essência da técnica e a sua dinâmica além das bases instrumentais. Heidegger (2008, p. 375-376) entende que o sentido essencial da técnica não está relacionado ao fenômeno da causalidade instrumental, de forma que sua concepção, enquanto meio destinado a finalidades diversas, não condiz com a sua dinâmica, que é oposta à unilateralidade de imposição da vontade humana. A crítica de Heidegger vale ser ressaltada quanto à sua oposição ao modelo de neutralidade da técnica, apontando esta como uma projeção que nos cega, referindo, assim, à existência de vieses definidores por trás da técnica, enquanto desencobrimento. A sua falta de neutralidade referia-se, portanto, a uma manifestação técnica moderna, enquanto um declínio da essência humana e um esgotamento da cultura (ZIMMERMAN, 1990, p. 63), afastando-a do ser. A perda de controle sobre a técnica refletiria a sua utilização enquanto finalidade instrumental, abstraindo totalmente a faceta da técnica enquanto “compreensão do ser”, a visão existencialista entre o ser humano e o mundo que o circunda.

Apesar da oposição de Heidegger quanto à sua essencialidade, a instrumentalização da técnica mostra-se como uma tendência marcante entre os filósofos modernos da técnica, que assumem posturas gnósticas ou mesmo antropomórficas, mantendo a compreensão desta enquanto instrumento causal. Enquanto o gnosticismo se apoia na sobreposição das bases naturalmente humanas, como o caso de Voegelin (2012, p. 20), as correntes antropomórficas concebem a técnica como projeção das funcionalidades humanas, focada, assim, na produção de dinâmicas e coisas contrafeitas às bases biológicas humanas, seguindo as bases do pensamento de Ernst Kapp (MARTINS, 2012, p. 15-16).

Heidegger (2007, p. 381), assim como Ellul (1968, p. 80), compreendem distinções marcantes entre a técnica em sua manifestação histórica e na modernidade, percebendo uma dinâmica focada nas ciências exatas e contradição com uma técnica simbólica, concebida sob uma pluralidade de fatores. Nesse sentido, a técnica parte de um enfoque fenomenológico singularizado, que se entorpece na repetição do que é exato, e substitui uma abordagem simbólica cultural (VANDERBURG, 2013, p. 23), devendo-se considerar a técnica moderna como uma abordagem pouco ampla, limitada a aspectos condicionantes e, acima disso, estabelecida com base nas ciências exatas. A técnica moderna, compreendendo esta enquanto uma ciência abstratamente centrada na exatidão, acaba denotando uma realidade muito particular, pautada, majoritariamente, em procedimentos indutivos de conhecimento, situação essa que daria à técnica um espectro limitado de abordagem da realidade.

A ausência de um suporte axiológico, capaz de oferecer uma derivação cultural significativa, limita, expressivamente, a face da realidade amparada pela técnica moderna, de forma que o conhecimento vislumbrado, ou como diria Heidegger, desabrigado, unicamente pelas ciências exatas refletiria uma realidade fracionada, sem entender tais dinâmicas com base em um aporte valorativo individual e cultural (RICKERT, 1896, p. 246-250). A base neokantista de Henrich Rickert oferece suporte para compreender a técnica não como simples ciência da natureza, mas como também uma ciência cultural, que, sob um ponto de vista de Willen Vanderburg (2013), tem valor simbólico, portanto, com uma dialética dos fenômenos com relação à vivência humana e o meio que a cerca, no sentido de que esses fenômenos conseguem engendrar influências recíprocas entre o indivíduo e o meio.

Jaques Ellul compreende a técnica enquanto um fenômeno historicamente humano, portanto, que, desde épocas primordiais, manifestar-se-ia como um “ponto de contato entre a realidade material e o conhecimento científico”, muito embora afirme o autor que essa visão seja errônea (ELLUL, 1968, p. 6). Para o autor, o fato histórico que marca a técnica leva à compreensão de uma disparidade temporal entre o surgimento da técnica e o surgimento da

ciência, o que colocaria aquela como um catalizador das projeções técnicas a partir do momento de sua ocorrência. O impulso criado pela ciência sobre a técnica acabou por estabelecer uma situação de indissociabilidade entre ambas na modernidade, instituindo uma tecnociência.

A técnica, assim, possui características marcantes, capazes de condicionar sua relação com o homem, sendo elas: o automatismo técnico, simbolizando as escolhas enquanto fenômeno hermético distante da subjetividade humana, o auto crescimento, enquanto o progresso desvinculado da atuação humana, a sua unicidade, manifesta na não dissociação entre os fenômenos técnicos o seu próprio uso e as condições da sua existência, o universalismo técnico, em sua face temporal e geográfica, e a sua autonomia, como uma força com capacidade própria de perseguir os objetivos que se propõe (ELLUL, 1968, p. 83 e ss).

As características inerentes à técnica acabariam impondo-a uma dinâmica racional, capaz de derrocar objetos sagrados da humanidade por meio de sua predominância, ocupando ela o plano mítico e religioso através do desvendamento daqueles mistérios, antes embaixadores de regras de vivência (BARRIENTOS-PARRA; MELO, 2008, p. 200). Figurando a técnica como condição universal para o alcance de qualquer finalidade, Umberto Galimberti (2015, p. 9), partindo de uma construção Hegeliana acerca das relações entre grandezas qualitativas e quantitativas, concebe tal questão como capaz de engendrar uma inversão entre o criador e a criatura, figurando a técnica como um fim, e o homem, por sua vez, enquanto um meio, assim, manifestando uma derrocada da vontade humana diante da técnica, enquanto condição universal para a obtenção de um resultado. Em sentido semelhante, Habermas (2009, p. 50) considera a técnica e, por sua vez, a própria ciência, como um engendramento orientado pelas dinâmicas de dominação das classes dominantes, sendo inconcebível obter da técnica qualquer efeito emancipatório.

Indo além do racionalismo que marca a técnica moderna e levando em conta todas as suas características essenciais, Ellul (2009, p. 262), seguindo Heidegger, a concebe como um fenômeno não neutro, portanto, entendendo que uma abordagem neutra constituiria um reducionismo que conduziria a uma visão superficial, exigindo que haja uma análise complexa dessa, enquanto marcada por uma ambivalência. A ambivalência da técnica a marca enquanto um fenômeno que não é bom, nem mau, nem neutro, mas, sim, um conjunto complexo, albergando a totalidade dessas manifestações. A técnica, assim, demandaria uma quantidade razoável de recuos necessários para a sua projeção avançada, impondo uma substituição vinculante entre aspectos da técnica existentes e potenciais. Dessa forma, haveria a produção de mais problemas que, anteriormente, buscava-se resolver, por meio da inseparabilidade dos efeitos maléficos e benéficos e a imprevisibilidade de seus efeitos (ELLUL, 2009, p. 264). Na

visão de Ellul, não caberia qualquer forma de juízo moral sobre a técnica, visto que sua unicidade garante que sua análise se limite aos aspectos técnicos (BARRIENTOS-PARRA; MELO, 2008, p. 199).

Hermínio Martins (2012) reflete acerca da sua natureza enquanto reflexo subjetivo da humanidade. A técnica é analisada pelo autor conforme dois paradigmas tradicionais do pensamento ocidental, um paradigma inicial de melhoramento tecnológico da vida humana, por meio da sobreposição à natureza, em uma visão antropomórfica da técnica, e um paradigma crítico, concebido sob uma visão da técnica enquanto aspecto anestesiante da percepção humana, de forma a suprimir do campo de visão aqueles efeitos deletérios.

O autor (MARTINS, 2012, p. 20) compreende, inicialmente, uma visão “prometeica”, assemelhando a técnica ao titã grego em razão do seu “papel intrinsecamente libertador”, colocando a técnica como conjuntura científica capaz de livrar o homem de suas dificuldades e alçá-lo ao nível dos “deuses”, denotando uma visão instrumental. A técnica, em uma visão difundida pela filosofia positivista francesa e pelos socialistas utópicos, “furtaria o fogo dos deuses” por meio do oferecimento de mecanismos de emancipação e melhoramento de condições humanas de vivência, especialmente considerando a técnica e a ciência contemporâneas.

Por outro lado, opondo-se à visão prometeica, há a técnica “fáustica”, vinculada ao pensamento fenomenológico alemão, em especial Heidegger, pressupondo a apropriação humana ilimitada sobre os ambientes naturais (FERRAZ, 2000, p. 7), por meio do engendramento de uma técnica utilitarista, infinitista e, por sua vez, cega, incapaz de conceber os riscos que decorrem de tais práticas (MARTINS, 2012, p. 55). Enquanto o modelo técnico prometeico se ancora sobre a racionalidade, a técnica fáustica baseia-se em um modelo pouco razoável, capaz de ensejar uma tirania das possibilidades tecnológicas e de afetar, consideravelmente, o ser humano e sua esfera existencial (MARTINS, 1996, p. 245).

A técnica, dessa forma, assumiria um contexto fáustico e, como consequência, haveria seu engendramento em benefício de estruturas opressivas, totalitárias, capazes de sujeitar o indivíduo por meio de uma técnica onisciente. Ellul (1968, p. 317-319) aborda a relação estrita entre o Estado e a técnica, indicando que tal entrelaçamento mostra-se como objetivo central desta instituição, fazendo uso de reiterados meios para alcançar a técnica mais eficiente. Os entes estatais, assim, lançam mão de diversas estruturas institucionais e mercadológicas, visando desenvolver técnicas eficientes em todas as esferas, compondo-se enquanto um ente técnico, cuja lei-base é a busca frenética pela eficiência. A projeção dessa perseguição à eficiência da técnica reflete na expansão das práticas de poder do Estado, que coaduna com uma

organização complexa de técnicas mobilizadas, que diminuem o papel do ser humano, haja vista a assimetria de magnitude da técnica disponível (ELLUL, 1968, p. 323). A estruturação dessas técnicas, pelo Estado, acaba por incrementar seu poder, estabelecendo formas de condicionamento do ser humano aos padrões de controle estabelecidos.

Colocados tais paradigmas, há que se considerar a técnica informacional, que será a seguir abordada, enquanto uma manifestação pós-moderna da técnica humana, seja sob um ponto de vista gnóstico ou mesmo antropomórfico (FERKISS, 1980). Ainda aqui, mantemo-nos dentro de uma realidade epistemológica terrestre, pouco capaz de se adequar à vivência no ambiente digitizado, que demanda uma epistemologia oceânica, fluída, suficiente para conceber um fluxo na compreensão. Uma visão da técnica digital compreende a necessidade de uma nova visão acerca da técnica, levando em conta, sim, as bases técnicas filosoficamente concebidas anteriormente, mas indo além disso, concebendo uma fluidez desse novo meio que estamos inseridos.

1.2 Técnica informacional

Compreendida a técnica em sua dinâmica filosófica, é possível afirmar que a técnica moderna aponta um instante de ruptura com as bases anteriores que orientavam a dinâmica social, econômica, política e, por sua vez, jurídica. A técnica, enquanto um fenômeno humano, atua em uma constante realidade responsiva ao meio que a cerca, constituindo base fundante sobre a qual se estrutura a cultura humana e, por sua vez, sujeita a constantes reflexos culturais que a moldam e estruturam conforme novas dinâmicas humanas exasperadas no ambiente social (BARRIENTOS-PARRA, 2011, p.66). É necessário conceber a técnica como um contexto que embasa as manifestações existenciais humanas em sociedade, um anteparo que molda a forma das relações do homem entre si e com a natureza que o cerca.

A técnica informacional assume uma conotação instrumental, tipicamente atrelada às necessidades humanas que ascendiam nos períodos de estruturação das bases computacionais, devendo ter em mente uma instrumentalidade em sentido Heideggeriano, portanto, partindo de uma contextualização essencial. Dessa forma, há uma visão instrumental da técnica em sua face informacional, no entanto, concebendo esta enquanto fenômeno atrelado à sua essência. Leva-se em conta que, durante a abordagem dos fenômenos técnicos, ocorre o surgimento de toda a compreensão do ser humano enquanto ser imerso na era da informação. Dentro dos limites traçados, considerando a dinâmica instrumental e, ao mesmo tempo, entendendo o atrelamento direto desta com sua esfera existencial, há que se avaliar a técnica informacional e suas

projeções aos âmbitos dos seres humanos, compreendendo, ainda, sua possível natureza enviesada, prometeica e fáustica.

Essa especificação informacional do fenômeno técnico pautar-se-ia sobre uma dinâmica de não-objetos, que, apesar de se referir a uma dinâmica de informações, alcança tais questões sob uma óptica inovadora, não mais atrelada às experiências anteriormente existentes. Assim, conforme apresenta o Flusser (2006, p. 39), existiam sim informações antes da “era da informação”, e estas tinham demasiada importância, no entanto, as informações assumem posição central na atualidade, isso sem contar com uma profunda reestruturação na forma que esta existe e é circulada. As informações, enquanto “inobjetos”, que “escapam de nossos dedos” adquirem forma enquanto realidade vigente, portanto, não mais simples dados, mas concepções que, intermediadas pelo ambiente imagético, constroem um novo mundo. Byung Chul Han (2018, p. 68) indica que essa nova realidade é capaz de estabelecer uma sintonia quase supressora entre a informação e o ser em sua existência, de forma que a coincidência entre essas esferas é capaz de confluir aspectos entre si, sendo que a informação e seu fluxo se tornam constituintes essenciais da realidade existencial. Nas palavras do autor: “o que não é informação não é”, indicando uma clara alteração da nossa relação com o mundo, este agora não mais sujeito a uma realidade objetiva, mas, sim, sujeito a uma realidade superficial, sensível ao toque e, por sua vez, alternativa.

Essas novas informações, responsáveis pela criação de uma realidade menos palpável, mais nebulosa dependem diretamente de objetos materiais capazes de intermediar o processo de sua criação e armazenamento. Assim, a informação precisa de *chips*, válvulas catódicas, transistores, objetos que viabilizem a sua existência projetada em telas e sensores, ainda que tais objetos-base sejam, cada vez mais, desprezíveis e irrelevantes dentro do mundo virtualizado (FLUSSER, 2006, p. 40). A emergência dessa nova realidade instaura um rompimento com o *homo faber* e o surgimento do *homo ludens*, na qual os objetos adquirem uma relevância relativamente desprezada em contraponto à emergência da informação, enquanto paradigma humano central na atualidade.

Conforme foi apresentado por Habermas (2009, p. 70-73), há que se considerar a ascensão da técnica enquanto força produtiva principal dentro do modelo capitalista, mostrando-se como fator base da evolução social, de forma que a primazia moderna do âmbito informacional se mostra como uma decorrência autônoma dos meios técnicos, sempre objetivando a máxima eficiência e tendo como expoente um efeito reflexo sobre toda a existência humana conectada a esses meios.

1.2.1 Técnica informacional, imagens técnicas e a vivência humana: olhar filosófico

A abordagem da técnica informacional, tipicamente imaterial, não acessível às mãos, no entanto, alcançável pelas mãos (HEIDEGGER, 2001, p. 36) deve percorrer a visão flusseriana acerca da técnica, concebendo a questão das imagens técnicas, seu potencial influenciador sobre a “pós-cultura”, haja vista a inerente superficialização que marca a sociedade da informação, que tende a assumir formas mosaicas, instaurando uma nova base axiológica, sobre a qual se pauta a humanidade, inclusive, a esfera jurídica.

Flusser (2010) parte de um olhar fenomenológico, sofrendo expressiva influência das filosofias da linguagem e também de um olhar ontológico, encaminhando, assim, para a abordagem da técnica e sua relação com o ser humano. O olhar relacional de Flusser concebe um importante papel sobre a técnica, afetando o ser humano em seus cenários sociológicos, cultural, político e antropológico, contextualizando essa interação sob a óptica da reestruturação da história no entorno das comunicações humanas e sua capacidade de transmissão intergeracional de conhecimento.

A técnica apresenta-se como um espírito incorporador das mudanças essenciais que rodeiam a vivência humana, de forma que toda revolução, seja ela econômica, social ou cultural, tem como base fundante uma revolução técnica. O ser humano, enquanto ser técnico, portanto, dotado de capacidade de influenciar, motivadamente, o mundo material, dá forma e função às coisas que o cercam, empreendendo estas para a sua vivência (FLUSSER, 2019, p. 10). As revoluções técnicas da história, por sua vez, possuem uma tendência antropomórfica, com reiteradas sinalizações para reflexos humanos, seja na forma de instrumentos, ferramentas ou processos que simulam funções motoras e orgânicas do corpo humano. A atualidade, portanto, a pós história, inova ao deixar de se referir a manifestações corporais humanas, máquinas e ferramentas, mas ao sistema nervoso, incutindo uma técnica referida a imagens, transportando a liberdade de imaginação reinante no intelecto humano (ENTREVISTA, 1988).

Imagens técnicas seriam informações digitizadas, informações inseridas no ambiente digital e, portanto, rompendo com a linearidade e unicidade do fluxo informacional histórico, assim, instaurando uma revolução no pensamento. A linearidade da escrita e sua unidirecionalidade acaba por limitar, em muito, nossa capacidade de expressão, exigindo um sistema pouco versátil de mediação, que é a linguagem linear. A descrição do mundo em suas facetas atuais, principalmente pós-modernas, passa a demandar o uso de cálculos e descrições matemáticas, que descrevam um mundo em uma base não linear, multi óptica (FLUSSER, 2010, p. 54). A humanidade e toda sua construção cultural mostram-se diretamente

programadas pelas imagens técnicas, pelas superfícies representativas que emergem da técnica em rompimento à linearidade histórica (FLUSSER, 2013, p. 125).

Dentro de um ambiente informacional digitalizado, marcado pela pós-história e, por sua vez, pelas imagens técnicas, há a marcação concreta da forma como concebemos nosso conhecimento, enquanto ligado, diretamente, aos paradigmas de transmissão e registro da informação (FLUSSER, 2019, p. 10). O ambiente informacional, na visão Flusseriana, a pós-história, estaria marcado pela sintaxe desconstruída da linearidade da escrita, de forma que os pontos são reagrupados para formarem superfícies mosaicas, imagens técnicas que compõem uma metalinguagem, fora da linearidade (FLUSSER, 2002, p. 11). As imagens técnicas, enquanto planos visuais representativos, passam a transmitir o conhecimento na forma de conexões entre pontos individualmente concebidos, portanto, efetivos *pixels*⁴ que compõem uma realidade superior, correlacionada a um sentido específico e não linear (FLUSSER, 2007, p. 49). Tornando mais palpável tal concepção, pode-se conceber as imagens técnicas como *QR codes*⁵, códigos de acesso digital às informações, em que são agrupados gráficos de pontos que, superficialmente, interagindo entre si e com um anteparo mediador, concebem uma comunicação e comunicam uma informação muito diferente daquela simplesmente assimilada pelos olhos.

Os meios comunicacionais, antes atrelados a um modelo gutenberguiano, eram focados na linearidade da escrita e na realidade tipográfica, comunicando de forma unidirecional e pouco abstrata. Com o aporte imagético, os meios comunicacionais sofrem reiteradas renovações, efetivas revoluções que remoldam a comunicação humana, instaurando “galáxias comunicacionais” distintas daquela decorrente da criação de Gutenberg (MACLUHAN, 1969, p. 49). O ambiente comunicacional pós-Gutenberg, por sua vez, instaura uma nova realidade, primeiramente afetada pela conjuntura técnica fundante e, além disso, capaz de projetar uma nova galáxia de comunicação, agora orientada pela eletricidade e eletrônica.

A galáxia pós-Gutenberg teria como paradigma técnico a projeção de constructos enquanto extensão do sistema nervoso central, não mais tendo como objetivo constituir formas de extensão corporal humana, mecânica ou visual, ressaltando, aqui, uma visão antropomórfica da técnica. A nova realidade comunicacional humana, atrelada à emersão da técnica elétrica, em uma atividade revolucionária, impõe mudanças no sentido de uma menor concretude das

⁴ *Pixels* é o menor ponto luminoso que compõe uma tela, um ponto que, conjuntamente, consegue manifestar formas e imagens sobre um dispositivo.

⁵ *QR Code* ou Código barramétrico bidimensional é um código composto por uma composição de pontos e tonalidades, capazes de representar informações diversas.

dinâmicas de comunicação, essas mais etéreas do que os meios fisicamente disponíveis anteriormente, como os livros e demais meios comunicacionais pautados na unidirecionalidade da comunicação. Por sua vez, com ascensão da eletrônica, concebe-se uma nova realidade comunicacional, uma segunda revolução pós-Gutenberg, esta marcada pela quebra da linearidade, por meio da instauração de mecanismos e refluxos de informações, substituindo a palavra pelo visual, de forma a possibilitar a existência de uma realidade marcada por imagens, projeções virtualizadas do pensamento humano (MACLUHAN, 1969, p. 49), esta nova realidade é capaz de projetar efeitos sócio culturalmente.

Bernard Stiegler (1996, p. 74-75), aproximando-se dessa visão, descreve a teleficação da escrita como um fenômeno marcante da atualidade, especificamente, a era da informação, avaliando a escrita atual, enquanto conexa com a realidade das superfícies, ou seja, compondo, juntamente aos anteparos tecnológicos, métodos de comunicação. A compreensão da sociedade informacional, que nos envolve, passa inerentemente pela questão das imagens técnicas, enquanto mecanismo comunicacional, que assume posição central nas comunicações humanas e, por sua vez, impactando culturalmente as sociedades humanas. A tendência em “tornar superfície” a comunicação humana assume substancialidade dentro do ambiente digital da *Internet*, no qual os *hipertextos* e as telas de comunicação permitem um aparato escrito que vai além dos sentidos materializados na escrita, e conseguem empreender efetivas re-imaginações do mundo. A informatização, apoiada de perto pela técnica computacional, permite que nossa imaginação não seja mais limitada pelos instrumentos de escrita, estruturando ambientes inovadores, capazes de compor novas significações e novas realidades.

Cumprido, ainda, conforme alerta Macluhan (1969, p. 49), compreender o perigo do afastamento antropomórfico advindo dessa nova significação, fornecida pelo ambiente de informações, levando em conta que a supressão das captações externas, tipicamente humanas, advindas de realidades mais concretas e menos abstratas, conduz, inerentemente, a um movimento alucinatório, com reverberações sociais. Assim como a hiperexposição humana às realidades sensoriais, concretas, é capaz de conduzir à alucinação, a privação de tais anteparos de linearidade e materialidade, pelo avanço da superficialização, também produz semelhante efeito, conduzindo àquilo que Byung-Chul Han (2018, p. 2) chama de enxame de cegueira e estupidez típicos da embriaguez na técnica informacional.

A transição entre o átomo e o *bit* (NEGROPONTE, 1995, p. 14) representa muito mais que uma simples alteração entre a linearidade comunicacional para uma composição mosaica, indicando uma efetiva mudança do paradigma analógico, escrito, para um estado de representatividades, configurando toda uma ambiência com base em estados transitórios

programáveis, centrada no *bit*, linguagem binária fluida e amplamente correlacionável para a estruturação de imagens técnicas. Os números e sua significação, quase metalinguística, acabam tornando-se uma realidade do ambiente digital, de forma que esse novo anteparo comunicacional serve para o engendramento das construções imagéticas, assim, as programações necessárias às aplicações digitizadas. O reflexo dessa nova realidade, pautada nos números e na exatidão, é, acima de tudo, a derrocada de padrões valorativos, na qual o digital só recebe em suas ambiências aquilo que pode ser convertido em linguagem numérica ou ao menos enumerável (HAN, 2018, p. 60), atendendo a um padrão de eficiência orientado à exatidão, que exclui da “existência digital” tudo aquilo além de tais arquétipos.

A era da informação altera, consideravelmente, a realidade, migrando-a para um sistema de superação da dicotomia em nome de sistemas dualógicos, que refletem a influência da matemática e da programação sobre as demais searas sociais (FLORIDI et al, 2015, p. 19).

O mundo estruturado no ambiente digitalizado assume formas cuja matéria deixa de ser física e adquire uma conotação flexível, digitizada, composta, essencialmente, de mosaicos técnicos, científica e matematicamente amparados, que nos apresentam uma visão remasterizada do nosso mundo, agora intermediado por computadores e telas sensíveis ao toque. Se antes olhávamos nos olhos das pessoas e conversávamos pessoalmente (HAN, 2018, p. 30-31), hoje, a forma da pessoa existe digitalmente, porém, enquanto uma imagem técnica, uma série de *bits* que informam *pixels* que, por sua vez, compõem uma imagem representativa, sobre uma tela para a qual podemos nos comunicar. As formas resistem, porém, a matéria de tudo sofre uma reestruturação profunda, impactando nossa forma de ser, estar, pensar e saber.

A informação, diante de uma ótica gnóstica, assume posição de relevância para a técnica enquanto fenômeno humano “sobrenatural”, refletindo uma visão ontológica superior, além do mundo das coisas e mais próxima, portanto, do espírito, do mundo das ideias. O mundo material é limitado e incapaz de fornecer meios suficientes para as novas demandas socioeconômicas humanas, exigindo uma alteração do mundo concreto, material, marcado pelos “*fleshwares*”⁶, para um ambiente intermediado pelas formas de processamento de informação, etéreas e mais próximas das ideias humanas (MARTINS, 2012, p. 18), o que Flusser chamaria de mais imagético, mosaico e não linear.

O *cogito* transfigura-se em *computo*, de forma que a informação virtualizada em máquinas se torna uma noção dominante, na qual tudo que não é informacional precisa assumir condição de informação para existir e possuir relevância dentro do atual estágio técnico-

⁶ Trata-se de uma terminologia computacional, usada para referir-se aqueles aparatos biológicos humanos, corpos em seu sentido material.

evolutivo (MARTINS, 2012, p. 22), transfigurando o *homo faber* em *homo ludens/homo digitalis* (HAN, 2018, p. 55). É necessário que o mundo físico passe pela tradução das máquinas e ingresse no ambiente da gnose para que “exista” nessa nova realidade, visto que, “na era da informação, a invisibilidade equivale à morte” (BAUMAN, 2007, p. 21), dado que a realidade técnica vigente impõe, exponencialmente, uma regência geral sob as dinâmicas etéreas do informacionalismo. As imagens formadoras dessa nova realidade conseguem desestruturar os padrões usuais de representação, “revigorando a sua semântica e poética” (HAN, 2018, p. 52), de forma que a digitalização acaba por desconstruir a relação entre as imagens e os fatos, rompendo a linearidade temporal e instaurando uma condição de unitemporalidade, no qual o presente se torna algo permanente.

A separação do passado, enquanto recordação, e o futuro, enquanto imagem projetada, torna simples aspectos do presente, de forma que a intangibilidade, antes marcante sobre essas duas searas temporais, agora é acessível ao toque, por intermédio dos aparatos digitais. Gerações de conhecimento e projeções do nosso futuro são acessíveis de quase a totalidade de aparelhos eletrônicos conectados à *Internet*, mostrando uma realidade mais viva, “mais bonita”, conforme indica Byung-Chul Han (2018, p. 48), apesar de não conter toda aquela carga axiológica, decorrente da percepção linear, intermediada pelos sentidos.

Esse mundo fluido que nos cerca é estruturado com base em aparatos técnicos, instrumentos tecnológicos que são extensões profundas das funções orgânicas humanas, tendo ênfase junto às funções psíquicas, que se refletem no ambiente informacional regente e programado. Esse ambiente informacional, de imagens técnicas, necessita de um conjunto de aparatos também técnicos, que sejam capazes de estabelecer um universo programável, acessível pela linguagem matemática e passível de, com o intermédio desses sistemas de tradução, em seu sentido flusseriano, criar uma superfície que tem a forma do nosso mundo. Dessa maneira, há que se conceber a técnica computacional como suporte material sobre o qual se estrutura a dinâmica informacional que vige na atualidade, considerando a *Internet* enquanto rede informativa modelo, com base na qual se desenvolve quase a totalidade das relações e fluxos de dados comuns.

Mark Poster (2013, p. 76) concebe a quebra da linearidade da escrita por meio dos impactos da *Internet* e da realidade virtual, teorizando acerca da concatenação de palavras e imagens típicas da comunicação humana, sob a óptica da informatização técnica. Afirma o autor que a não-linearidade da construção comunicacional reflete em uma maior agilidade, no entanto, também causa um crescimento carcinogênico, não natural, ausente de qualquer

centralização construtiva, denotando uma alteração da comunicação centralizada para uma rede descentralizada.

Sob essa dinâmica, a técnica informacional marca-se pela superficialização, uma transformação efetiva de todos os aspectos da realidade humana manifesta no rompimento da linearidade escrita e histórica, dando lugar a um ambiente imagético, complexo tecnicamente e simples, aos olhos dos utilizadores. Esse engendramento técnico-imagético marca a realidade informacional que envolve o final do século XX e início do século XXI, sendo necessário tomar as concepções filosóficas desenvolvidas sobre e, de maneira posterior, avaliar efetivamente a emergência desse engendramento técnico e seus impactos na esfera social, econômica e jurídica.

1.2.2 A emergência da técnica informacional

A remodelagem do padrão de desenvolvimento no final do século XX, especificamente manifestada na transição de uma base industrial para informacional (BELL, 1974, p. 146), reflete, de forma concreta, na vivência social, impactando o modo de produção vigente e, assim, a própria dinâmica estatal estabelecida. A alteração afeta de forma expressiva o sistema capitalista, migrando os processos de produção, bases econômicas e culturais da produção de riquezas, para a dependência a níveis incrementados de acesso e utilização de informações, sobrepujando o valor inerente à informação e mitigando a importância das coisas (CASTELLS, 2013, p. 41). A informação assume posição de relevância nas décadas posteriores aos anos de 1970, adquirindo a centralidade no ambiente técnico e, acima de tudo, impactando todas as bases sociológicas humanas.

A era da informação (CASTELLS, 2013), pós-história ou pós-modernidade, marca-se pela reformulação profunda das perspectivas humanas, estas alteradas em razão de uma mudança basal nos fenômenos produtivos amparados na técnica⁷. A alteração técnica apresenta-se enquanto fenômeno de ignição de uma revolução produtiva, esta manifesta na ascensão da chamada quarta revolução industrial (SCHWAB, 2016), tida, por muitos, também como capitalismo informacional. Essa nova realidade produtiva marca-se, primeiramente, pela centralidade produtiva na informação, denegando a importância antes alocada sobre os bens

⁷ Embora haja divergência entre os autores, pode-se afirmar que a era da informação tem seu alvorecer na década de 1970, com a criação e popularização de sistemas computacionais de maior capacidade, como os *micro chips* e micro processadores, muito embora haja uma série de situações socioeconômicas que reflitam a alteração do padrão técnico, rumo à prevalência da informação. Sua transição, efetivamente, ocorre com o surgimento da *Internet*, especificamente no ano de 1975, com a expansão dos estudos sobre a *Arpanet*.

materialmente concebidos, além de uma velocidade exponencial e não linear do surgimento de novas técnicas e aparatos, ancorada sobre uma base procedimental ampla e profunda, características essas que se agregam, formando uma revolução técnica com impactos sistêmicos, capazes de reverberar efeitos sobre todas as dinâmicas humanas da existência (SCHWAB, 2016, p. 16-17).

A alteração se desenrola, portanto, primariamente, sobre o meio da técnica, produzindo efeitos consequentes sobre a economia, sociedade e cultura, de forma a transformar o paradigma dos comportamentos humanos e suas comunicações. É necessário compreender a readequação de todas nossas instituições, modelos de convivência e manifestações, após a emersão da técnica informacional, estabelecendo um novo paradigma sobre o qual toda realidade construída precisa se adequar (SCHWAB, 2016, p. 15).

O ponto de partida da técnica informacional foram as bases computacionais estabelecidas nas fases finais da terceira revolução industrial (SCHWAB, 2016, p. 19), portanto, a informação estabelece-se como eixo central das dinâmicas produtivas, tendo condições materiais para assumir tal posição através do desenvolvimento de máquinas de computação, semicondutores, *mainframes*, e *microchips*, estruturas substanciais, que são capazes de intermediar o ambiente informacional e o ambiente físico.

A técnica computacional⁸, ainda atrelada ao paradigma produtivo industrial, materialista, apresentava-se como um passo para o alcance da técnica informacional, uma etapa necessária de intersecção entre ambientes tecnicamente distintos, o meio material sobre o qual foi possível estruturar o modelo produtivo centrado na informação (CASTELLS, 2013, p. 67). Não bastasse isso, foi necessária uma verdadeira “revolução dentro da revolução”, para que a técnica computacional pudesse servir enquanto plataforma estável e eficiente para o engendramento de sistemas interligados (CASTELLS, 2013, p. 79), migrando de *chips* e *transistores* centimétricos ou milimétricos para aqueles micrométricos, tipicamente os *microchips*, capazes de elevar as capacidades computacionais e, além disso, difundir seu uso. Apesar das bases informacionais já precederem ao surgimento dos *microchips*, a sua estabilidade é facilitada e acontece sua maior projeção diante da proliferação dos meios de computação, que ocorrem na segunda metade da década de 1970, uma vez que a informação assume relevância central, quando passa a fluir de forma esparsa, por uma grande parcela da sociedade.

⁸ A técnica computacional indica uma passagem basilar de um padrão socioeconômico industrial para o informacional, fornecendo condições materiais, portanto, aparatos de processamento capazes de garantir a ascensão da informação e seus fluxos.

Portanto, a técnica informacional e suas expansões surgem de uma interligação entre o fluxo informacional, que assume uma conotação central, imagética e matemática (tipicamente intermediada por linguagens binárias) e os sistemas computacionais, máquinas orientadas à computação de dados e ordenação de valores simbolicamente concebidos (MARTINS, 2012, p. 18). A ascensão da informação à centralidade das dinâmicas produtivas e, por sua vez, socioculturais, demandou uma base computacional capaz de ofertar substratos materiais suficientes para conceber, imgeticamente, um novo meio de existência e manifestação, agora não mais linear como a escrita, substratos capazes de traduzir linguagens e dados em realidades acessíveis aos seres humanos, embora não palpáveis ontologicamente.

As válvulas, os transistores, condutores, placas integradas, *chips*, *microchips*, computadores, microcomputadores, servidores, todos esses aparatos, tiveram sua concepção no pós-guerra, ainda atrelados a uma dinâmica técnica industrial (CASTELLS, 2013, p. 77), e serviram como instrumentos de operacionalização da informação. Os *softwares*, desde seus primórdios, junto ao núcleo duro da técnica computacional, já indicavam uma relevância ímpar da informação, por meio da operacionalização de aparatos técnicos, no entanto, somente na década de 1970, com a ascensão de novas dinâmicas de comunicação, é que passa a ocorrer uma revolução técnica, centrada na informação (CASTELLS, 2013, p. 76).

A centralização técnica da informação assume condições de viabilidade diante da proliferação de mecanismos de interconexão, mediados por ambientes computacionais, formas ágeis de comunicação, capazes de elevar a fluidez informacional a um nível nunca antes presenciado. As redes de circulação de dados, amparadas de perto pelos sistemas de comunicação, conseguem estabelecer um ambiente de primazia das redes de dados (CASTELLS, 2003, p. 16), tendo como paradigma central o melhoramento das estruturas de telefonia e das bandas de transmissão de dados, atingindo ápice junto à optoeletrônica, a transmissão de dados por meio da luz, que foi capaz de firmar as bases da revolução técnica já existente e estabilizar seus prolongamentos no tempo e espaço.

O universo comunicacional, ainda atrelado a uma dinâmica analógica, em tese, unidirecional (MCLUHAN, 1969, p. 104), surpreende-se e renova-se ao estabelecer uma nova esfera de comunicação, agora virtualizada, não mais linear e, por sua vez, capaz de fluir, livremente, entre os componentes de comunicação, criando meios de comunicação em que o refluxo comunicativo⁹ é possível e, assim, capaz de projetar uma série de efeitos (HAN, 2018, p. 37).

⁹ Refluxo comunicativo diz respeito à possibilidade de agentes atuarem como emissores e receptores de informações, não mais recebendo uma postura meramente passiva.

A conjugação da base computacional aprimorada, que adquiria, exponencialmente, relevância coletiva, juntamente com a expansão dos sistemas de comunicação, foi capaz de estabelecer um empuxo massivo sobre as dinâmicas em rede, especialmente em razão do surgimento, expansão e aprimoramento da *Internet* (CASTELLS, 2013, p. 81). A *Internet*, enquanto um aparato informacional, que rearranjou as dinâmicas e relações humanas, marcou a técnica informacional e assentou-se como “mais revolucionário meio tecnológico da era da informação”. Esse aparato figura, assim, como elemento primordial dentro da dinâmica da informação, servindo enquanto rede para o estabelecimento das principais reações informacionais virtualizadas, tendo sua base atrelada à conjugação das tecnologias computacionais, sistemas de intercomunicação e as arquiteturas avançadas de *softwares*.

Conforme expõe Luciano Floridi et al (2015, p. 14), a realidade que nos pautamos é melhor compreendida como uma era informacional e não computacional, considerando a informação como um fenômeno que permeia a vida humana, tendo a esfera computacional uma diminuta influência nesse fenômeno. Portanto, a sociedade pauta sua realidade econômica, social e cultural sobre os processos de informação em estágio avançado (ANTUNES, 2008, p. 3).

A era da informação e o seu nascimento, muitas vezes, são confundidos com o próprio surgimento da *Internet*, dada a importância desse acontecimento para o rearranjo das dinâmicas socioeconômicas e culturais. A computação e a informação formam uma relação sinérgica, de variação recorrente entre causa e efeito, em que, constantemente, os meios computacionais ofertam capacidade de fluxo informacional nas redes que, por sua vez, determinam os novos aspectos dos aparatos técnicos, que intermediarão os ambientes físico e virtual (CASTELLS, 2013, p. 81). A *Internet*, por sua vez, nasce dessa relação sinérgica entre a informação e a técnica computacional, no entanto, assumindo uma posição de centralidade, quando passa a se projetar sobre o ser humano e sobre a técnica em geral, moldando, de forma eficiente, o ambiente dos aparatos e as relações humanas (CASTELLS, 2003, p. 123), assumindo uma noção fluida junto à própria informação.

A relação constante junto à técnica computacional e os sistemas de comunicação, que marcava a informação, acaba sendo exercida, também, por um de seus instrumentos, a *Internet*, que é capaz de engendrar padrões sobre a técnica e sobre as relações humanas, fazendo com que a *Internet* seja separada da informação, enquanto dinâmica, de forma muito tênue. Falar da *Internet* presume referir-se às dinâmicas informacionais, e vice-versa, ressaltando sua importância e sua ascensão, enquanto uma técnica modelo da era da informação.

Essa visão acerca da *Internet* pode ser extraída do pensamento de MacLuhan (1969, p. 22), visto que esse meio de comunicação se confunde, também, com a própria mensagem. Assim, trata-se de um produto direto do ambiente informacional e capaz de comunicar, em si, uma série de questões enquanto informação, assumindo funções conjuntas de meio e mensagem. A natureza do meio comunicacional acaba por interferir diretamente sobre o conteúdo das mensagens, portanto, das informações circulantes por essas estruturas, além de causar reflexos sobre o ambiente humano, no qual a técnica de comunicação, vigente naquele período, tem a capacidade de definir, concretamente, a informação e as formas de recepção e reação a essas por parte dos indivíduos.

A *Internet*, assim, figuraria enquanto técnica típica do ambiente informacional, mostrando-se como uma metodologia apta para mediar o conflito entre a ontologia e a deontologia, portanto, capaz de oferecer soluções concretas e eficientes para a estruturação de uma “noosfera”, uma esfera de dados ampla e profunda (MARTINS, 2012, p. 70), capaz de migrar traços materiais da realidade para uma vivência virtual, digitizada. Esse meio assumiria, também, a manifestação da informação, enquanto mensagem circulante, confundindo-se em um único supra constructo, com uma capacidade de projetar impactos expressivos, alterando as relações de sentido e as estruturas de percepção (MACLUHAN, 1969, p. 32).

Manuel Castells (CASTELLS, 2013, p. 89) considera a penetrabilidade das novas tecnologias, junto a todas as atividades humanas, enquanto uma característica inerente à centralidade informacional da técnica, dado que a informação é um meio presente em toda manifestação humana e, sendo as tecnologias amparadas sobre esse meio catalizador, haveria uma incidência ampla sobre a existência individual e coletiva da grande maioria da população mundial, em constante sujeição às dinâmicas técnicas ascendentes.

Seguindo essa dinâmica, haveria que se considerar a dinâmica técnica tendente à adoção de padrões de rede, estes mais flexíveis e condizentes com um sistema amplamente integrado de relações informacionais, favorecendo uma incidência mais esparsa. O novo paradigma tecnológico é marcado pela sua capacidade de reconfiguração, de forma que a flexibilidade e reversibilidade dos fatores são aspectos decisivos no seio de uma sociedade marcada pela constante mudança e fluidez, demandando um sistema com morfologia aberta, capaz de se expandir, qualitativamente ou quantitativamente, e estabelecer-se sob uma regência dinâmica (CASTELLS, 2013, p. 565).

A adoção de redes torna-se uma característica inerente à era da informação, havendo um engendramento de tal modelo junto às diversas manifestações sociais, econômicas e técnicas. As redes, enquanto aglomerados de nós, interconectados (CASTELLS, 2013, p. 565), atuam

com eficiência diante das dinâmicas fluidas da modernidade, permitindo que a fluidez ocorra dentro de determinado sistema, mas que, ainda assim, haja funcionalidade e eficiência nas suas atuações. As tecnologias informacionais passam a afetar concretamente a esfera social, inclusive com efeitos inesperados, promovendo consequências técnicas, sociais, econômicas, jurídicas e políticas (FLORIDI et al, 2015, p. 16).

A *Internet*, enquanto constructo representativo da técnica informacional em seu apogeu, mostra-se enquanto um meio de comunicação marcadamente quente, em razão da alta definição, promovida pela expressiva saturação de dados que fluem por esse sistema comunicacional (MCLUHAN, 1969, p. 37). Na visão de MacLuhan (1969), os meios de comunicação eram, tipicamente, meios quentes ou frios, dependendo do nível de saturação informacional, promovida enquanto prolongamento de um sentido humano, portanto, sua definição, de acordo com a projeção de informações, simulando uma função tipicamente humana de percepção da realidade ontológica. Trata-se, assim, de um meio marcadamente massivo, permitindo a circulação de quantidades muito altas de informação, aqui representada em *bytes, kilobytes, megabytes, gigabytes, terabytes e zetabytes*, valores que se adensam, cada vez mais, com a expansão da *Internet* e suas redes afluentes.

Apresentando-se como a “rede das redes”, a *Internet* assume, desde seus primórdios, um desenho em rede, capaz de, dentro da sinergia técnica, ser impactado por bases computacionais e comunicacionais anteriores e, além disso, modelar as manifestações de redes que seriam adotadas nas diversas dinâmicas que surgiam. A *Internet* tem seu nascimento atrelado às pesquisas militares e acadêmicas no âmbito da Secretaria de Defesa dos Estados Unidos da América, na década de 1970, especificamente, junto ao programa *Arpanet*, demarcando-se como um projeto estatal, nascido para finalidades militares e que, após a verificação de suas utilidades comerciais e científicas, passou por diversas partições, renomeações e privatizações, até assumir a forma que possui na atualidade (CASTELLS, 2013, p. 82). Assim como abordado antes, a *Internet* decorre diretamente da técnica computacional, haja vista ser esta, em sua concepção, um mero aglomerado de aparelhos computacionais, comunicando-se por meio de protocolos pré-definidos (FEIR, 1997, p. 362-363).

A *Internet* adquire relevância e importância em razão de seu ritmo expressivo de expansão, demarcando a ferocidade específica da técnica informacional. Klaus Schwab (SCHWAB, 2016, p. 19) indica que a revolução técnica informacional (tida pelo autor como a quarta revolução industrial) possuiria uma velocidade de expansão incomparável com relação às outras revoluções técnicas, demonstrando como, em menos de uma década, a *Internet* conseguiu espalhar-se pelo mundo.

A robustez do fluxo informacional formador da *Internet*, este tipicamente não linear e imagético, consagrando as construções flusserianas, define muito mais que um simples meio de comunicação de alta definição dentre diversos outros, capaz de carrear informações de forma saturada. Há que se conceber a *Internet* como o meio disponível de maior dimensão, seja pelo seu alcance sobre os mais diferentes lugares e comunidades, seja pela noção macluhaniana de saturação informativa. Os fluxos informacionais da *Internet* garantem a formação de novas circunstâncias globais, tipicamente uma nova escala de globalização, marcada pela instantaneidade e onisciência, capaz de desconstruir a distância, seja ela geográfica ou mental (HAN, 2018, p. 8).

Por meio das novas tecnologias da informação e comunicacionais, em especial, a *Internet* e todo seu aparato remodelador, há a possibilidade de alcance de uma nova etapa na escala da globalização, esta marcada pelo rompimento drástico das distâncias e pela implementação de novas bases econômicas globalmente relacionadas (CASTELLS, 2003, p. 178). Assim, estrutura-se um modelo de capitalismo informacional, pautado em sistemas de comunicação ágeis, que garantem novas formas de exercício da atividade econômica, não mais pautada em padrões industriais, mas, sim, na alimentação de sistemas de produção por meio de informações, existentes em demasiada saturação no ambiente da *Internet*.

Há a assunção de papel primordial no meio informacional por parte da *Internet*, despontando como uma realidade concorrente com o mundo físico, dentro do qual há diversas manifestações de vivência e, inclusive, a presença de mecanismos jurídicos regulatórios de conduta, sejam eles estatais ou não. Assume-se, assim, a atemporalidade da informação não linear para ingressar em uma ambiência tida até mesmo utópica, onde é possível comunicar-se de forma facilitada, firmar relações contratuais, cometer delitos, manifestar poder e, por sua vez, praticar, simbolicamente, muitas coisas que, antes, eram realizadas no mundo físico.

Sem adentrar profundamente no assunto, há que se levantar a adoção de padrões de comportamentos virtuais, que antes eram realizados fisicamente, partindo de uma visão isotópica da *Internet*. É notável a diferença entre o mundo físico e digital, no entanto, a maior parte das ações humanas realizadas no mundo digital eram realizadas fisicamente, como exemplo, transações econômicas, o exercício da liberdade de expressão ou mesmo a comunicação digital, demarcando, assim, a adoção das redes enquanto aparato intermediador para a prática usual de nossa vivência. É necessário considerar a *Internet*, enquanto um meio de menor resistência, em diversos aspectos, no qual é mais fácil, seguro e ágil agir por intermédio da rede, motivo pelo qual é possível afirmar sua relevância prioritária e adoção massiva (CASTELLS, 2003, p. 416).

Luciano Floridi et al (2015, p.3) compreende que a vida hiperconectada, típica da realidade que nos cerca, é capaz de impor transformações relevantes na nossa vivência, refletindo diretamente na sociedade, quais sejam, um ofuscamento entre o real e o virtual, entre humano e máquina, havendo uma superposição das informações massivamente tratadas à realidade analógica.

A transição para o ambiente digital traz em si uma série de efeitos sociológicos, tendo como base não somente a transição técnica, mas uma efetiva remodelagem dos valores sobre os quais se estrutura a vivência humana. Migrando do mundo dos átomos para o mundo dos *bits*, visualiza-se uma transformação na consciência dos indivíduos, especialmente considerando a efetiva imersão na realidade informacional, na qual os indivíduos passam a ser marcados por uma cegueira quase deliberada e uma embriaguez na técnica informacional, afetando efetivamente a consciência individual e coletiva (HAN, 2018, p. 5), no qual malefícios problemas relacionados à técnica passam a ser omitidos em nome de um suposto avanço. Um ponto que merece atenção, em especial, por possuir uma carga econômica, é a derrocada das barreiras da vida privada, com uma aproximação da intimidade às questões públicas, tratando-se de uma realidade que reflete, diretamente, a dissolução de todas as balizas objetivas que sustentam a vivência, havendo a estruturação de toda uma economia pautada na exploração econômica de informações privadas. Acumulando-se a essa realidade, haveria, também, a erosão do espaço público, no qual a individualidade passa a se projetar, especialmente considerando a demarcação da natureza privada do ambiente informacional e a retração do Estado dentro de um ambiente amplo e transfronteiriço.

Inserindo-se em um meio sem balizas estáveis, portanto, formado por um simples “ponto modal de virtualidades que se cruzam (HAN, 2018, p. 56-57), a superficialidade passa a ser uma realidade marcante, conforme demonstrado antes no pensamento de Fluesser, sugerindo um estado transitório, que se projeta à grande parte da vivência digital. Portanto, sob o aspecto sociológico, percebe-se a suplantação de fatores e características inerentes à vivência física, com a ascensão de uma realidade digital, fluida e que se marca pela expansão do individualismo e, ao mesmo tempo, a retração dos espaços de intimidade.

Ao adentrar em discussões jurídicas, é necessário ter em mente a realidade da *Internet* como aquela derivada da técnica informacional, assim, de natureza imagética e decorrente da realidade física, de forma que diversas das projeções jurídicas incidem sobre a *Internet*, desconsiderando a diferença técnica desse meio com relação à essência jurídica. A própria migração rápida da vivência física para a digital, intermediada pela *Internet* (SCHWAB, 2016,

p. 19), acaba por causar uma espécie de “refração jurídica”¹⁰, havendo demanda regulatória sobre aquele ambiente, no entanto, existindo teorias distintas acerca da aplicação de modelos jurídicos usuais sobre aquela nova realidade. Conforme apresenta Julie Cohen (2007, p. 250), é necessário compreender as teorias do direito no ciberespaço, conjuntamente à compreensão das ciências e técnicas atinentes a essa nova realidade, como forma de evitar teorizações pobres e sem apego à realidade.

1.3 A Manifestação Digital do Direito

Ocorrendo o surgimento da *Internet*, diversos autores lançam-se sobre o tema para discutir a incidência de manifestações jurídicas sobre esse ambiente, seja para a regulação de relações ali estabelecidas, limitação de assimetrias de poder, ou mesmo a tutela e garantia de interesses individuais e coletivos. O ponto inicial da discussão sobre a incidência do direito do ambiente digital parte de construções de comunidades virtuais nascidas nos anos de 1990 (CASTELLS, 2013, p. 87), que agregavam integrantes dedicados à projeção da *Internet* como uma nova realidade, um novo ambiente sobre o qual seria possível reestruturar as relações de poder e, dessa forma, impor barreiras às práticas violatórias de direitos que eram comuns na vivência física.

Assim, a discussão dos pontos de encontro entre a *Internet* e a seara jurídica surge de bases anarquistas e libertárias de pensamento, estruturalmente ligadas ao próprio surgimento da *Internet* e seu desenvolvimento nos anos 1970, refletindo acerca da vedação desse novo ambiente com relação à antiga estruturação de poder, centrada na lógica estatal. Diversas comunidades virtuais, como o caso dos *cypherpunks*, com conotação anarquista, produziram variados documentos, como declarações e manifestos, indicando e orientando a *Internet* sob um paradigma de ausência estatal, e, dessa forma, vacante de qualquer regulação jurídica advinda do Estado.

Portanto, a teorização acerca do vínculo entre a *Internet* e o direito estatal advém de uma realidade não-jurídica, mas, sim, político-ideológica, frutificada na elaboração de manifestos e outros documentos encarregados de apresentar, ainda que sem apego coercitivo, uma série de princípios e intenções que deveriam reger o ambiente da *Internet*. Posteriormente,

¹⁰ Tomando empréstimo junto à seara das ciências da natureza, a refração diz respeito às mudanças de comportamento de uma onda, ao transitar entre meios de propagação. Refração jurídica, em semelhante sentido, diria respeito à incidência de normas típicas de uma realidade sobre outra, que, ao mudar de meio de incidência, sofrem robustas alterações e, da mesma forma, demandam alterações nas suas características para surtir efeitos minimamente viáveis.

após uma onda de autores debruçarem-se, ideologicamente, sobre a *Internet* e a natureza das relações ali desenvolvidas, passam os juristas a discutir tais questões, tendo como ponto de partida uma abordagem valorativa da rede, como ponto inicial da compreensão da incidência jurídica da rede.

Cumprido, aqui, citar que a abordagem da incidência jurídica sobre a *Internet* nasce nos Estados Unidos da América, na última década do século XX, advindo de uma maior popularização da tecnologia entre a sociedade, já estabelecida a base político-ideológica acerca do assunto e a ascensão das demandas jurídicas por parte da sociedade, que passavam a chegar, massivamente, no judiciário (OLSON, 2005, p. 11). Diante de novas tecnologias, dificuldades interpretativas e de aplicação de normas à *Internet*, seja sob a dinâmica dogmática ou política, visualiza-se um fomento da atividade acadêmica sobre o assunto, com juristas consagrados debruçando-se sobre o tema, como Orin Kerr (2003), David Johnson (1996), David Post (1996) e Lawrence Lessig (2006), dentre diversos outros.

Ressalta-se que o foco com relação à incidência jurídica sobre a *Internet* funda-se no papel primordial dessa tecnologia dentro da realidade informacional, especialmente considerando o seu quase monopólio na concentração dos utilizadores, fazendo comunicações e atuando dentro de um ambiente virtual. Dessa forma, partindo de uma análise técnica, sobre a qual se indica a suposta falibilidade da realidade jurídica incidir sobre as estruturas ligadas à técnica informacional, seu principal expoente, em razão até de comungar bilhões de utilizadores em todo globo, deve ser a análise da *Internet* e a sua relação com o direito.

1.3.1 Conflito de perspectivas acerca da *Internet*

Considerando a *Internet* enquanto uma ambiência de convivência humana, marcada pela realidade técnica informacional, é necessário compreender a existência de manifestações de poder sobre esse ambiente, que ocorrem de forma regulada na maior parte dos casos e, dessa forma, ensejando a manifestação digital do direito, considerando sua adequação à realidade informacional regente. As bases da incidência do direito sobre a *Internet* dependem, conforme expõe Orin Kerr (2003, p. 357), de um ponto de partida sobre o qual serão compreendidos os fatos sujeitos à regulação normativa, assim, sendo esses fatos determinados conforme padrões “reais” de existência, externos à rede, e padrões “virtuais” de realidade, interno à perspectiva da *Internet*. Nesse momento, vê-se presente a discussão tão bem trazida pelos filósofos da técnica e da informação, indicando a relação direta do direito com a técnica e, especificamente, as formas pelas quais o direito na *Internet* assumiria uma conotação “imagética”.

Assim como em outros casos de divergência técnica entre a norma e o aparato intermediador das condutas humanas, há que se conceber as dificuldades inerentes à aplicação do direito, seja pela divergência técnica da dogmática ou pela incapacidade compreensiva do Estado-Juiz (KERR, 2003, p. 362). A aplicação incondicional do direito vigente, o recurso às metáforas interpretativas (OLSON, 2005, p. 10), ou mesmo a adoção de práticas legislativas condizentes com a nova realidade técnica, acabam por ter origem na apreensão dos fatos ocorridos naquelas realidades, conforme um padrão definido de valores, que são aportados pelos atores do ambiente jurídico sobre as práticas humanas sujeitas a medidas deontológicas, motivo pelo qual o fator base da compreensão de todas as possibilidades de incidência jurídica partem da captação dessa realidade pelas experiências humanas.

O ponto base para a manifestação digital do direito e a sua compreensão é a análise da dualidade de perspectivas existentes sobre os fatos da *Internet*, que são capazes de alterar, completamente, a incidência normativa sobre a rede informacional e definir a ambientação jurídica cabível. O conflito entre as perspectivas demonstra nada menos do que o choque entre construções técnicas baseadas em realidades divergentes, aparatos construídos sobre realidades técnicas distintas e, assim, sofrem com certo grau de incompatibilidade.

Enquanto o direito estatal, ainda atrelado à técnica industrial, é pautado na ambiência física e materialista, dependendo de uma compreensão palpável da realidade que o cerca para cumprir seus objetivos, a *Internet* e as tecnologias informacionais mostram-se pautadas sob um paradigma técnico informacional. Assim, as redes são marcadas pela superficialização da realidade, em seu sentido flusseriano, concebendo “realidades virtualizadas”, metaforicamente construídas sobre espaços onde não há espaço¹¹, ambiente que confronta, diametralmente, com a realidade física do mundo externo à *Internet*. Desse choque de realidades técnicas, surge o problema das perspectivas incidentes sobre os fatos advindos da *Internet*, fator essencial para a compreensão das dinâmicas jurídicas incidentes ou emergentes da rede, sendo ponto essencial de discussões jurídicas envolvendo a *Internet*.

A *Internet* figura como a primeira tecnologia a ensejar o surgimento de um conflito de perspectivas com tamanha predominância nas discussões jurídicas, levando a diversas teorizações a respeito. A *Internet* apresenta-se como uma tecnologia de uso constante que, na sua estruturação, garante a existência de uma realidade virtual aos seus utilizadores que é

¹¹ A noção do espaço na *Internet*, enquanto ciberespaço, acaba por ser uma construção metaforicamente concebida, trazendo para um ambiente superficial conceitos aplicáveis, especificamente, ao ambiente físico que nos cerca. A adoção metafórica refere-se à necessidade de interseção entre as duas realidades, de forma a construir meios adaptáveis para compreender uma realidade nova, inovadora (SANTOS, 2004).

extremamente realista, possibilitando, até mesmo, a aplicação de metáforas quanto à existência de um espaço além do espaço (KERR, 2003, p. 388).

Diversos autores debruçam-se sobre a questão dos paradigmas envolvidos na regulação jurídica dos fatos da *Internet*, havendo indicações de viabilidade, legitimidade e adequação em ambas as perspectivas, no entanto, com cada uma delas gerando resultados jurídicos muito diferentes (FRISCHMANN, 2003, p. 207). A incidência regulatória sobre fatos jurídicos novos, sujeitos às inovações técnicas marcantes, depende, inicialmente, da perspectiva que adotamos para os fatos dali emergentes, compreendendo-os sob um paradigma virtual ou material, permitindo, assim, a captação das dinâmicas e práticas sob um ponto de vista já estabilizado. Definida a perspectiva de análise, seja essa interna ou externa, surge a demanda regulatória sobre os fatos ali presentes, exigindo a aplicação metafórica do direito vigente, em clara atividade supletiva (OLSON, 2005, p. 10), a abstrata atividade legislativa das relações emergentes ou mesmo ensejando a regulação prática provida por fontes privadas, conforme descreve, com maestria, Lawrence Lessig (2006, p. 22).

Importante ressaltar que, conforme apresentam diversos autores (KERR, 2003, p. 362), as perspectivas são dois caminhos distintos para a compreensão das relações jurídicas existentes na *Internet*, de forma que essas perspectivas não são, necessariamente, paralelas, podendo livremente se cruzarem, muito embora ressalte Orin Kerr que isso não ocorreu, e provavelmente não ocorrerá. Ainda assim, é necessário conceber a possibilidade de confluência entre as perspectivas distintas, considerando a importância dessa definição de perspectiva para compreender qual é ou será a legislação aplicável a essa realidade virtual.

1.3.1.1 Perspectiva Externa e o Isotopismo Jurídico

A primeira perspectiva a ser considerada é a externa, tipicamente marcada por uma concepção técnica industrial, assim, caracterizada por uma análise fática apartada da superficialidade virtual da *Internet*. Apesar de ser uma tendência tida por muitos autores como uma reação ao utopismo jurídico (COHEN, 2007, p. 219), a abordagem técnica que se segue no trabalho exige construir, primeiramente, tal ponto de vista, que tem menos rupturas com o modelo jurídico incidente sobre o mundo real. Portanto, inicia-se a abordagem junto à visão externa, tipicamente tida como não excepcionalista ou mesmo isotópica, fluindo de uma tendência técnica industrial e materialista para, posteriormente, abordar teorias jurídicas mais condizentes com um filtro valorativo técnico-informacional, aquelas tidas como internas, excepcionalistas ou utópicas.

A visão externa, conforme expõe Orin Kerr (2003, p. 360), vê a *Internet* sob o ponto de vista de seu funcionamento no mundo real, abandonando completamente a “experiência de percepção dos utilizadores”. Portanto, partindo de uma visão externa, a *Internet* consistiria em um aglomerado de computadores e servidores, conectados por cabos telefônicos de alta velocidade e comunicando por meio de protocolos pré-estabelecidos do tipo TCP/IP (FEIR, 1997, p. 362-363), através dos quais há a transmissão de sinais binários (uns e zeros representados por signos elétricos), que são traduzidos por *hardwares* e *softwares* em comandos, textos, sons e imagens. As virtualidades são simples superficialidades, de forma que a real importância incidiria sobre os detalhes técnicos que compõem a rede de estruturação da *Internet*, de forma que essa ambiência física seria composta por realidades físicas, pouco manipuláveis, em contraste à facilmente manipulável percepção da virtualidade (KERR, 2003, p. 362).

Dessa forma, a perspectiva externa não diferencia o ciberespaço e o espaço real com relação aos fatos ali ocorridos, assemelhando aquele “ambiente” com qualquer outra forma de comunicação, desconsiderando, portanto, toda a dinâmica disruptiva que advém do incremento da técnica informacional. Goldsmith (1999, p. 1238-1239) concebe que as diferenças entre o ciberespaço e as tecnologias comunicacionais anteriores não são nada maiores do que as mudanças entre as tecnologias pré e pós-telégrafo ou pré e pós-telefone, motivo pelo qual se pode inferir que a regulação estatal usual seria suficientemente cabível para incidir sobre as relações provenientes da rede.

A *Internet* e o ciberespaço, sob essa visão, seriam conceitos apartados, nos quais o primeiro termo referir-se-ia a um espaço real e lógico, formado por infraestruturas físicas de aplicação e comunicação (*hardwares*), computadores, servidores, cabos, *modems* e centrais de direcionamento de dados, enquanto o ciberespaço, metaforicamente concebido, seria o conjunto das experiências humanas advindas do uso de aplicações e realização de comunicações por intermédio dos *hardwares* (FRISCHMANN, 2003, p. 217). Diante dessa noção, a essência da *Internet* seria sua existência física, enquanto toda virtualidade advinda da percepção humana não teria relevância jurídica alguma, sendo mera construção, uma pareidolia diante de uma realidade que reflete superficialmente a existência física.

O ciberespaço, enquanto conjunto de experiências humanas intermediadas pela rede, na visão de alguns outros autores excepcionalistas, seria sim um “espaço”, levando em conta uma visão metafórica. No entanto, seria um espaço como qualquer outro, imerso na realidade física, constituindo mera transposição informativa de espaços reais (físicos), mera representação daqueles lugares e experiências vividas no mundo físico (EASTERBROOK, 1996, p. 82-84).

Aproximando-se de uma abordagem técnica, o ciberespaço consistiria em uma visão antropológica da rede, uma valoração humana capaz de trazer artificialidade a uma existência material, real e, assim, sob uma óptica orteguiana, conseguir ascender além das naturalidades que nos cercam.

A visão não excepcionalista ou isotópica da *Internet* considera que as relações humanas, realizadas por meio da *Internet*, não teriam qualquer diferencial quanto às questões essenciais (COHEN, 2007, p. 219), motivo pelo qual seria uma simples transposição da realidade e, assim, sujeita à ordinária regulação jurídica advinda dos padrões de soberania territorial. Apresentando exemplos, uma compra efetivada em algum site da *Internet* não teria diferenças essenciais com relação a uma compra efetivada em uma loja física, inexistindo diferenças, também, quando comparamos a supressão virtual de privacidade e a violação epistolar ou de sigilo telefônico.

Dessa forma, a concepção jurídica da *Internet*, pautada na externalidade, conceberia uma visão isotópica dos mundos virtual e físico, apontando uma linearidade entre esses “espaços” a ponto de justificar que o direito não sofreria qualquer exceção ao ser aplicado àquela nova “realidade”. Não haveria a necessidade de qualquer juízo adaptativo, dada a inalterabilidade das bases essenciais sobre as quais se agarrariam os mecanismos regulatórios do direito. Inexistiria qualquer dificuldade ou empecilho à efetiva aplicação e exequibilidade do direito sobre o mundo virtual, cabendo, além de semelhante incidência normativa, semelhante exequibilidade de direitos e deveres (COHEN, 2007, p. 220). Ignora-se, assim, a experiência tida pelos utilizadores no ambiente digital e o reflexo desta sobre as questões jurídicas.

Brett Frischmann (2003, p. 205) conceitua a *Internet* enquanto um simples mecanismo comunicacional, voltado às diversas práticas de operacionalidade do mundo físico. Todas as relações humanas não seriam desenvolvidas no ciberespaço, mas, simplesmente, intermediadas por uma série de máquinas e protocolos, ocorridos, em última análise, dentro do espaço real, dentro do mundo físico, portanto, sujeitos ao *ius imperii* do Estado e, por sua vez, regulados pelos ordenamentos jurídicos competentes. Jack Goldsmith (1999, p. 1238-1239) parte de uma concepção externa da rede para arguir a inexistência do ciberespaço, de forma que a sensação de ambiência gerada pela *Internet* não passaria de percepção humana projetada. Ante a inexistência do ciberespaço e a respectiva abrangência de toda *Internet* sob o manto do espaço real, caberia aos Estados exercer sua soberania jurídica e impor regulações sobre as atividades *on-line*.

A aplicação do direito sobre a *Internet*, dessa forma, não seria nada inovadora, sendo mera incidência de leis sobre fatos reais, intermediados por instrumentos de comunicação

(*Internet*), necessitando, no máximo, a realização de juízo analógico para adequação do ordenamento. Dessa forma, o conceito de *cyberlaw* ou direito cibernético seria um conceito totalmente vazio (SOMMER, 2000, p. 1147), dado que sua existência estaria limitada pela capacidade da doutrina jurídica preexistente de abarcar os novos fatos (HARDY, 1994, p. 1054), sendo essa capacidade ampla, diante da manutenção das essencialidades dos fatos ocorridos por intermédio da *Internet*. Conforme indica Jack Goldsmith (GOLDSMITH, 1999, p. 1238-1239), o ciberespaço não existiria enquanto espaço, motivo pelo qual a soberania poderia e deveria ser exercida pelos Estados sobre essa realidade, como forma de enfrentar uma sensação de “ciberanarquia” vigente no intelecto popular, inexistindo qualquer novidade na aplicação de leis sobre a *Internet*, demandando o simples estabelecimento de analogias, capazes de correlacionar a incidência da legislação vigente (KERR, 2003, p. 380).

Exemplificando, a visão externa da *Internet* foi densamente aplicada pelas cortes estadunidenses no final da década de 1990 e início dos anos 2000¹², adotando, analogicamente, à *Internet*, a legislação e doutrina referentes aos direitos reais. Concebia-se a *Internet* como uma experiência ocasionada por uma série de bens e direitos (servidores, *modems*, cabos, redes de transmissão, computadores, *softwares* e protocolos de comunicação e etc.), de forma que o acesso forçado a dados localizados em determinado computador, por intermédio da *Internet*, demandaria a aplicação da legislação e doutrinas referentes à violação da posse de bens móveis (tidas na *common law* como *trespass to chattels*) (MCGOWAN, 2003, p. 353-354).

Portanto, no ambiente de regulação, a visão isotópica conceberia a legitimidade da incidência do *ius imperii* dos Estados sobre a *Internet*, projetando suas soberanias com base na localização física dos aparatos técnicos viabilizadores da rede, sendo plenamente cabível aplicar o direito estatal sobre as vivências da *Internet*. Tracejando juridicamente a *Internet* com base em um ponto de vista externo, simplesmente, aplica-se a lei relativa à operação ou ato realizado por intermédio da rede, ou seja, uma transação virtual ensejaria a aplicação da norma contratual geral, assim como uma injúria online exigiria a simples aplicação do tipo penal (KERR, 2003, p. 361). Não havendo relevância jurídica nas “existências” virtuais das pessoas, o direito exerceria sua coação pela simples incidência sobre a existência física, ou seja, o exercício da

¹² Vale citar os casos *Ebay v. Bidde's Edge* (EUA, 2000), *Intel Corp. v. Hamidi* (ESTADO DA CALIFÓRNIA, 2003), *Thrifty-Tel v. Bezenek* (ESTADO DA CALIFÓRNIA, 1996), casos em que há a aplicação de um paradigma externo da rede, concebendo formas de acesso não autorizado a dados, via *Internet*, como uma violação do direito de propriedade sobre os bens móveis que compõem a estrutura da rede. Assim, a utilização não autorizada de um servidor, um bem móvel, seria a essência de uma violação de privacidade sob o paradigma externo.

coação física institucionalizada que, por causar efeitos sobre a realidade espacial humana, acabaria gerando reflexos na representação virtual da *Internet*¹³.

A parte essencial da incidência jurídica diante da perspectiva externa seria a aplicação de analogias capazes de, diante de uma realidade técnica divergente daquela que rege o ordenamento jurídico, indicar paralelos de compreensão e compor bases comuns de entendimento. Diante de um conflito entre o direito e a técnica sujeita à regulação, dado o paradigma isotópico, torna-se necessário fugir a metáforas, fazendo comparações com outras tecnologias já melhor compreendidas e fagocitadas¹⁴ pelo direito para, dessa forma, conseguir aplicar o ordenamento vigente (OLSON, 2005, p. 10). Assim, o ordenamento jurídico é suficiente para regular as relações jurídicas ocorridas na *Internet*, bastando, por sua vez, mero exercício compreensivo e analógico por parte dos juristas, mantendo-se, dentro de uma dinâmica juridicamente segura, sob a regência hermenêutica das regras hierarquicamente constituídas.

1.3.1.2 Perspectiva Interna e o Utopismo Jurídico

Por outro lado, uma visão interna da *Internet* levaria à concepção da *Internet* como uma ambiência *sui generis*, uma nova realidade espacial sobre a qual as relações humanas tomam novas roupagens, perfazendo uma teorização tida pelos autores como o utopismo da *Internet*¹⁵. Pautando-se em uma base técnico-informacional, concebe-se a *Internet* como o reino da mente humana, um local afastado do ambiente físico e, assim, sujeito a uma nova incidência normativa, que diverge daquela existente sobre o mundo físico. Dessa forma, parte-se de uma visão pautada nos paradigmas internos da *Internet*, ou seja, uma visão que tem todas suas

¹³ Conforme indica Orin Kerr (2003, p. 362) as correlações entre o espaço e o ciberespaço não são bilaterais, de forma que o real é capaz de produzir reflexos sobre o virtual, enquanto a virtualidade, por sua vez, não é capaz de se manter dentro dos limites exatos da realidade. Essa falta de correlação entre o real e o virtual acaba por produzir efeitos legais, de forma que a adoção de um conjunto ótico interno, para aplicar modelos regulatórios e averiguar os resultados, consegue existir independentemente dos resultados obtidos na externalidade da rede, no mundo real. Ou seja, a aplicação legal, sob um paradigma interno, é capaz de produzir estritamente virtuais, sem reflexos latentes no mundo exterior.

¹⁴ Utilizo a expressão fagocitar para referir à compreensão e incorporação jurídica de “corpos estranhos”, realidades técnicas que divergem daquela vigente sobre a norma e, por procedimentos analógicos, conseguem ser adquiridas pela esfera de incidência jurídica.

¹⁵ Utopismo, em seu sentido primogênito, relacionado a um “não lugar”, uma ambiência divergente da nossa realidade e que, dada sua novidade e propensão às mudanças sociais, políticas e econômicas, pode ser atingida futuramente. É importante fazer essa desambiguação visto que, conforme ressalta Marília Pinheiro (2006, p. 147), utopia e utopismo adquiriram conotações ambíguas, muitas delas até mesmo pejorativas, afastando-se em muito da visão de Thomas More, que tem por base projetar uma sociedade ideal. A *Internet*, diante da visão utópica, daria indícios claros de que essas mudanças teriam sido atingidas, criando uma sociedade e um “espaço” que divergem do mundo físico ao constituírem-se “reinos da mente humana e da sua liberdade” (BARLOW, 1996).

diretivas oriundas da experiência humana dentro da realidade virtual. A *Internet* é concebida nos termos das suas aplicações e de como elas impactam na experiência dos utilizadores (FRISCHMANN, 2003, p. 205).

Surgindo de uma dificuldade técnica de conceber novas realidades e aparatos, é necessário compreender a *Internet* como um ponto de inflexão, um ponto em que a concepção técnica adota novos modelos e, por sua vez, passa a ocorrer incompatibilidades nas suas relações. A *Internet* seria uma realidade metafórica, de forma que a novidade técnica atinente a esse meio, as relações ali desenvolvidas e as experiências, não teriam forma de compreensão, senão através de metáforas da realidade física (OLSON, 2005, p. 10).

A limitação, ao menos temporária, em compreender essa nova realidade técnica informacional é explicada, por alguns autores, por meio do uso de jargões e termos típicos da realidade física para descrever a vivência na *Internet*, indicando um pensamento ainda fincado no mundo dos átomos¹⁶. Juridicamente, essa limitação inicial, de conceber *Internet* e sua ambiência, é representada pela aplicação forçada (e sem apego técnico) da legislação sobre o ambiente físico, visando causar reflexos sobre a ambiência virtual que, apesar de causarem certos efeitos regulatórios (FIRMINO et al, 2018, p. 390), ainda não conseguem ser eficientes na sua incidência, impondo gravame a grande parcela do pensamento jurídico isotópico.

Um exemplo da aplicação ineficiente do direito sobre o mundo dos átomos advém da difícil produção de efeitos legais sobre práticas de violação da intimidade, por intermédio da rede, nas quais a vastidão da rede e seu alto grau de anonimato propiciam uma dificuldade regulatória (GÓIS JR, 2002, p. 95), de forma que a legislação do mundo físico possui mínimo apego até mesmo para entes sujeitos a limitações estritas, como o caso do Estado. A prática nos mostra que, mesmo diante de exigências legais robustas para o acesso à privacidade por parte do Estado, há reiteradas medidas de acesso a dados privados adotadas sem prévio cumprimento das formalidades exigidas (MARCHETTO; BARRIENTOS-PARRA; RODRIGUES, 2019).

Apesar de ter sua origem atrelada à realidade física, a virtualidade provida pela *Internet* firma-se como um espaço autônomo, possuindo uma base de vivência que se distancia do

¹⁶ Há uma dependência, ao menos inicial, do uso de metáforas da realidade física para compreender a vivência digital, como, por exemplo, “Navegar pela *Internet*”, através dos “sítios” virtuais, “correntes e cadeias de dados”, dentre outros diversos termos. Autores aproximados com a visão utópica da *Internet* tentam afastar os efeitos dessa “metaforização” do ambiente digital, especialmente com relação à esfera jurídica. Segundo esses autores, como Kathleen Olson (2005, p. 11), o emprego de metáforas jurídicas, de forma excessiva, durante a compreensão inicial da realidade virtual, levou a uma equalização fictícia do ciberespaço e do espaço físico, um isotopismo forçado e antinatural, carreando para uma regulação ineficiente e pouco adequada. Essa equalização de realidades distintas foi vista, por exemplo, no surgimento de uma visão da *Internet* enquanto propriedade privada, sujeita, portanto, aos regimes dos direitos reais, opondo-se àquela realidade como um espaço público de construção e convivência.

mundo físico e garante que as experiências ali vividas tenham relevância autônoma. O mundo virtual teria uma existência apartada, paralela do mundo físico, que é legítima em si (KERR, 2003, p. 385), sendo a *Internet* uma porta de acesso a essa nova realidade, em que podemos restabelecer nossas relações e, além disso, criar novas situações de incidência jurídica. Apesar da *Internet* contar com um conjunto de aparatos técnicos (*modems*, cabos, servidores, etc.) que a estabelecem, a abordagem desses aparatos não teria qualquer relevância jurídica, visto que as interações humanas ocorrem sob o manto de uma realidade *on-line*. Sob a vigência de uma realidade apartada do mundo físico, ao menos ao nível da experiência, haveria que se considerar a validade de relações jurídicas distintas, capazes, até mesmo, de afetar a manifestação do Estado nesse ambiente informacional (COHEN, 2007, p. 15).

Barlow (1996) instaura uma visão utópica sobre a regulação jurídica da *Internet*, compreendendo-a como uma ambiência totalmente afastada do meio jurídico incidente sobre a realidade física, cujos institutos jurídicos e conceitos legais não contam com qualquer aderência, diante das relações estabelecidas na seara virtualizada. Assim como São Thomas More concebeu o “não-lugar” como uma realidade perfeita e totalmente afastada do mundo e suas dinâmicas, John Barlow estrutura sua argumentação, indicando que o meio digital se apresenta como um refúgio frente às práticas dos Estados, uma ambiência sobre a qual não incidem quaisquer normativas jurídicas do mundo real.

O autor indica a afetação à legitimidade sobre o ambiente digital por parte do Estado e, por outro lado, aproxima-se, também, da discussão acerca da sua incapacidade regulatória, manifestada na incompatibilidade dos espaços. Barlow (1996) estrutura o pensamento no sentido de que o mundo virtualizado constitui um “espaço social global” além dos limites da legitimidade dos governos estatais, motivo pelo qual inexistiriam pressupostos capazes de impor aos utilizadores dinâmicas regulatórias provindas dos Estados, sejam normas gerais e abstratas ou sua aplicação concreta. A coletividade na construção do espaço virtual e seu desenho em rede, incapaz de se limitar dentro dos padrões fronteiriços dos Estados, acabariam por impedir uma clara definição da sujeição jurídica dessa realidade às diretivas normativas provindas de Estados específicos¹⁷.

O ambiente digital, nessa visão, consistiria em uma realidade afastada do mundo físico, um espaço paralelo, apartado da realidade, com condições de experiência divergentes e

¹⁷ Barlow constrói o manifesto como uma resposta à elaboração e aprovação do *Telecommunications Act of 1996* (Ato das comunicações de 1996), normativa estadunidense, que passou a prever regulação sobre diversos aspectos da *Internet*, muitas dessas, conforme apresenta Barlow, inconstitucionais e diretamente atentórias aos direitos dos utilizadores da rede.

expressões de autoridade incondizentes com a lógica jurídico-estatal, motivo pelo qual o Estado encontraria barreiras reais para exercer poder sobre o ciberespaço. O Estado não possuiria qualquer legitimidade legislativa e jurisdicional, tratando-se de uma jurisdição apartada do mundo real, na qual as estruturas de poder e a manifestação do direito no mundo dos átomos não conseguiriam ter qualquer apelo, o que afetaria, diretamente, sua manifestação de soberania e a validade das normas jurídicas positivadas (BARLOW, 1996).

A concepção utópica, assim, pautar-se-ia na construção de uma governança da *Internet*, de forma que a rede e seus agentes, de forma análoga ao mundo físico, seriam capazes de estabelecer regras específicas àquela realidade, regras essas tecnicamente coerentes e legítimas (KERR, 2003, p. 372). Acerca da regulação da *Internet* sob uma perspectiva interna (LIMA, 2000, p. 18):

[...] (o funcionamento da rede) não é plenamente conhecido por aqueles que a utilizam e, mais ainda são incipientes e exploratórias as formas de sua regulamentação. [...] a tentativa de regulamentar um espaço destes- que produz, mesmo, um meio específico, o ciberespaço, anárquico, individualista, autônomo, com dimensões incontroláveis, em que os utilizadores se movem com enorme rapidez e se relacionam de forma profundamente igualitária- teria necessariamente de levar em consideração essas características, geradoras de uma multiplicidade de regras em constante reformulação, para entender aos aspectos profundamente dinâmicos das interações ali atualizadas.

David Johnson e David Post (1996, p. 1379) compreendem a aversão exposta por Barlow ao teorizarem acerca das fronteiras do real e a regulação jurídica. Os autores partem da noção de que o ambiente digital da *Internet*¹⁸ possuiria uma jurisdição apartada do mundo dos átomos, de forma que toda produção legislativa ou jurisdicional não teria sintonia com as práticas desenvolvidas naquele reino e sofreriam a ausência de mecanismos de persecução. Assim, as normas vigentes no ambiente dos átomos não vigeriam, necessariamente, no âmbito da *Internet*, visto que as fronteiras estatais, dentro do espaço digital, não possuem qualquer clareza, fragilizando o exercício da soberania e afetando a legitimidade da incidência regulatória dos Estados.

O Estado e seu direito, ainda amparados em concepções industriais e materialistas, sofrem graves fragilidades na projeção da sua soberania sobre o ciberespaço, haja vista a intensa nebulosidade que ainda paira sobre a imposição de dinâmicas legais regulatórias sobre essa

¹⁸ A realidade física e o mundo digital estariam bem delimitados, sendo facilmente perceptível a transição entre o espaço digital, intermediado por telas e outros aparatos capazes interpretar, superficialmente, a realidade imagética do mundo virtual. Apesar da ausência de dimensões espaciais, muito bem encaminhadas à discussão pelos geógrafos (SANTOS, 2004, p. 277), há que se conceber que o ciberespaço estaria além das fronteiras entre Estados, enquanto uma nova zona além dos limites materiais, estabelecendo uma nova realidade, inacessível pelos institutos jurídicos que disponibilizamos (JOHNSON; POST, 1996, p. 1379).

nova realidade. Conforme esclarecem Johnson e Post (1996, p. 1397), a aplicabilidade e a legitimidade das normas jurídicas sofrem degradação diante do fenômeno da *Internet*, tendo como paradigma central a estruturação de uma nova realidade, afastada do mundo físico e, por sua vez, estruturada externamente às fronteiras geográficas, que delimitam o direito estatal, não sujeitas diretamente ao exercício do poder de fato.

As fronteiras seriam, conforme apresentam os autores (JOHNSON; POST, 1996, p. 1379), bases para a definição da incidência de determinado ordenamento jurídico sobre indivíduos e relações, de forma que a impossibilidade de definição fulgente do ordenamento jurídico, incidente sobre a *Internet*, impossibilitaria qualquer Estado de exercer, legitimamente, seu *ius imperii* sobre aquela realidade. A ausência de limitações expressas e de reconhecimento amplo às fronteiras estatais no ambiente digital cria um ambiente cheio de embaraços jurídicos à incidência regulatória estatal. Dessa forma, há importantes diferenças entre o espaço e o ciberespaço que acabam por minar a capacidade de os Estados exercerem soberania e regularem as relações.

Conforme indica o manifesto político de Barlow (1999), muito bem respaldado por Johnson e Post, é possível conceber a extraterritorialidade do direito enquanto sua possibilidade de aplicação junto a outros locais, que não seu território originário, no entanto, ao se deparar com o ciberespaço, estaríamos confrontando uma realidade paralela, apartada da lógica do “mundo dos átomos”. Seria um “ambiente” sem materialidade, pautado pela mera técnica informacional, enquanto uma superfície etérea de significação, incapaz de se sujeitar ao poder de fato exercido pelo Estado.

Essa situação faria surgir uma inadequação jurídica do direito estatal sobre a realidade digital e, como consequência, esse ambiente proveria sua própria legalidade e seus próprios institutos de regulação, nascidos junto à realidade informacional e, assim, adaptados àquele ambiente imaterial, levando em conta que, conforme indicam Johnson e Post (1996, p. 1389), seria impossível afirmar, com clareza, que a *Internet* ou qualquer de seus domínios estaria vigendo em um modelo “alegal”, ideologicamente próximo à anarquia.

É importante considerar que, dentro de uma visão utópica, há que se conceber a fragilidade da força normativa do Estado sobre a *Internet*, portanto, abrigando maior importância junto às demais instâncias reguladoras, que contariam com apego técnico à realidade virtualizada. Inicialmente, haveria que se falar na regulação jurídica exercida pelo mercado na *Internet*, provendo normas capazes de regular, ao menos na esfera mercadológica, as relações estabelecidas dentro daquela ambiência, além da regulação costumeira e codificada.

As incertezas acerca da aplicação do direito estatal na *Internet* levariam os entes privados a proverem regulações mínimas para a vivência digital, ao menos sob a égide de seus sítios digitais e aplicações (YEN, 2002, p. 1258-1259), refletindo, assim, uma privatização do ambiente digital, com o exercício do poder concentrando-se na esfera privada, muito embora tenha que se considerar a incapacidade desses interesses regulatórios de entidades privadas em atender aos objetivos da grande maioria dos utilizadores da rede (OLSON, 2005, p. 16), relembrando, assim, uma visão crítica sobre as estruturas de regulação, típica da primeira onda de pensadores utópicos.

Há que se conceber, também, o papel dos costumes da rede, enquanto padrões de conduta socialmente estabelecidos para a vivência no mundo digital. Indica Lessig (1998, p. 662) que o costume teria uma importância secundária dentre as forças, portanto, em uma posição intermediária entre a regulação estatal e as demais forças, indicando um valor decorrente da prática social. Ao contrário das normas estatais, promulgadas e executadas por intermédio da ameaça de sanções legais, os costumes teriam vigência através da simples aquiescência social (POSNER, 1997), confluindo, em muito, com as bases de expansão da *Internet*¹⁹ e a estruturação de ambientes regulados livremente pelos costumes dos utilizadores da rede. Trata-se de uma regulação comunitária, aproximando-se muito da visão utópico-anarquista de John Barlow, concebendo normas de convívio digital com base “na ética, nos interesses iluminados e no bem comum” (BARLOW, 1996)²⁰, sendo esses a base para a construção de um contrato social costumeiro, capaz de reger o mundo dos *bits*.

1.4 A Dicotomia Átomo-Bit²¹ (?)

Compreendidas ambas as visões atinentes à incidência jurídica da *Internet*, é necessário visualizar uma dualidade constante entre as perspectivas jurídicas da *Internet*, ocorrendo uma dualidade ferrenha entre a regulação da *Internet* por meio de uma incidência jurídica externa,

¹⁹ A ideia da *Internet*, enquanto passa a se expandir com a popularização, ao menos em nível de países desenvolvidos, dos meios computacionais de acesso à rede, momento esse em que a *Internet* passa a adquirir uma noção segmentada, com diversas comunidades se formando, cada uma delas voltada para determinadas práticas no ambiente virtual (CASTELS, 2002, p. 88). Cada comunidade, ligada por interesses em comum ou práticas correlatas, como o caso da comunidade *hacker* ou da comunidade *cypherpunk*, passa a ter um conjunto de práticas virtuais que adquirem noção de costume, vinculante pela simples acessão dos utilizadores.

²⁰ “*We believe that from ethics, enlightened self-interest, and the commonweal, our governance will emerge.*” (BARLOW, 1996) (tradução livre).

²¹ Termo inicialmente utilizado por Jean-François Blanchette (2011) no artigo “*A material history of bits*”, no qual há a discussão da *Internet* com uma natureza dúplice, material e imaterial. Termo utilizado na esfera jurídica no artigo “*A técnica informacional como ferramenta de redução da privacidade na rede: análise do caso Wikileaks*” (MARCHETTO; BARRIENTOS-PARRA; RODRIGUES, 2019).

advinda do direito estatal com singelas adaptações à realidade técnica da rede, ou por meio de uma regulação jurídica interna, advinda de fontes normativas nativas da própria *Internet*, tão bem descritas por Lessig (2006) como as forças codificantes da *Internet*. Assim como descreve Orin Kerr (KERR, 2003, p. 362), tratam-se de visões que não são necessariamente paralelas, com cada uma dessas possuindo relevância na concepção jurídica da realidade informacional.

Partindo de uma concepção utópica da rede e da sua regulação, conceber-se-ia uma realidade na qual a incidência jurídica sobre os átomos e os *bits* é expressivamente divergente, de forma que os ordenamentos jurídicos vigentes na realidade física não teriam força normativa dentro da *Internet*, prevalecendo uma abordagem da derrocada da soberania estatal. Assim, haveria que se considerar uma crise de legalidade (RODRIGUES; MARCHETTO, 2020, p. 737) no ambiente virtual, sob o ponto de vista do direito estatal, de forma que a isenção de uma incidência jurídica, nessa perspectiva, ocorreria somente com relação ao Estado enquanto estrutura de poder, ainda concebendo e, na verdade, ratificando a incidência jurídica de outras formas de regulação.

Ainda que sob uma perspectiva utópica extremada, seria forçoso assumir que a *Internet*, mesmo diante de uma fragilidade de exercício de soberania por parte do Estado, adquiriria uma noção anárquica, de total ausência de mecanismos regulatórios. Com a devida *vênia*, a *Internet*, mesmo que regida por uma dinâmica utópica, não se comportaria como uma ambiência de completa inexistência normativa, como sugere Antonio Jeová dos Santos (2001, p. 11), estando presente, em seu meio, formas não usuais de incidência jurídica, mas que, ainda assim, trariam à virtualidade noções estritas de regulação. Ainda que sob a forma de costumes, regras mercadológicas ou codificações auto executivas, deve-se analisar a existência de regulações incidentes.

O direito incidente sobre o meio físico estaria diretamente sujeito ao exercício da soberania pelo ente estatal, que garante o substrato material de que as relações humanas sujeitas à regulação terão, em última instância, amparo no monopólio da força exercido sobre bases territoriais delimitadas. Recordando as lições de Hans Kelsen (1984, p. 50), a norma jurídica, enquanto instrumento típico de regulação das condutas humanas, teria como anteparo instrumental a existência de reprimenda direta ou indiretamente atrelada à violação de seu conteúdo, formando uma dualidade entre a imposição e a coação. A ordem jurídica teria como expressão uma série de diretivas orientadas ao plano do “dever-ser”, de forma que, qualquer ação realizada em sentido oposto a deontologia, exigiria a incidência de sanção, que é de conteúdo inseparável da própria norma.

Seja a norma positiva em seu aspecto abstrato, ou mesmo a norma individualizada aplicada pelo Estado-juiz, estas teriam dependência direta com relação à execução externa das medidas de coação, por meio do poder estatal institucionalizado, firmado na sua soberania sobre o sistema legal (KELSEN, 2007, p. 526). O poder soberano seria, portanto, aquele exercido pelo ordenamento jurídico, capaz de emitir comandos obrigatórios e, visando garantir sua própria essência (KELSEN, 1984, p. 371), estabelecer, sob a égide estatal, o exercício último do poder de fato como mecanismo de coação.

Assim, a soberania estaria atrelada ao exercício da coação, enquanto atividade necessária à manutenção da própria estrutura fundante do ordenamento jurídico. O exercício da coação pelas vias estatais, em última instância, seria condição *sine qua non* para o aporte desse sistema teórico sobre a realidade da *Internet*, de forma que a ausência de coercibilidade junto ao meio digital refletiria na derrocada da norma jurídica enquanto simples juízo hipotético (KELSEN, 1984, p. 51), que não prevê uma conexão clara e linear entre o rompimento da imposição e a incidência da coação. Em semelhante compreensão, Brennen e Kreiss (2016, p. 9-11) entendem que a nova realidade técnica instaurada foi capaz de fragilizar a soberania dos Estados, de forma a afetar, consistentemente, a capacidade legislativa e jurisdicional.

Castells (2003, p. 173) parte da mesma noção, afirmando que “a *Internet* solapou decisivamente a soberania nacional e o controle do Estado”, enquanto mecanismo comunicacional que, por excelência, foi capaz de retirar do Estado (ao menos em uma óptica inicial) seus mecanismos de controle. A fragilização do ente estatal, por meio da desestruturação dos seus engendramentos de poder (pautados, evidentemente, no direito, tendo como paradigma final o poder organizacional), representava a necessidade de uma remodelação desse ente e de suas projeções à esfera informacional, demandando um efetivo reaparelhamento técnico, capaz de harmonizar com a nova dinâmica informacional regente.

Assim como descreve Alfred Yen (2002, p. 1234), o ciberespaço tem como características inerentes a fragmentação dos poderes do Estado e, por sua vez, uma abordagem da autoridade política enquanto decorrência da propriedade privada, situação que posicionaria o exercício da soberania e a incidência jurídica mais próximos a uma realidade feudal. Portanto, dentro do ciberespaço haveria um afastamento com relação aos padrões de soberania e regulação jurídica firmados pós-Westfália²², causando embaraços às aplicações legais da realidade física sobre a *Internet*.

²² Fala-se aqui na Paz de Westfália, uma série de tratados, nos quais houve a fixação de um entendimento acerca da soberania dos Estados e sua limitação territorial, portanto, definindo os componentes e a extensão da figura do Estado (GROSS, 1948). Portanto, o Estado como conhecemos, enquanto poder jurídico aplicado sobre uma

Diante disso, alguns autores concebem a fragmentação da autoridade política e o exercício privado do poder no ciberespaço (YEN, 2002, p. 1248), o que afastaria o exercício da soberania nos moldes do Estado moderno e, ainda mais, inviabilizaria o exercício coativo do direito do mundo físico, apontando, portanto, uma diretiva utópica acerca da *Internet*, demandando normas atinentes a essa própria realidade.

Anna Mancini (2002, p.64) compreende a inviabilidade de aplicação do direito vigente à *Internet*, dada a natureza territorial que marca substancialmente esses constructos jurídicos. Sendo as normas do mundo físico estritamente ligadas às questões territoriais, ao seu nível substancial, há que se conceber a incapacidade dessas regras, sob uma visão interna, tutelar eficientemente o ambiente informacional da *Internet*. Diante dessa constatação, Mancini prevê a necessidade de o direito incidente sobre a *Internet* possuir linhas base mais ligadas à moral, fluidas e capazes de responder corretamente à liquidez da *Internet*, considerando o livre fluxo informacional como a base da governança cibernética.

Já aproximando dos criptoativos e tecnologias correlatas, outros autores, como o caso de Yochai Benkler (2013, p. 247), possuem fortes tendências utópicas e indicam o papel essencial da criptografia e do anonimato da rede para a imposição de empecilhos ao exercício de poder estatal sobre o ambiente virtual. Conforme traz o autor, o avanço dos métodos de criptografia e a estruturação de redes descentralizadas seriam construções comunitárias da *Internet* que acabariam por barrar o exercício da coerção estatal, instaurando um anarquismo prático. Partindo de uma base comunitária, Benkler (2013, p. 217) entende que haveria a possibilidade de, por intermédio dessas novas aplicações da *Internet*, construir uma regulação com base nos fracassos do Estado e do mercado, por meio do qual os utilizadores da rede conseguiriam estabelecer uma autogovernança pautada na circulação de informações em redes produzidas por pares comuns²³.

Nesse sentido, a autogovernança retrataria uma codificação, *lex informatica* em si, regulação provida por estruturas algocráticas (BOLDRINI, 2017), que seriam capazes de representar interesses comunitários, costumes de grupos voluntariamente agregados compondo ambientes democráticos ou não. Os ambientes autogovernados seriam, na visão de Benkler (2013, p. 217), anarquias funcionais, enquanto um dos métodos coerentes para evitar “a

população estrita a um território, adviria de uma noção Westfaliana de Estado e Soberania. Pós-Westfália representaria uma quebra com essa dinâmica, trazendo novas formas de soberania e de manifestação de poder.

²³ *Commons-based peer production* (em tradução, produção de informações por pares comuns) trata-se de um modelo inovador de circulação e produção de redes informacionais colaborativas, centrado na atuação comunitárias de agentes digitais (BENKLER; MORELL; HASSAN, 2020).

dependência direta ou delegada de poder estatal”²⁴, estruturando formas eficientes de regulação, estas capazes não só de incidir sobre relações virtualmente realizadas, mas também impor medidas executórias, estas advindas da utilização de mecanismos procedurais decorrentes da construção comunitária de códigos.

Sob esse paradigma, interno e utópico, a *Internet* não possuiria total sujeição ao direito estatal, apresentando os autores diversas teorias acerca dos motivos dessa situação. Seja a incapacidade de exercício da soberania, afastamento da legitimidade Estatal, fragmentação do poder político e da capacidade coercitiva dos meios estatais na rede, vê-se uma impossibilidade técnica do Estado, diante da expressividade da rede e sua fluidez, conseguir lançar meios capazes de garantir a aplicação do seu direito.

Partindo dessa visão, haveria a incidência de mecanismos regulatórios secundários sobre as relações existentes na *Internet*, como o caso da regulação mercadológica, dos costumes, da *lex informática* ou mesmo a ascensão de um modelo múltiplo, tendo como fundamento o utopismo²⁵ da incapacidade de o Estado incidir regularmente seu direito sobre a esfera digital. Não bastasse o utopismo jurídico, é necessário conceber também a construção de mecanismos não-estatais de regulação impostos por esferas de poder informacional, o chamado *law of code* (DE FILIPPI; WRIGHT, 2018, p. 52), que instauram códigos algocráticos (BOLDRINI, 2017), diretivas de controle sobre a rede que, de forma *ex ante*, impõem controle e sujeição.

Ainda que robustas as argumentações corroborando uma visão utópica da rede, sob um paradigma claro de divisão entre a incidência jurídica sobre o mundo dos átomos e sobre o mundo dos *bits*, há pontos chave na visão isotópica que, dentro da própria concepção de Orin Kerr, acerca das perspectivas jurídicas sobre a *Internet*, merecem ser consideradas, rompendo parcialmente com um unitarismo utópico.

O isotopismo, lançando-se sobre constatações práticas da realidade que nos cerca, consegue também indicar a relevância da sua perspectiva por meio da indicação de similitudes gritantes entre o mundo virtual e o mundo físico, apontando, especificamente, tais similaridades por meio da incidência, ainda que de forma reflexiva, do direito estatal sobre as relações ocorridas na *Internet* e seus utilizadores. Até certo ponto, haveria que se considerar um rompimento com a ideia primogênita da dicotomia átomo-bit, de forma que o direito estatal

²⁴ “By working anarchy, then, or mutualism, I mean voluntaristic associations that not depend on direct or delegated power from the State, and in particular do not depend on delegated legitimate force [...]” (tradução livre).

²⁵ Novamente, em seu sentido primordial, sem qualquer referência metafórica.

teria incidência similar sobre ambas superfícies e, dessa forma, não justificaria uma visão polarizada típica dos teóricos ideologicamente exacerbados.

Dentro mesmo dos utópicos, como o caso de Barlow (1996), há o reconhecimento de medidas adaptativas do Estado para a incursão junto à realidade informacional, como forma de incidir seu poder sobre aquela ambiência por intermédio das estruturas jurídicas. De certa forma, quando nos deparamos com a fragilização dessa dicotomia entre a incidência nos átomos e nos *bits*, torna-se possível compreender que o isotopismo jurídico abarcaria, em si, ambas as perspectivas, interna e externa, duas visões sobre as quais é possível compreender a incidência jurídica similar entre o mundo real e o mundo virtual. Ambas as perspectivas estariam presentes no pensamento jurídico isotópico de forma não conflitante, compreendidas, teoricamente, enquanto simples acepções para o Estado, no exercício da sua projeção de soberania, alcançar eficácia regulatória junto à rede.

Se, por um lado, o Estado incidiria sua regulação através de pontos de ancoragem da rede no mundo dos átomos, por meio de uma forma de refração regulatória²⁶ tipicamente externalista, o mesmo Estado também contaria com estruturas de poder nativas à rede, cooptando mecanismos computacionais para exercer regulação direta e interna sobre o mundo dos *bits*, indicando uma atuação pautada no paradigma interno.

A “terceirização” dos mecanismos regulatórios, exercidos através de agentes intermediários da rede, teria origem em um fracasso da regulação autônoma por parte do Estado, onde práticas ainda atreladas à lógica territorial de soberania e à censura e repressão (mecanismos típicos de uma dinâmica técnico-industrial) se mostrariam incapazes de incidir efetivamente sobre a vivência digital (CASTELLS, 2003, p. 175). John Barlow (BARLOW, 1996) fornece indícios do exercício do poder estatal sobre a rede através das estruturas de ancoragem, ou seja, sistemas de *hardware*, que existem fisicamente e viabilizam a virtualidade, de forma que é possível incidir regulações sobre essas estruturas e, assim, produzir reflexos sobre a esfera digital.

As estruturas de ancoragem são agentes intermediários entre o mundo dos *bits* e o mundo dos átomos, pessoas físicas ou jurídicas que administram sistemas de comunicação, servidores, prestadores de serviço de *Internet* e telefonia, desenvolvedoras de sítios virtuais e aplicações, dentre outros. Esses “componentes físicos da cadeia de funcionamento da rede” (MARCHETTO; BARRIENTOS-PARRA; RODRIGUES, 2019, p. 500) seriam porções de espaço sobre as quais é possível o Estado incidir seu direito (FIRMINO et al, 2018, p. 390),

²⁶ Vide nota 4.

lançando mão do seu poder organizacional²⁷ para, ao perpassar o meio digital, conseguir obter eficiência no exercício do poder legal (HOOD; MERGETTS, 2007, p. 171-173).

Tomando como exemplo, é possível incidir normas sobre utilizadores de determinada rede social, impondo regulações sobre a empresa administradora da rede, de forma a compelir os agentes intermediários a seguir diretivas normativas e, por sua vez, produzir reflexos sobre o objeto indiretamente regulado, que são os utilizadores.

Ocorrendo algum caso de injúria veiculada dentro de qualquer mídia social, basta que um magistrado officie à empresa administradora para o fornecimento de maiores informações acerca daquele utilizador, de forma que, com a inter-relação feita pelo agente intermediário, torna-se possível incidir normativas estatais sobre condutas digitalmente manifestas. Ressalta-se que a possibilidade de incidência do direito sobre a esfera digital advém do exercício de poder estatal nas esferas virtuais, no qual a utilização de agentes intermediários com melhores capacidades técnicas torna possível a manifestação digital do poder, reiterando a importância do componente coercitivo para a aplicação do direito.

Enquanto tema já consagrado na discussão acadêmica²⁸, vale abordar o caso do mecanismo chinês de controle de fluxo²⁹, uma série de serviços de filtragem de conteúdo e imposição de ônus a agentes intermediários (empresas fornecedoras de serviços de *Internet*, provedores de *Internet*, administradoras de aplicações e sítios digitais), que visam garantir controle do Estado sobre o conteúdo acessado pelos utilizadores e, além disso, promover atividades de vigilância (FEIR, 1997). Escapando do mérito das normativas de controle de acesso ao conteúdo digital e vigilância digital, percebe-se que há o emprego de agentes intermediários, estes com sujeição ao direito do mundo dos átomos, para impor regulações sobre o ambiente virtual.

Partindo para uma visão interna acerca do isotopismo, há a possibilidade de o Estado lançar mecanismos de regulação nativos à rede, portanto, não dependendo da refração do poder jurídico sobre a rede, de forma a exercer regulações por meio da *lex informatica* ou mesmo do exercício do poder organizacional, especificamente reflexo sobre a rede. Sob esse paradigma,

²⁷ Conforme descreve Hood e Margetts (2007, p. 9-11), o poder organizacional comportaria todos os instrumentos disponíveis ao Estado para agir diretamente, referindo-se ao poder material mantido pelos governos. Assim, por exemplo, a utilização de mecanismos coercitivos, pautados no monopólio da força, seriam manifestação do poder organizacional. O poder organizacional seria, portanto, o pessoal e meios disponíveis ao Estado para o exercício e *enforcement* da regulação.

²⁸ O tema é alvo de várias discussões multidisciplinares envolvendo a seara da liberdade e privacidade digital, tendo como paradigmas teóricos autores como os juristas Jack Landman Goldsmith e Tim Wu (2006), além de especialistas das ciências da computação, como Richard Clayton, Steven J. Murdoch e Robert N. M. Watson (2006).

²⁹ Mecanismo de controle de fluxo chamado pela doutrina de *The Great Chinese Firewall*.

não há que se falar na adequada incidência do direito estatal sobre a *Internet*, motivo pelo qual surge a necessidade de recorrer a outras ferramentas de poder.

O exercício do poder por meio da *lex informática* estaria diretamente atrelado à modalidade regulatória, enquanto uma das ferramentas de poder disponível ao Estado (HOOD; MARGETTS, 2007, p. 5-11), haja vista a sua atuação enquanto uma espécie de regulação, promovida por meio da elaboração ou supressão de códigos e programas capazes de balizar o comportamento dos utilizadores dentro de sítios digitais e aplicações. A modalidade regulatória diria respeito à preponderância de poder técnico por parte do Estado no interior da rede (DE BRUJIN; HEUVELHOF, 2018, p. 134), de forma que esse seria um nó essencial dentro da cadeia de informações na *Internet*, dando ao Estado posição estratégica dentro da rede para circular ou restringir a circulação informacional. Adentrando a rede enquanto nó essencial, teria o Estado capacidade para controlar a sua arquitetura, estipulando, por códigos de programação, quais seriam as condutas admitidas dentro da *Internet* e quais, por sua vez, não teriam sequer a condições de ocorrer.

Não bastasse isso, o poder organizacional do Estado também seria capaz de impor mecanismos de regulação advindos diretamente da expressiva capacidade técnica do Estado no interior da *Internet* (O'TOOLE JR; MEIER, 1999, p. 511). O Estado, conhecendo a técnica informacional de forma ímpar, teria a capacidade de forçar vias não admitidas pelos códigos de programação e, fazendo uso de fragilidades do sistema, impor regulação e controle sobre os utilizadores, atuando por meio da chamada “alegalidade” (LAPRISE, 2013).

A alegalidade seria, na visão de John Laprise (2013), uma decorrência da aplicação de poder organizacional puro sobre a realidade informacional sem a devida sujeição desse poder aos ditames constitucionais, de forma que a capacidade de codificar sítios digitais, acessar redes privadas e sistemas de aparelhos eletrônicos daria ao Estado uma capacidade cognitiva e regulatória extensa, muito além dos limites da legislação democraticamente constituída. O Estado adotaria uma nova arquitetura de controle pautada no rompimento com a própria legalidade do mundo dos átomos, lançando mão de meios ilícitos de controle e vigilância que partem de mecanismos sub-reptícios do próprio poder organizacional do Estado ou da imposição de deveres de controle a terceiros com maior capacidade técnica (CASTELLS, 2003, p. 182).

Muito além de um espaço semianárquico, seria um ambiente virtual ocupado pelo Estado para, fazendo uso do manto da “alegalidade”, agir conforme seus interesses regulatórios, promovendo práticas legalmente vedadas no mundo dos átomos. Um exemplo prático da regulação alega seria a obtenção de informações pelo Estado para medidas executivas, como o

combate ao terrorismo mediante informações privilegiadas obtidas de espionagem digital (PELL; SOGHOIAN, 2014, p. 23-26), ou a execução de medidas de controle e enfrentamento à pandemia de COVID-19 através da obtenção (sem autorização judicial) de dados de geolocalização de aparelhos celulares (RODRIGUES; MARCHETTO, 2020).

A alegabilidade, na visão do seu teorizador, aproximar-se-ia de um estado de exceção, marcando-se como um espaço desprovido de lei, seguindo de perto as icônicas construções de Giorgio Agamben (2004, p. 39). Seguindo os pensamentos do filósofo, não haveria que se considerar o espaço digital como um modelo ditatorial ou totalitário, haja vista que, mesmo sob tais circunstância, haveria uma estrutura jurídica reinante, apesar de uma “displasia”³⁰ na estruturação dos direitos (AGAMBEN, 2004, p. 13). Por outro lado, os espaços alegais seriam ambientes de excepcionalidade ao ordenamento jurídico estatal vigente, marcando-se por um estado de sítio.

Manuel Castells (2003, p. 181) observa tais práticas estatais, seja a atuação ilegal (aqui chamada de “alegal”) ou a prática codificante³¹, enquanto respostas do Estado face ao enfraquecimento da sua soberania e, por sua vez, a derrocada dos seus meios de controle do fluxo informacional. A junção de medidas legítimas e ilegítimas representaria a essência da atuação do Estado junto aos meios digitais ao menos sob a óptica interna, culminando no empreendimento de modelos algocráticos de regulação da vivência na *Internet*.

Considerando toda a capacidade técnica do Estado e seu papel essencial na criação e estabelecimento da *Internet* (CASTELLS, 2013, p. 44), entende o autor que o Estado contaria com efetivos meios para adotar diversas práticas na rede mundial de computadores, promovendo modelos de atuação que se opõem às limitações constitucionais do Estado. Portanto, através da “alegalidade” e do exercício de poder organizacional sobre a rede, haveria uma espécie de transplante do poder tradicionalmente manifesto no mundo físico para o ambiente da *Internet* (CASTELLS, 2003, p. 182).

Assim, compreendidas as fragilidades e pontos de sobreposição entre as perspectivas jurídicas acerca da *Internet*, vê-se uma inicial possibilidade de rompimento com a dicotomia átomo-bit, haja vista a validade e constatação de diversas manifestações jurídicas que incidem concomitantemente sobre a *Internet*, sejam elas provenientes de uma dinâmica utópica ou

³⁰ Uma má construção de determinada estrutura.

³¹ A prática codificante representa a capacidade de estruturar sítios e aplicações digitais com estruturas ocultas de controle e limitação, capazes de balizar as condutas para padrões já estabelecidos. Assim, um sítio digital pode não liberar acesso ao seu conteúdo, caso o utilizador não autorize a obtenção de dados de localização, indicando a utilização de algoritmos para a estruturação do exercício do poder de forma *ex ante* (GILLEPSIE, 2018, p. 102).

isotópica. Portanto, medidas nativas à rede, e oriundas do mundo dos átomos, acabam por relativizar e impor dúvida acerca de uma dualidade formal e estável entre a incidência jurídica nos ambientes físicos e virtuais, fazendo surgir a hipótese de cumulação de medidas externas e internas, compondo um ambiente de constante semelhança e dualidade entre o mundo dos átomos e o mundo dos *bits*.

Nesse sentido, Luciano Floridi et al (2015, p. 33) compreende uma realidade ubíqua, na qual passa a haver tamanha hibridização entre os átomos e os *bits* que se torna dificultosa a percepção das divisas entre essas duas realidades e, por sua vez, promoveria efeitos relevantes sobre as diretivas deontológicas. A dualidade de situações dá origem a uma unicidade de experiências, o que aproximaria as visões humanas sobre a *Internet* e o mundo físico.

Lawrence Lessig (1998, p. 663) concebe uma terceira via além do dualismo utópico-isotópico, compreendendo a incidência jurídica sobre a *Internet* como a ação coletiva de quatro forças regulatórias, cada uma delas sendo aplicada sobre a rede e as relações ali estabelecidas. Essas forças teriam uma atuação responsiva junto às matérias reguladas no ambiente da *Internet*, havendo uma autocompensação entre as forças regulatórias, de forma que a redução da atividade de uma delas representaria um avanço das demais. Não bastasse isso, qualquer alteração na incidência regulatória representaria uma mudança robusta em toda estrutura de incidência jurídica, seja ela autorregulada ou heterorregulada, reconstruindo os padrões de todas as forças incidentes (LESSIG, 1998, p. 664).

As forças regulatórias incidentes sobre o ambiente digital seriam as normas estatais, os costumes da rede, as regras do mercado e, por fim, a arquitetura programada da rede, cada uma destas atuando em concomitância com os demais e levando em conta a estrutura regulatória aplicada na prática, na qual as forças devem se equalizar sobre o objeto regulatório. Exemplificando, no caso do exercício regulatório estatal, por intermédio de normas, ser reduzido ou ampliado, essa prática geraria respostas sobre as demais forças, que, levando em conta uma nova dinâmica de incidência, deveriam adequar suas formas de regulação para se equalizarem com o novo conjunto de forças incidente e retornarem ao estado de equilíbrio.

Conforme expressa Lessig (1998, p. 666), há uma preponderância das medidas regulatórias com relação às normas provenientes dos entes estatais, assim, demarcando um rompimento do autor, ao menos inicialmente, com uma visão utópica da incidência jurídica. Conforme indica, a norma se sobressairia às demais forças regulatórias, ao passo que possuiria, além de um efeito direto sobre o objeto regulado, um efeito indireto, indicando uma capacidade do Estado em regular as demais forças. Assim, “as normas usam ou cooptam as outras forças

regulatórias em favor de seus próprios interesses”³², indicando uma dependência das demais forças regulatórias com relação às normas estatais. Dessa forma, há que se ver a regulação estatal sobre a *Internet* como a principal força, com as demais comportando-se como práticas de regulação alternativas que, apesar de terem relevância, não se sobrepujariam à regulação do Estado de Direito.

Ao atribuir uma relevância secundária à regulação mercadológica, Lessig (1998) encaminha uma visão ampla sobre o objeto regulado, que pode ser carregada perfeitamente à *Internet* de forma a não resumir toda a sua vivência aos padrões de mercado e experiências de consumo. A abordagem da *Internet* dentro de padrões estritamente mercadológicos, nos quais padronizações de oferta, demanda e preço seriam capazes de regular toda a vivência ali carregada, sufocaria expressivamente a ideia da *Internet* enquanto um ambiente plural e democraticamente concebido.

A mercantilização excessiva da *Internet* levaria a uma lógica estritamente privatista, rompendo em muito com a ideia da rede como uma ambiência em que os utilizadores são portadores de direitos, esses exercidos e advindos, primariamente, da própria lógica virtualizada da *Internet*. Essa dinâmica se oporia concretamente às noções primárias dos teóricos utópicos da rede, que concebiam a *Internet* como um ambiente garantido à liberdade humana em um estado nunca antes experimentado. A título de exemplo, vale citar que a adoção de uma visão estritamente mercadológica sobre a *Internet* a conceberia como um ambiente cuja liberdade e privacidade dos utilizadores decorreriam do exercício de um direito de propriedade, afetando consideravelmente a autonomia dos demais direitos exercidos na vivência digital e, de certa forma, carregando a uma abordagem externa fundamentalista, desconsiderando a totalidade das vivências virtuais.

Uma visão acerca dos direitos digitalmente manifestos, enquanto simples decorrências do direito de propriedade, acabaria por suprimir uma noção necessária de dignidade humana na rede. Sob o fundamento da dignidade do ser humano virtualmente presente, há que se conceber a impossibilidade de equivalência dos vários componentes dos direitos humanos ao simples direito de propriedade decorrente do mundo dos átomos, como bem descreve Kant ao discorrer sobre a dignidade (KANT, 2008, p. 81).

Seguindo de perto os problemas trazidos pela sobreposição da regulação secundária, a adoção de padrões costumeiros para a regulação do meio digital poderia representar aspectos de fragilidade na garantia e efetivação dos direitos fundamentais na rede, com a sobreposição

³² “*In this, the law uses or co-opts their regulatory power to law’s own ends.*” (tradução livre).

de medidas práticas que podem, diante de comunidades específicas, orientar a regulação para um caminho lesivo à própria dignidade da pessoa humana dos utilizadores. Toma-se como exemplo as comunidades virtuais da chamada “*dark web*”³³, como o famoso *site Silkroad* (SILVEIRA, 2018, p. 112), por onde eram comercializados produtos e serviços ilegais. Por meio de comunidades tendencialmente ilícitas, há a formação de padrões costumeiros opostos ao ordenamento jurídico e, dessa forma, opostos à própria tutela dos direitos humanos. Situação essa que, sob o ponto de vista de Lessig (1998), foge muito da dicotomia utopia-isotopia, justificando a sobreposição dos interesses estatais às dinâmicas comunitárias da rede, enquanto vinculados ao Estado de Direito, no entanto, sem estrangular essa regulação, que continuaria atuando sob um pretexto secundário.

Corroborando, em muito, a abordagem proposta por Lessig (1998), há que se ver uma realidade fluida da *Internet*, com a presença de experiências claramente utópicas, manifestadas pela omissão do direito estatal sobre a *Internet* ou mesmo a adoção de padrões de regulação estatal inovadores (como o caso citado da “alegalidade”), e experiências isotópicas, por meio de agentes intermediários. A presença de semelhantes experiências regulatórias acaba por desestabilizar a ideia da chamada dualidade átomo bit, mostrando que, sob certas condições, há uma paridade entre a regulação dos átomos e dos bits, mas, em outras situações, há a efetiva dualidade.

Manuel Castells (2003, p. 174) aborda bem esse rompimento com a dualidade regulatória ao indicar a *Internet* como um terreno contestado, onde ocorreria uma batalha constante entre forças opostas, tipicamente manifesta em um conflito pela privacidade e liberdade dos utilizadores. A *Internet*, assim, não seria um ambiente livre e neutro, com projeção de liberdade quase anárquica e ausência regulatória do Estado, no entanto, também não seria uma “profecia orwelliana” de controle e sujeição aos poderes institucionalizados, indicando que a *Internet* e sua regulação estariam mais próximas de uma interseção entre as visões utópicas e isotópicas, assim, desestruturando o paradigma maniqueísta.

Vê-se a necessidade de suplantar essa visão de dualidade, muito bem implantada no senso comum jurídico acerca da *Internet*, visão que é oriunda das construções ideologicamente exacerbadas dos utópicos da *Internet*. Semelhantemente, uma visão que toma o ponto de vista isotópico como uno acaba por desconsiderar uma série de eventos e experiências típicas do

³³ Conforme descrevem Pompéo e Seefeldt (2013, p. 439), a *Internet* navegável (chamada *surface web*) compreende todo um emaranhado de sítios e aplicações acessíveis por intermédio de sistemas de busca usuais, como o icônico *Google*. A *dark web* ou *deep web*, por sua vez, compreende todos aqueles sítios e aplicações que se “escondem” dos motores de busca usuais, seja por deliberação dos motores de busca, seja por ausentarem-se dos padrões dos técnicos dos protocolos da rede.

ambiente virtual e da realidade técnico-informacional, mostrando-se como uma abordagem jurídica tecnicamente inadequada e até mesmo omissa. Nesse sentido, Luciano Floridi et al (2015, p. 3) indica, especificamente, que a hiperconexão teria o efeito de causar indistinção entre a realidade física e a virtual, o que justificaria uma suplantação do dualismo inicialmente suposto.

Sob esse paradigma, compreende-se a possibilidade de a *Internet* comungar forças regulatórias distintas e não anulatórias, que são capazes de, concomitantemente, impor normas incidentes sobre esferas, situações e dimensões distintas. Sobre essa base, rompida com aquela de natureza dicotômica, torna-se possível conceber estruturas regulatórias na *Internet* que não aquelas oriundas dos poderes legitimamente constituídos, capazes de construir novas concepções da legalidade vigente sob a esfera digital. Adianta-se que a natureza fluida da *Internet* acarreta, por sua vez, dificuldade na compreensão dos fundamentos dos direitos dos utilizadores, considerando a concomitância de bases regulatórias incidentes sobre esse meio.

Torna-se necessário entender a fluência de um direito centrado na técnica industrial que, ao se sujeitar a uma mudança paradigmática para a pós-modernidade, tipicamente marcada pela técnica informacional, sofre com diversos entraves e dificuldades. A compreensão de formas regulatórias tecnicamente nativas à informacionalidade emergem da *Internet* e assumem importantes papéis dentro dos fluxos jurídicos da rede, rompendo em muito com a visão material e adquirindo uma noção imagética e superficial, à semelhança da visão flusseriana. Apesar disso, não se justifica segregar totalmente o direito incidente sobre o mundo dos *bits* daquele direito exercido sobre os átomos, considerando, portanto, adaptações, “refrações” e até mesmo reformulações das estruturas regulatórias anteriores, já sob o paradigma informacional.

Portanto, considera-se que a técnica informacional exerceu papel essencial sobre o direito, remodelando consideravelmente as relações ocorridas sob o âmbito das vias de informação. Toda essa realidade multifacetada, não dualógica e fluida que marca a incidência jurídica sobre a *Internet*, mostra-se essencial para compreender a fragilização dos direitos digitalmente manifestos/existentes e, mais que isso, primordial para visualizar como os criptoativos, *Blockchains* e tecnologias correlatas emergem já como regulações informacionais, nativas à rede e, portanto, adaptadas a uma realidade totalmente polar à realidade industrial que rege, primordialmente, o direito incidente sobre o mundo dos átomos.

CAPÍTULO 2 O AMBIENTE DA *INTERNET* E SUAS DINÂMICAS DE PODER

A seção que segue busca construir uma visão acerca do problema da *Internet*, haja vista que as suas bases filosóficas, valorativas e concepcionais foram lançadas. Há indicativo de que haveria uma suplantação da visão jurídica positivista, estritamente focada na atuação do Estado, em nome de uma realidade jurídica múltipla natural do meio virtual, compreendendo como há a manifestação do poder na *Internet*, as maneiras pelas quais há a violação de direitos na *Internet* e, dentro das vias ordinárias, como há a protetiva de direitos que são refletidos sobre a realidade virtual da *Internet*.

O ambiente da *Internet* figura como um emaranhado complexo de relações sujeitas a padrões distintos dos usuais do mundo físico, que, apesar da relativa marca isotópica em alguns aspectos dessa realidade, constitui um espaço marcado por novas manifestações de poder e, por consequência, novas manifestações de dinâmicas violadoras e garantidoras de direitos. A transição das modalidades técnicas, conforme apresentadas na seção anterior, foi capaz de remodelar o poder e sua manifestação conforme os ditames da informação, sujeitando-o às realidades fluidas, binárias e exatas que marcam esse ambiente intermediado pelos aparatos informáticos, de forma que todas as suas decorrências foram, conseqüentemente, também impactadas.

Poder, seguindo a lição clássica tomada da sociologia Weberiana (2009, p. 33), pode ser descrito como a capacidade de imposição de vontades sobre relações sociais, visão esta que é ampla e abrange diversas modalidades, como o poder político, econômico e cultural, constituindo um fenômeno presente dentro do ambiente digital, com diversas ramificações que conduzem a formas isotópicas e utópicas de exercício do poder. O poder, *lato sensu*, já vem sendo pensado como objeto de uma complexa reestruturação há certo tempo, com diversos autores apontando uma concepção pluralista e desconcentrada do exercício do poder, em especial o poder político.

Ralph Miliband (1982, p. 14), muito antes de vislumbrar o apogeu da técnica informacional sobre as sociedades, já previa uma descaracterização do poder por meio da desconstrução de um centro integrador das forças, capaz de abalizar normativamente as diversas instituições componentes do corpo social e impedir uma difusão conflitiva do poder. Robert Dahl (1988, p. 53) direciona a mesma difusão, considerando o poder político exercido primordialmente pelo Estado, apontando para uma dissolução do poder de fato perante o meio social e a sua aglomeração sob a tutela de atores dispersos do ambiente social.

O ambiente digital consegue inserir-se de forma adequada junto às realidades propostas pelos autores indicados, apresentando-se como ambiente potencialmente modificador, capaz de reordenar a lógica da manifestação do poder e seus limites. Apesar de sua origem junto à figura estatal, a *Internet* foi capaz de desestruturar as modalidades de exercício do poder político e regulatório, portanto, afetando concretamente a ordenação das forças nesse ambiente e causando reverberações sobre a seara dos direitos e sua protetiva. Manifesto por meio da capacidade de imposição deontológica amparada na coerção, o poder político não consegue transitar com fluidez para o ambiente virtual e exercer diretivas de controle naturalmente, dependendo de uma nova modalidade de poder para adquirir conotação vigente sobre o ambiente virtual.

Conforme indicado na secção anterior, o direito, enquanto ferramenta formal do exercício do poder, consegue promover influência sobre o ambiente digital por meio de algumas figuras intermediárias, situação essa que não é extensiva a toda seara virtual, dada a também referenciada realidade utópica da *Internet*. Ainda assim, o poder exercido amplamente sobre o mundo dos átomos demanda efetiva tradução e remodelagem dentro das diretivas técnicas do ambiente virtual, levando à ascensão do poder programacional³⁴ como ferramenta de viabilização das manifestações de poder.

Nesse sentido, Vittorio Frosini (1996, p. 85) apresenta o poder da *Internet* na reinterpretção dos comportamentos humanos e, conseqüentemente, o poder que os regula: “[...] as novas condições da vida artificial têm propiciado novos comportamentos, que tem originado novos modelos jurídicos, os quais, por sua vez, têm favorecido a aceitação ou difusão de novos comportamentos.”³⁵

Lawrence Lessig (1999) expressa muito bem tal situação ao definir o ciberespaço como um ambiente primordialmente regulado por ele mesmo, portanto, um ambiente em que o exercício do poder deriva de linguagens próprias e, apesar de aceitar certas situações de transição de poderes externos (o que chamamos de situações isotópicas de aplicação do direito, considerando ferramenta institucional de exercício do poder), ainda assim demanda uma

³⁴ Entende-se o poder programacional como o interstício essencial para a manifestação do poder no ambiente digital, cuja utilização é necessária para qualquer forma de imposição de interesses e padrões dentro de um meio virtualizado. Seja o exercício do poder nativo da rede ou o exercício de um poder advindo do mundo dos átomos.

³⁵ “[...] *las nuevas condiciones de vida artificial han propiciado nuevos comportamientos, que han originado nuevos modelos legislativos, los cuales, a su vez, han favorecido la aceptación o difusión de los nuevos comportamientos*” (tradução livre).

linguagem cognoscível e adequada àquela ambiência. Adaptando as palavras de Charles Clark³⁶ (1996, p. 139), as respostas para ambiente digital estão exatamente no ambiente digital.

Seja o Estado exercendo seu poder institucional, uma grande corporação, com extensiva capacidade econômica, ou mesmo um líder religioso, socialmente aclamado, a manifestação do poder, por meio das vias digitais, demandará a sua anterior conversão ao ambiente digital programado, de forma que os poderes antes vestidos de naturezas distintas (econômico, político, social e etc.) agora tomam forma, na *Internet*, através do poder programacional, a capacidade de compor algoritmos e estruturas digitais por meio dos quais se impõem vontades de forma unilateral.

Haveria uma série de novos agentes atuando no ambiente informacional, derivando seu poder de capacidade técnica ou mesmo de outras formas de poder, passando a atuar efetivamente no controle dos fluxos digitais (FLORIDI et al, 2015, p. 26).

A *Internet*, apesar de sua noção sobrenatural, em seu sentido Gassetiano, trata-se de uma simples rede de comunicação padronizada entre aparelhos eletrônicos, tendo todas suas “ambiências” construídas por meio da atuação de programadores, especialistas da tecnologia da informação, que são capazes de compor algoritmos para estruturar e funcionalizar seus aparatos. Assim como as leis da física regem o mundo dos átomos, os teclados dos programadores definem os limites do que é possível no ambiente virtual, de forma que toda essa realidade demanda uma atividade ativa de programação e ordenação de funcionamento. Toda e qualquer forma de ação digitalmente manifesta depende, inicialmente, de um ambiente programado para ocorrer, algoritmos de funcionalização da situação pretendida e, além disso, ausência de impedimentos algorítmicos.

Pensa-se, como exemplo, no exercício do poder jurídico-estatal para o empreendimento de uma restrição sobre ativos bancários de determinada pessoa, no qual, independentemente do respaldo formal (jurídico) e de fato (coercivo, com atinência ao ambiente físico) sobre a figura estatal, a restrição somente ocorrerá caso o sistema bancário tenha sido programado para aceitar situação e, além disso, caso haja um sistema, também programado, que empreenda tal restrição.

De fato, conforme definem Primavera de Filippi e Aaron Wright (2018, p. 194), trata-se da ascensão dos códigos enquanto objetos reguladores, indo além para afirmar que também podem ser concebidos como objetos de poder, linguagens pelas quais todas as manifestações de poder do mundo dos átomos precisam incorporar para conseguirem exercer suas vontades

³⁶ Charles Clark (1996, p. 139) prevê que o ambiente das máquinas é capaz de promover soluções para si mesmo, com respostas para suas questões advindas de sua própria realidade.

no ambiente da *Internet*. Concebe-se, portanto, uma realidade algocrática³⁷, com o poder advindo daqueles sujeitos com capacidade técnica para programar domínios e aplicações (ANEESH, 2002, p. 8), uma efetiva “epistocracia” (DANAHER, 2016, p. 15).

Sob um ponto de vista fático, se o poder nasce do cano de uma arma (TSÉ-TUNG, 1989, p. 17), necessariamente, o poder no ambiente virtual “nasce diretamente do teclado dos programadores” (RODRIGUES; MARCHETTO, 2021, p. 126), ocorrendo a sua cooptação por meio de outras forças dotadas de poder no mundo dos átomos, como o caso dos Estados e grandes corporações, que empregam o poder programacional em favor do seu já estabelecido poder empregado na seara física.

Tramontina e Cruz (2019, p. 164) compreendem os programadores como efetivas “mãos invisíveis do ciberespaço”, que possuem amparo direto na atuação dos Estados e do mercado para empreender suas formas de exercício do poder e, por consequência, regulação, ainda assim, sob vias que não são transparentes e suficientemente claras aos indivíduos sujeitos ao exercício do poder. Trata-se de uma manifestação isotópica da rede, no qual poderes do mundo físico migram para o ambiente digital e, apesar de empreenderem outras formas de veiculação de vontades, ainda integram as diretivas de ordenança.

Ainda que diversos autores, como Aneesh (2002, p. 7) e Gillespie (2018, p. 106) entendam o poder algocrático como um movimento fragmentador da autoridade institucional e do exercício do poder, aproximando da figura do poder difuso, como proposta por Dahl (1988, p. 53), há que se considerar seus poderes de cooptação, claramente manifestos por meio de instrumentos de poder do mundo físico, como o poder organizacional (Estado exercendo controle sobre indivíduos com capacidades de programação) e o poder econômico (contratação de programadores por conglomerados de tecnologia e agências estatais), aos moldes do que fora proposto por Hood e Margets (2007, p. 10-11).

Rodrigues e Marchetto (RODRIGUES; MARCHETTO, 2021, p. 128) definem o modelo algocrático como aquele que “por meio de uma atuação pautada na suavização dos métodos coercitivos oriundos de uma manifestação negativa, cria espaços macios que impedem a percepção do dominado acerca de sua condição de subjugado.”

A algocracia, enquanto uma manifestação do poder de controle no ambiente informacional, marca-se por uma manifestação negativa, portanto, que não transparece meios ativos de coerção, uma vez que se pauta no impedimento da possibilidade por meio da supressão das vias, e não no controle repressivo típico da realidade panóptica (MARX, 2002, p. 9-12).

³⁷ Poder advindo da regência dos algoritmos, enquanto construção originada das produções do sociólogo Aneesh (2009).

Ainda assim, é presente uma deslegitimação do exercício do poder, que deixa de encontrar-se majoritariamente regulado e pautado por instituições vinculadas constitucionalmente a deveres jurídicos e pode, simplesmente, ser exercido por quem quer que tenha capacidade técnica (DANAHER, 2016, p. 15). Há, portanto, a desestruturação da autoridade e das suas noções hierárquicas (ANEESH, 2002, p. 7), que, em um primeiro momento, indicaria a possibilidade de compartilhamento social do poder, no entanto, demonstra direcionamento contrário a tal utopia, com uma realidade pautada na cooptação das capacidades programacionais e no poder sobre os processos de tomada de decisão regidos por poucas pessoas (DANAHER, 2016, p. 7).

Nesse sentido, Byung-Chul-Han (2018, p. 26-27) compreende uma migração do Biopoder, poder de controle e decisão sobre a vida e morte dos indivíduos, para o poder programacional, manifestado na capacidade de administração e controle da realidade virtual. Portanto, compreende-se o poder programacional como uma capacidade efetiva de controle e imposição de padrões comportamentais, tendo o autor a visão de que o seu exercício está atrelado diretamente às práticas de vigilância dentro de uma sociedade digital centrada no controle (HAN, 2018, p. 24). Aproximando-se da visão distópica de Burrhus Frederic Skinner (2005, p. 275-276), trata-se de um poder que transcende o uso da força e torna-se capaz de controlar o “espírito humano” por meio de instrumentalizações do comportamento através de diretivas arquitetônicas.

O poder programacional, descrito como a capacidade de estruturar as arquiteturas da *Internet*, constitui efetivo poder regulatório sobre o ambiente virtual, impondo efetivas limitações ao nosso comportamento. Conforme expressa Lessig (2006, p. 125), o poder arquitetônico sobre a rede constitui efetivo comportamento de fazer outros comportamentos possíveis ou impossíveis, dessa forma, denotando a capacidade permissionária ou anulatória do poder no ambiente virtual. Se no ambiente físico há maiores restrições ao exercício do poder pelas vias arquitetônicas (usualmente exemplificado por barreiras, travas e redutores de mobilidade urbana), na *Internet*, esse poder adquire projeção elevada, dada sua natureza artificial e a automática execução das modalidades programadas (DE FILIPPI; WRIGHT, 2018, p. 204).

Nesse sentido, fala-se em um poder digitalmente exercido, marcado pela sua autoexecutoriedade, lastreado no exercício oligárquico das capacidades programacionais, que se mostra embebido em certos valores e inviabilizador de outros (LESSIG, 2006, p. 125). Nas palavras de Lessig (1999), a arquitetura do ciberespaço mostra-se tão importante quanto a

legislação, quando falamos em definir e frustrar liberdades na *Internet*³⁸, situação muito bem descrita por Primavera De Filippi e Aaron Wright (2018, p. 205) como “*vires in numeris*”, a força manifesta em números, referenciando a linguagem binária da programação, que reflete a fonte de poder da qual as demais forças dependem para se empoderar no ambiente virtual.

Ao se debruçar sobre a manifestação do poder no ambiente virtual, dada a realidade já adiantada anteriormente, há que se considerar uma efetiva reconstituição conceitual do que seria o poder e a sua manifestação no ambiente digital, haja vista a intensa distinção que tal ambiência causou sobre esse fenômeno. Opondo-se em parte ao que propõe Hannah Arendt (2001, p. 34) para o ambiente físico, o poder exercido sobre o ambiente informacional não é abalizado pelo consentimento em sua totalidade, tendo, por outro lado, o marcante traço da violência, de forma que a realidade digital tem diretivas de poder marcadas pelo exercício da coação algorítmica para a imposição de padrões, ainda que se fale em poderes institucionais legítima e democraticamente constituídos.

O poder programacional pauta-se, sobretudo, numa diminuta transparência aos olhos dos objetos do poder, que se veem sujeitos a dinâmicas de controle, sejam elas legítimas ou não, sem conseguir perceber, com clareza, a manifestação do poder. Lessig (1999) indica o poder programacional como um sistema pautado em modelos de codificação fechada, no qual os códigos regentes, enquanto *longa manus* das manifestações de poder, são ocultos da grande massa de regulados. Os códigos sujeitam os indivíduos, no ambiente digital, a padrões de conduta, regulando, efetivamente, sua vivência nesse âmbito, no entanto, geralmente não contam com indicativos de transparência, o que retira a capacidade de conhecimento dos regulados e, mais que isso, fulmina a ideia de consentimento em grande parte das dinâmicas de manifestação de poder na rede.

Portanto, no sentido que demonstra Aneesh (2002, p. 3), o emprego do poder programacional reveste-se de mecanismos opressivos de imposição (mesmo que impostos de forma negativa e sub-reptícia), fugindo da noção de consentimento e legitimidade que regem o poder hierárquico exercido no ambiente físico. Seja o acesso a um simples sítio digital ou mesmo medidas de violação da privacidade engendrados por governos dentro dos limites da alegabilidade, o poder exercido por esses meios possui em si diretivas forçosas, que independem

³⁸ Lessig (1999) descreve uma dualidade de forças impactando diretamente a liberdade, a privacidade, o livre acesso à informação, sendo, de um lado, os Códigos da Costa Leste (referenciando-se ao poder Estatal legítimo, com sua sede em Washington, na costa Leste dos Estados Unidos da América), e os Códigos da Costa Oeste (referenciando-se ao poder programacional, tendo suas origens no Vale do Silício, da Costa Oeste dos Estados Unidos da América).

do consentimento livremente estabelecido pelos utilizadores da rede (RODRIGUES; MARCHETTO, 2021, p. 126).

Vale ressaltar que Lessig (1999) entende que a transparência não é um elemento inerente ao poder, de forma que o exercício regulatório por parte do Estado, enquanto instituição legítima, também é marcado por traços ocultos, seja uma ocultação efetiva dos mecanismos legais ou mesmo uma ocultação epistemológica, que exige capacidades técnicas excepcionais para compreender sua manifestação e perceber sua performance. No entanto, a principal questão, por detrás do poder programacional, é a possibilidade do seu exercício por meio de códigos de natureza fechada, com seu funcionamento e base restritos a um número reduzido de indivíduos, enquanto seus efeitos se projetam além de grupos reduzidos, com indivíduos sujeitos aos seus efeitos, que não possuem capacidade material de conhecer seus termos ou seu funcionamento, diferindo-se bastante das formas de ocultação do poder institucional exercido sobre o ambiente físico.

Dessa forma, vê-se a primeira característica a afetar o poder, exercido por meio do ambiente digital, a derrocada ou degradação da legitimidade das manifestações de poder. Bonavides (2000, p. 146) indica que a legitimidade se mostra atrelada diretamente à teoria de poder reinante sobre o ambiente analisado, de forma que é possível afirmar, nos termos do que fora exposto, que o ambiente digital possui formas de manifestação de legitimidade que se diferem concretamente da manifestação da legitimidade no mundo físico. O poder é remodelado para se adequar às dinâmicas do mundo dos *bits*, situação essa que precisará ser efetivamente considerada na compreensão do fenômeno da legitimidade do poder programacional.

Maurice Duverger (1956, p. 39) compreende a legitimidade como uma noção relativa, em dependência direta com relação às crenças de determinado momento, condição essa que permite visualizar uma inadequação imediata dos modelos de legitimação ao ambiente digital. A legitimidade, simploriamente concebida sob o ponto de vista da legalidade³⁹, visão tão perpassada pelos teóricos positivistas, como Kelsen (2003, p. 103) e Carl Schmitt (2004, p. 9), não possui total apego ao ambiente digital, levando em conta uma série de fatores e a realidade fática que envolve o mundo virtual.

A legalidade no ambiente digital decorre da própria codificação, construção programacional das estruturas e protocolos que regem a vivência sob o ambiente virtual. Sob

³⁹ A legitimidade baseada na legalidade pauta-se na visão de que o exercício do poder é legítimo pelo simples fato de decorrer da lei, tendo como fundamento normas constituintes de poder, formalmente coerentes dentro de um ordenamento jurídico. Portanto, a legitimidade decorre de uma fundamentação hierarquicamente concebida das normas.

uma concepção utópica da rede, a desvinculação do mundo dos *bits* do mundo dos átomos rompe os laços entre a legalidade, de forma que o exercício de poder no ambiente digital não tem fundamento nas normas regentes do mundo físico, mas sim no próprio funcionamento daquela ambiência. Não importa o agente que queira exercer poder no ambiente virtual, tenha ele autoridade legal para exercê-la ou não, ele não possuirá o poder de fato (poder de programar) de forma imediata, e nem possuirá anteparos na própria estrutura da rede que garanta a sua legitimidade⁴⁰, situação que degrada a ideia de que a lei projete efeitos de legitimidade para o poder na *Internet*.

Mesmo sob um ponto de vista isotópico seria improvável justificar uma forma de legitimidade que diverge daquela regente sobre o ambiente físico, indicando padrões tão distintos e que, ainda que possua certos pontos de confusão, não advém da própria dinâmica da *Internet*. Casos em que há o exercício do poder legítimo do mundo físico sobre a *Internet* dependem de uma relação de poderes advinda do mundo dos átomos e direcionada, mediante conversão ou cooptação, para a forma de poder programacional, sem relação natural e sinérgica com a origem do poder no ambiente digital, o que dificulta o estabelecimento de uma linha clara entre a legalidade no mundo físico e a legitimidade no ambiente da *Internet*.

Determinada entidade, mesmo que tenha um arcabouço jurídico no mundo dos átomos justificando e fornecendo subsídios jurídicos para a sua legitimidade, não possui capacidade fática de exercer, singularmente, o poder e fazer com que a sua transmissão ocorra dentro dos moldes previstos pela legalidade. O ambiente digital, dessa forma, encontra-se em uma outra esfera de funcionamento, em que mesmo instituições que, ordinariamente, exercem poder sobre o mundo físico, de forma legítima, não conseguem reproduzir tal situação no mundo dos *bits*.

Semelhantemente, pensar a legitimidade sob a base de pensamento de autores modernos, como o caso de Maurice Hariou (1926, p. 198), Duverger (1956, p. 39-41) e Julien Lafférière (1947, p. 838), encontra certa dificuldade para adequar eficazmente a noção de legitimidade para as manifestações de poder no ambiente da *Internet*. Na visão dos referidos autores, a legitimidade encontra-se centrada na ordenação e disciplina do poder, de forma que, dentro de dinâmicas principiológicas pautadas na democracia, há a necessidade de procedimentos para a manifestação do poder e, acima de tudo, reger a sua transmissão.

Defrontando-se com o ambiente digital, com especial atenção aos códigos e programações como manifestações do poder, vê-se uma extensa liberdade nas formas de

⁴⁰ Há casos explícitos da dependência do Estado, instituição efetivamente possuidora de legitimidade e dotada de instrumentos legais de ordenação do poder, com relação a entidades privadas, dotadas de capacidades programacionais, efetivos detentores do poder de fato (PELL; SOGHOIAN, 2014, p. 23-26).

codificação e exercício do poder, com ausência de meios efetivos, até então, para impor limites e ordenar o exercício do poder. Nas palavras de Primavera De Filippi e Aaron Wright (2018, p. 194), trata-se dos códigos como normas supremas do ciberespaço, portanto, demarcando o poder programacional como uma estrutura que foge naturalmente de uma noção usual de legitimidade. Basta nos debruçarmos sobre a realidade da *Internet*, que é possível perceber a ausência de pressupostos limitadores do poder exercido por meio da rede, manifesto por meio da ilegalidade estatal (LAPRISSE, 2013) ou do abuso da vigilância de dados pelas empresas privadas do setor digital (SNOWDEN, 2019, p. 166).

O poder programacional, aqui abordado, refere-se ao exercício de uma manifestação de poder de controle e regulação social que opera através de codificações e aplicações informáticas, construindo estruturas incidentes sobre o comportamento humano na rede, com distinções marcantes quanto ao exercício do poder regulatório, do poder econômico e da soberania estatal. Há que se falar no poder programacional como um poder inerentemente instrumentário, opondo-se a uma realidade de coerção física, moral e econômica, operando por meio de modificações comportamentais, em uma dinâmica de governamentalidade (FOUCAULT, 2008, p. 143-144), o que permitiria, com a devida *vênias*, conceber tal poder como uma tecnologia de segurança, em seu sentido foucaultiano (LEMKE, 2017, p. 60).

Ainda sob o poder programacional, este não conta com uma realidade usual de transmissão e direcionamento democrático, mantendo-se centrado em práticas e agentes digitais específicos. Muito embora pensa-se na possibilidade de a programação ser difundida e permitir um empoderamento individual no ambiente da *Internet*, tal situação foge concretamente da realidade, na qual a capacidade técnica para programar é um conhecimento restrito (DANAHER, 2016, p. 15), que depende de estruturas de programação (*hardwares* e *softwares*) robustas para que seja possível fazer frente ao já estabelecido poder programacional cooptado pelo Estado e pelas corporações digitais.

A atual dinâmica globalizante e a ascensão de companhias digitais, as *bigtechs*⁴¹, acabou por projetar, ainda mais, mudanças nas dinâmicas de poder, emergindo, juntamente com a relevância do poder programacional, um contexto de migração do poder para essas companhias, que passaram a possuir tanto poder quanto o Estado (SHELTON, 2002, p. 273). Não bastasse isso, há que se falar no efeito de erosão causado pelo fluxo de informações sobre o Estado, apontando alguns autores, como Dinah Shelton, que tais dinâmicas enfraqueceram o Estado e,

⁴¹ Nome dado às maiores empresas do setor de tecnologias da informação

por consequência, abriu-se espaço para violações de direitos humanos (SHELTON, 2002, p. 278).

O enfraquecimento do Estado dentro das vias legítimas, por sua vez, reflete também na tentativa de ampliação dos seus poderes pelas vias tecnicamente adequadas, lançando mão de diversas medidas que impactam a garantia dos direitos dos utilizadores (LYON, 2001, p. 15-154). A expansão do Estado sobre as vias digitais representaria, também, um aumento das medidas de controle e a ampliação da sua capacidade lesiva aos indivíduos, com a tolerância dos Estados com relação às tecnologias de vigilância, fazendo uso delas ou cooptando agentes privados que possuem capacidade técnica para fazer. Cita-se, como exemplo, as exigências estatais feitas sobre as empresas de telefonia móvel referentes ao fornecimento de dados de geolocalização dos utilizadores de aparelhos de telefone celular (CLARKE; WIGAN, 2020), exigências feitas, muitas vezes, externamente às formalidades exigidas para a obtenção desses dados (BENNARDO, 2017, p. 2397).

De fato, a *Internet* permitiu um refluxo informacional e um maior acesso das massas ao conhecimento e direitos em geral (HAN, 2018, p. 37), no entanto, a manifestação do poder nesse ambiente, dentro dos moldes teóricos usuais, não possui regras balizadoras ou bases democráticas robustas para fazer frente às práticas lesivas empreendidas por essa via, dando indicativos de que a legitimidade se dilui frente ao poder de fato advindo da rede e suas dinâmicas⁴². Trata-se de um poder oculto, exercido às margens do conhecimento dos utilizadores da rede (ASSANGE, 2013, p. 43), o que, na visão de Foucault, foge do escopo esperado para o exercício do poder nos Estados democráticos (FOUCAULT, 1987, p. 211).

O enfraquecimento da legalidade e da legitimidade no ambiente digital aproximam-se, diretamente, das dinâmicas de supressão de direitos que se desenvolvem no ciberespaço, de forma que o exercício do poder programacional passa a ser usado na *Internet* para suprimir direitos, seja por meio de práticas ativas, que violam abertamente direitos, ou por meio de práticas negativas, manifestas em medidas arquitetônicas da rede que impedem o livre exercício de direitos (GILLEPSIE, 2018, p. 106).

Vale ressaltar que o ambiente da *Internet* não é totalmente ausente de estruturas que, legitimamente, exercem poder e se sujeitam a uma base principiológica capaz de direcionar sua atuação para as balizas democráticas. A liberdade programacional, que rege a rede, permite a

⁴² É importante citar a recente edição de normas relacionadas à regência do ambiente informacional, como o Marco Civil da Internet (2014) e a LGPD (2018). Ainda assim, há que se ressaltar que ambas, em especial a LGPD, possuíram uma dinâmica legislativa rápida e de poucas discussões, adotando-se modelos importados de outros ordenamentos e com mínima discussão pública.

instauração de ambientes que se sujeitam à referida dinâmica, no entanto, não compõe a da realidade virtual que cerca a maioria dos utilizadores da rede, que se vê envolvida de práticas de vigilância e controle exercidos por meio do poder programacional de Estados e empresas digitais.

Diante da questão, vê-se que o poder programacional possui fragilidades extensas com relação à sua legitimidade, marcando-se por sua natureza fática e, dessa forma, sem balizas estáveis de limitação. Se, nas palavras de Lessig (1999), somente os códigos conseguem reger com eficiência o ambiente digital, essas estruturas impõem um ambiente paralelo, marcado por diretivas alegais (LAPRISSE, 2013) e, em última instância, regido pelos meios de programação dos códigos da rede. A questão que merece ser analisada passa pelas características do poder programacional que rege o ambiente da *Internet*, para compreender como ocorrem violações de direitos humanos no ambiente digital, como decorrência da própria dinâmica do poder vigente. Portanto, em oposição às bases de legitimidade e sem medidas limitadoras do seu exercício, fala-se em uma realidade na qual as violações de direitos se proliferam diante das realidades marcantes do ambiente digital e sua manifestação de poder.

A questão é que, ao mesmo tempo que a *Internet* oferece benefícios para a proteção dos direitos humanos, permite-se também sérias intervenções por parte dos Estados e das companhias digitais, intervenções essas que alcançam uma escala nunca antes vista (PERRY; RODA, 2017, p. 2), lesionando direitos humanos e, por outro lado, permitindo também a sua tutela e efetivação.

Vale ressaltar que a própria natureza do ambiente digital, conforme apresentado anteriormente, favorece a dissipação do poder em diversas estruturas (que não são necessariamente legítimas), possibilitando que tal realidade seja marcada pela multiplicidade de manifestações de poder, que, por sua vez, impõem suas diretivas por meio de regulações distintas e, de forma geral, coexistentes. Nesse sentido, há que se falar na manifestação do poder sob a realidade programacional, enquanto poder atrelado às construções arquitetônicas do mundo dos *bits*, vinculado a padrões distintos de legitimação e, dessa forma, capazes de empreender práticas violatórias de direitos e, ao mesmo tempo, medidas de proteção e efetivação.

É importante notar que a *Internet* e suas dinâmicas de poder permitem uma dupla manifestação diante da abordagem dos direitos e sua tutela, na qual as características do ambiente virtual permitem a instauração de novas práticas protetivas de direitos e, ao mesmo tempo, instaurando novas modalidades de violação de direitos (TABORDA, 2017, p. 6). Em conexão com as bases do tecnicismo apresentadas anteriormente, dessa forma, há que se

visualizar a ambivalência da técnica projetada diretamente sobre a questão da tutela e efetivação de direitos no ambiente digital, indicando, dentro das bases ellulianas, uma neutralidade típica desse constructo. Não bastasse isso, adentrando na saga dual da técnica, surge a necessidade de tecnologias cada vez mais fortes e sofisticadas para fazer frente aos problemas criados pelas tecnologias anteriores. Demandam-se, portanto, tecnologias que consigam responder às dinâmicas decorrentes do poder programacional em sua faceta violatória de direitos, instaurando um ciclo com novas práticas lesivas, ainda mais alavancadas pelas novas realidades técnicas da arquitetura da rede.

Por fim, visando apontar pontos de discussão diante das questões e hipóteses levantadas anteriormente, há que se considerar a possibilidade do poder programacional ser dotado de elementos de legitimidade e, dessa forma, ser exercido de forma coerente e consentida por parcela robusta dos utilizadores da rede. Analisando os pontos que baseiam as principais problemáticas do poder programacional na rede, há que se considerar a legitimidade em uma dinâmica diametralmente oposta àquelas práticas tidas como violadoras de direitos no ambiente virtual, com especial ênfase às manifestações do poder que se revistam de meios para a garantia do conhecimento, proteção da privacidade, a autodeterminação digital e o direito de participação, em alguma medida, das codificações virtuais.

Sistemas dissipados e coletivamente controlados, como o caso das *Blockchains*, permitem que os referidos atributos de legitimidade estejam presentes nas manifestações de poder veiculadas por essa via, podendo citar, como outro exemplo, os *softwares* e programações baseadas no sistema *Open-Source*⁴³ ou *softwares* livres, no qual suas fontes de codificação são, respectivamente, abertas ao público e passíveis de reprodução (COLEMAN, 2009, p. 420) ou possível seu conhecimento, alteração e redistribuição (GNU, 2021). Dessa forma, surge a hipótese de que a legitimidade atrelada ao exercício do poder digital, legitimidade concebida sob seus termos estritamente vinculados ao ambiente da *Internet*, mostra-se diretamente alinhada à proteção e garantia de direitos no ambiente virtual.

Assim, a presente secção busca compreender como o poder programacional, enquanto manifestação do poder de fato no meio da *Internet*, realiza práticas de violação de direitos humanos e, em sentido oposto, permite a sua tutela e efetivação, tendo como suporte de análise as bases do poder programacional, suas manifestações ou não-manifestação de legitimidade, e o seu empreendimento por parte de Estados, empresas e organizações.

⁴³ *Open Source* ou código aberto refere-se a um *software* que tem seu código fonte (transcrição alfanumérica dos códigos de comando que guiarão determinado programa informático) livremente disponibilizado, portanto, passível de ser analisado, modificado ou distribuído, sem qualquer direito autoral ou limitação.

2.1 Dinâmicas violatórias e protetivas dos direitos na *internet*

Ocorrendo a compreensão da natureza do poder regente sobre o ambiente da *Internet*, vale adentrarmos, efetivamente, na questão dos direitos manifestados na *Internet* ou provenientes da vivência digital, sua violação dentro dessa mesma ambiência e, além disso, os mecanismos usualmente utilizados para responder e tutelar tais direitos no mundo dos *bits*. A realidade do poder empreendido altera-se concretamente, assumindo formas distintas, situação que transforma profundamente a maneira pela qual ocorrem as violações de direitos, que tomam forma agora de práticas realizadas através das estruturas arquitetônicas da virtualidade, seja por meio de atuações positivas, efetivamente praticando condutas que empreendem violações de direitos, ou seja através de arquiteturas e códigos de negatização, que impedem o exercício de direitos por meio de ambientes limitáveis pela programação.

Compreendida a alteração de paradigmas que ocorre com o adensamento da vivência humana no meio dos *bits*, há que se visualizar a fragilização das estruturas jurídicas usuais, com especial atenção àquelas destinadas para a proteção dos direitos humanos e sua tutela, que sofrem dificuldade de se manifestar no ambiente digital em razão da desconstrução do poder institucional, sua legitimidade e da dificuldade de execução da legislação vigente sobre o mundo dos *bit*.

A própria natureza do direito, vigente sobre o mundo dos átomos, impõe dificuldades diretas à tutela de direitos no ambiente virtual, mantendo a dogmática jurídica uma perspectiva centrada quase que exclusivamente em relações individualizadas e seus conflitos decorrentes (STRECK, 2011, p. 46), situação que gera dificuldade para o direito usual reger as demandas que emergem da vida digital, marcadas pela massificação em uma escala nunca antes vista.

Apesar da *Internet* ter sua origem atrelada a uma dinâmica ideológica, centrada na liberdade e na individualidade (CASTELLS, 2013, p. 43), a expansão dos fluxos informacionais, que ocorre no início da década de 2000, acaba por projetar uma massa de indivíduos ingressantes na vivência digital (SCHWAB, 2016, p. 20), conduzindo a uma realidade marcada pela massificação das relações e, por sua vez, que demanda medidas jurídicas adequadas. O contexto social, econômico e político se insere em uma dinâmica de massificação que adensa quantitativamente as relações humanas, refletindo diretamente no âmbito do direito, que passa a confrontar, diariamente, um número expressivo de situações que demandam sua atuação.

Ainda que o Estado e as demais instituições tenham iniciado uma reformulação de sua realidade para se adequarem a uma dinâmica massiva (SCHWAB, 2016, p. 15), vê-se que o

direito estatal mantém forte carga individualista, atrelada à primeira onda de constitucionalismo, que inseriu na estrutura dos ordenamentos jurídicos uma base liberal (SCHMITT, 1972, p. 33-37), situação que por si já dá indicativos dos embaraços, ou mesmo da incapacidade, das vias jurídicas usuais responderem eficientemente às violações de direitos que ocorrem nos ambientes virtuais. Trata-se, portanto, de uma crise do direito e do Estado que acaba por se projetar na pós-modernidade sobre os direitos humanos (SANTOS, 1989, p. 7).

Um dos pontos a ser destacado é a dificuldade ou mesmo incapacidade, dada a natureza individualista das bases dos ordenamentos jurídicos, dos mecanismos de tutela de direitos humanos serem capazes de produzir efeitos concretos sobre a dinâmica da *Internet*, regida pela massificação das relações e, por sua vez, por uma própria massificação das violações de direitos (OLIVEIRA et al, 2017, p. 561). Conforme indica Taborda (2017, p. 8), com o surgimento da *Internet*, há o destaque da necessidade de remodelagem das normas de proteção dos direitos humanos, dada a alteração robusta que afeta essa nova realidade e sua dinâmica particular com a sua tutela e efetivação.

Não bastasse a dinâmica individualista já marcante no ordenamento jurídico, há que se considerar a ampliação de uma ética individualista, promovida em razão da modernidade (SANTOS, 1989, p. 6), que impede a sociedade de compreender uma realidade social ou mesmo global, situação que se projeta, também, sobre a realidade jurídica.

Nos termos indicados anteriormente, há que se vislumbrar a relativa ineficácia executiva das normas jurídicas oriundas do mundo dos átomos sobre o mundo dos *bits*, fruto de uma divergência técnica capaz de desnaturar sua eficácia sobre as situações reguladas (ROHRMANN, 2005, p. 40-48). Considerando uma linha utópica moderada, há que se vislumbrar os impactos robustos da transição técnica sobre o Estado, seu direito e sua capacidade de tutela e efetivação de direitos humanos nesses novos ambientes.

A alteração na natureza do poder incidente sobre o ambiente digital acaba por impedir, concretamente, a eficácia dos mecanismos jurídicos positivados no ordenamento para a tutela e efetivação dos direitos humanos manifestos na *Internet*, considerando-se a total falta de entrosamento entre a dogmática tradicional e as visões regulatórias pautadas na arquitetura e codificação (LESSIG, 2006, p. 22). Dessa forma, a dogmática jurídica em geral, com especial atenção àquela voltada à tutela e efetivação dos direitos fundamentais, não conta com mecanismos mínimos de tradução do seu poder regulatório e executivo para a sua conversão ao ambiente digital, significando o que Ronaldo Lemos chama de ruptura da dogmática jurídica por meio da revolução tecnológica (LEMOS, 2005, p. 8).

Dada a natureza ambivalente da técnica, há que se compreender o impacto efetivo dessas novas tecnologias sobre a realidade dos direitos humanos, considerando a chamada contaminação das liberdades, fenômeno descrito por Antonio Enrique Perez Luño (2014, p. 28). Na visão do autor, o uso das novas tecnologias foi capaz de erodir consideravelmente os direitos fundamentais. Conforme expõe Barrientos-Parra (2011, p. 66), a defesa das liberdades e dos direitos fundamentais estaria constantemente ameaçada por um chamado “Leviatã tecnológico”, um reflexo claro da técnica que produziria efeitos ambivalentes sobre os indivíduos.

Por outro lado, alguns autores compreendem que as tecnologias digitais trouxeram mais visibilidade aos direitos humanos, de forma que, antes da ampliação dos canais de comunicação, havia mais casos de violação e menos respostas concretas por parte do Estado e da Sociedade (FROSINI, 1996, p. 85).

Há que se considerar a *Internet* como um ambiente de luta constante, no qual há uma intensa discussão, um embate acerca da autonomia e da democracia enquanto manifestações de uma sociedade (CASTELLS, 2003, p. 168). Assim como a sociedade, o papel da *Internet* como palco para os embates de poder que marcam a história jurídica da humanidade. Ao mesmo tempo em que a *Internet* encerra um elevado potencial para expressão dos direitos dos cidadãos e a comunicação de valores humanos, é relevante o seu potencial de nivelação de novas práticas de controle, dominação e vigilância. A *Internet*, enquanto uma ágora pública, servirá como espaço para a luta constante, que gerará o expoente da liberdade humana, de forma que o controle político sobre esse ambiente se torna uma situação propícia para os agentes de poder.

Outro ponto que merece ser destacado é a própria realidade histórica dos direitos humanos, de forma que uma alteração técnica, tão robusta como aquela experienciada com a ascensão da Era da Informação, acaba por projetar efeitos marcantes sobre a dignidade humana e sua tutela, que deixa de ser amplamente recepcionada pelos direitos fundamentais e seus mecanismos de tutela. Há que se falar na reconstrução de direitos humanos sob a égide da técnica informacional e, além disso, ascensão de novos direitos, ambos tendo como base as novas dinâmicas sobre as quais se pautam as relações digitais entre os seres humanos.

Tomando como exemplo, o direito à privacidade, antes atinente ao âmbito interno dos indivíduos, protegendo seus lares e intimidade, toma agora uma noção que exaspera o próprio indivíduo e as fronteiras territoriais que o cercam, assumindo projeção para um conjunto de decorrências digitais da privacidade humana, os chamados dados pessoais⁴⁴. Os moldes usuais

⁴⁴ Nos termos do artigo 5º, I da LGPD, trata-se de “informação relacionada a pessoa natural identificada ou identificável”.

do direito de privacidade não possuem aderência justaposta à noção de privacidade que emerge da realidade técnica da *Internet*, situação que desencadeia ausência protetiva, violações coletivas de direitos e, por consequência, a luta pela afirmação de direitos sob essa nova roupagem. Não se fala somente em novos direitos ascendendo do meio digital, mas, também, remodelagens desses padrões de dignidade já estabelecidos à realidade técnica da era da informação, considerando que os direitos humanos são, sob uma visão orteguiana, manifestações técnicas, portanto, que projetam o ser humano além da naturalidade (ARENT, 2005).

Há que se considerar a adequação dos direitos humanos aos padrões regentes da realidade socioeconômica, de forma que os padrões de dignidade humana e os instrumentos de efetivação seguem, *pari passu*, os caminhos da técnica. Não há conveniência ou adequação alguma à realidade falar em proteção à privacidade por meio de instrumentos jurídicos de tutela do segredo epistolar, por exemplo, situação que denota bem como os direitos humanos assumem novas conotações, mas mantendo seu espírito, assim, como passam a demandar novas modalidades de tutela e efetivação. Da mesma forma, a compreensão do que é digno ao ser humano, dentro da era da informação, possui novas acepções que merecem ser discutidas.

José Alcebíades de Oliveira Júnior (2000, p. 86) compreende os direitos humanos de quinta geração como aqueles vinculados às tecnologias informacionais, tendo como fundamento a própria realidade virtual de vivência sobre a qual os seres humanos passam a projetar sua existência. O autor chama atenção à relação entre os direitos decorrentes da realidade digital que se forma e o seu próprio papel na ruptura das noções territoriais que lastreiam o poder estatal, dando indicativos do poder de alteração dessa nova realidade digital e da própria perda de apego executivo por parte das dinâmicas de poder pautadas no direito regente sobre o mundo dos átomos.

Nesse mesmo sentido, Land (2009, p. 20) entende que a realidade digital acabou por suprimir grande parte das capacidades do direito estatal de tutelar os direitos humanos, de forma que há uma afetação direta a uma variedade de direitos humanos, cujas protetivas usuais não conseguem empreender uma tutela efetiva e capaz de evitar lesões, dando indícios de uma fragilidade ainda mais robusta dos mecanismos de tutela usual dentro da realidade virtual da *Internet*. Mesmo com obrigações claras e expressas dos Estados tutelarem direitos nesse ambiente, por meio de normas e políticas públicas (RONA; AARONS, 2016, p. 18), manifestando um efetivo dever de proteção dos indivíduos de violações emanadas do ciberespaço, há que se falar na fragilidade dos instrumentos isotópicos aplicados pelo Estado,

sejam ela inerente à realidade da legislação, seja ela originada da dificultosa tradução dessas normas ao ambiente digital, que possui dinâmicas de poder divergentes.

Partindo de um utopismo jurídico acerca do ambiente da *Internet*, concebe-se a necessidade da instituição de mecanismos viáveis para a tutela e efetivação de direitos no ambiente da *Internet*, portanto, demarcando o meio digital como passível de, seja por suas próprias vias ou por interferências do mundo físico, estruturar formas de violação de direitos humanos. Por sua vez, indicando um consenso, vê-se que um pensamento isotópico dá indicativos da necessidade de meios de proteção de direitos também no ambiente digital, reconhecendo o mundo virtual enquanto uma reprodução do mundo físico, constituindo um meio pelo qual ocorre a “propagação de conteúdos e discursos” (GOULART, 2012, p. 153). Nesse sentido, vê-se o consenso de ambas as escolas jurídicas da *Internet* acerca da necessidade da tutela de direitos no ambiente digital, dada as violações que podem ocorrer nessa via, restando controversos alguns outros pontos.

Concebendo a *Internet* como um ambiente utópico, haveria que se falar na manifestação de direitos como decorrência direta do ambiente relacional humano e, portanto, direitos que ascendem sobre aquela realidade, fruto das relações e vivências ali ocorridas. Os direitos nascem, mesmo que já intermediados por ordenamentos jurídicos vigentes sobre a realidade física, como um objeto de construção coletiva no ambiente da *Internet*, decorrendo da experiência específica do mundo dos *bits*. Fala-se, assim, na presença de uma natureza humana universal (PANNIKAR, 2004, p. 223), que se encontra também presente no ambiente virtual da *Internet* e, portanto, ensejando a ascensão dessas demandas à esfera do direito, sob o espectro da dignidade humana.

A situação mostra-se diametralmente oposta à visão isotópica, que parte da ascensão de direitos no ambiente físico, de forma que qualquer projeção de direitos sobre a seara da *Internet* consistiria em mera manifestação de um direito, e não um direito em si nascente daquela realidade e daquelas demandas. Nesse sentido, sob a óptica isotópica, se algum direito tivesse projeção sobre o ambiente digital, tratar-se-ia de mera produção de efeitos de direitos advindos do mundo dos átomos.

Havendo a ascensão de novas demandas coletivas, por direitos que caracterizam uma onda uníssona de proteção de determinada fração da dignidade humana, uma efetiva nova geração de luta por direitos humanos, há que se considerar a reestruturação de direitos já declarados e previstos pelos ordenamentos. As novas realidades, com padrões de dignidade humana que se distinguem daquelas vigentes em outros períodos, exigem que os direitos sejam

efetivamente adequados àqueles novos padrões, capazes de se comunicar, diretamente, com aquela nova realidade e, portanto, indicar um dinamismo construtivo.

Nesse sentido, partindo de uma base utópica, que será utilizada para a construção das hipóteses, há que se conceber os direitos como digitalmente existentes no ambiente dos *bits*, e não simples manifestações dos direitos existentes no mundo dos átomos. Trata-se de uma realidade com efetivas divergências técnicas e, portanto, com paradigmas socioeconômicos e culturais divergentes, capazes de ressignificar a dignidade humana, ensejando que as demandas coletivas e individuais dali oriundas tenham uma efetiva noção de direitos que, apesar de possuírem similaridade com aquelas advindas do ambiente dos átomos, refletem outras lutas.

Assim como as ondas de direitos humanos demarcaram a ascensão de novas demandas fruto de realidade distintas, há que se reconhecer a emergência de direitos digitalmente existentes, enquanto direitos humanos que ascenderam de uma realidade virtual que, apesar de não ser física, denota uma efetiva realidade de vivência.

A disciplina dos direitos humanos no ambiente digital mostra-se como uma questão pouco abordada, tanto no âmbito interno quanto externo, com escassas discussões a respeito e ainda menos medidas efetivamente focadas na garantia e efetivação dessas demandas emergentes da realidade informacional. Uma das poucas medidas existentes marca-se pela sua natureza isotópica, qual seja, a Resolução para Promoção, Proteção e Gozo dos Direitos Humanos na *Internet* (*Human Rights Council Resolution on Human Rights on the internet-A/HRC/20/L.13*), de iniciativa do Conselho de Direitos Humanos da Assembleia Geral da ONU, aprovada no ano de 2012 (ONU, 2012).

A Resolução referenciada abordou, sob uma óptica isotópica, a questão do exercício dos direitos humanos no ambiente virtual, compreendendo a necessidade das diretivas internacionais de proteção dos Direitos Humanos incidirem sobre esse ambiente. Dessa forma, tratou-se de uma medida voltada à tutela dos direitos humanos de forma similar àquela existente no ambiente físico, portanto, reconhecendo que os direitos manifestos, no mundo *off-line*, seriam semelhantes àqueles a serem reconhecidos no mundo *online*.

Apesar da relevância de tal Resolução para o reconhecimento dos direitos do ambiente digital, o isotopismo exacerbado do seu conteúdo representa risco de que a proteção dos direitos humanos, carreada pela normativa, possua natureza artificial, sem compreender as reais demandas coletivas e individuais emergentes da vivência digital. Ashley Deeks (2015, p. 299-300) critica o isotopismo exacerbado de tal medida, ao sugerir que a atual dinâmica digital não comporta mais medidas regulatórias pautadas em analogias do mundo físico, indicando que as normativas internacionais, incluindo a Resolução para Promoção, Proteção e Gozo dos Direitos

Humanos na *Internet*, não contam com meios suficientes para regular, eficientemente, o ambiente digital e as relações ali estabelecidas.

O dirigismo das medidas normativas advindas das figuras estatais ou mesmo de entidades internacionais, em choque com a natural construção das demandas de dignidade humana, mostra-se como uma desconsideração dos âmbitos coletivos e individuais de construção de direitos, afastando, concretamente, a noção dos Direitos Humanos das lutas que os envolvem (SÁNCHEZ-RUBIO, 2014, p. 106).

A concepção dos direitos humanos confinada ao direito estatal acabou por impor certas limitações à sua proteção e efetividade, impedindo a convivência com outros direitos cuja construção está relacionada a entes não estatais (SANTOS, 1989, p. 8). Nesse sentido, indica Boaventura de Souza Santos (1989, p. 8):

Por outras palavras, o titular de direitos humanos acabou sendo mais um cidadão no espaço público do que no espaço familiar ou no espaço de produção apesar de passar nestes a maior parte da sua vida. Ora, hoje torna-se claro que a expansão da cidadania e o aprofundamento da democracia tem que envolver esses espaços e para isso é necessário concebê-los como espaços de intersecção política, a qual, apesar de diferente, não é menos política do que a que tem lugar no espaço público, centrada no Estado.

Nesse sentido, há o entendimento de que os direitos humanos estatais, frutos de dinâmicas sociopolíticas, são aqueles relevantes, descartando a importância daquelas outras demandas de dignidade que emergem de contextos específicos. Haveria, portanto, uma proteção dos direitos humanos especificamente centrada no direito estatal e nos espaços públicos de convivência sociopolítica, deixando de compreender, sistematizar e incluir nas protetivas normativas todas aquelas exigências coletivas ou individuais que emergem de certas condições.

Deixar de conceber o titular de direitos humanos no espaço público de convivência digital, a *Internet*, tratar-se-ia de um isolamento dos direitos ali emergentes. Há a necessidade de compreender as demandas que advêm especificamente desse âmbito e dar-lhes a sua devida importância, ainda mais considerando a vivência humana no mundo virtual, que abrange quase a totalidade das interações humanas. A abordagem genérica e a abstração presentes nas normativas estatais acabam por limitar a eficiência dos direitos humanos normatizados em contextos divergentes (SANTOS, 1989, p. 8), o que reflete no baixo apego de cognição, aplicação legal e executividade das normativas sobre o ambiente digital.

A noção dos Direitos Humanos da *Internet* como frutos das próprias lutas da rede mostra-se como uma visão utópica, não necessariamente fundamentalista, que indica, no caminho do que afirma Sanchez Rubio (2014, p. 133), a capacidade dos indivíduos e das

coletividades reconhecerem a sua forma de dignidade, sem mostrarem-se passivas e pacientes com relação aos Direitos Humanos positivados. Assim, reconhecendo as próprias fragilidades dos Direitos Humanos sobre o ambiente digital, conforme já apresentado, depender da tutela protetiva do mundo dos átomos sobre a *Internet* dá indicativos de falibilidades e de extensivas lesões afetando a dignidade dos utilizadores da rede e das medidas pouco eficientes que podem ocorrer somente em uma dinâmica pós-violatória.

A marcante discrepância entre os Direitos Humanos promulgados e aqueles efetivamente aplicados (SANTOS, 1989, p. 10) traz um peso maior para a discussão isotópica dos direitos humanos, considerando, ainda mais, a natureza fluida e de difícil aceção da *Internet* pelas instâncias institucionais do mundo físico. Os principais ordenamentos jurídicos destinados à tutela dos direitos humanos, seja no âmbito interno, como o caso da Constituição Federal de 1988, ou mesmo no âmbito internacional, como a Declaração Universal dos Direitos Humanos e a Convenção Americana de Direitos Humanos, nasceram muito antes da efetivação da era da informação, o que pode sugerir certa fragilidade na tratativa da dignidade humana decorrente da realidade digital (PERRY; RODA; 2014, p. 66). Há, portanto, uma realidade totalmente diferente daquela enfrentada na época de construção dos ordenamentos, com violações e efetivações de direitos humanos muito distintas (HERRERA-FLORES, 2002, p. 9).

Não somente isso, os direitos humanos são constantemente infringidos no ambiente físico e digital, sendo possível pontuar que um vasto número dessas lesões ocorre em decorrência de mecanismos de execução (*enforcement*) relativamente fracos, com especial atenção aos mecanismos internos e externos de controle e as disparidades decisórias dos tribunais (PERRY; RODA; 2017, p. 7).

Há que se considerar as limitações estruturais e técnicas do direito estatal em tutelar os direitos humanos no ambiente digital, especialmente considerando as novas dinâmicas de poder e a amplitude do ambiente digital. O ciberespaço mostra-se como uma realidade não limitada por fronteiras estatais (DASKAL, 2015, p. 365-366), no qual há a convivência dos utilizadores em uma realidade que não conta com limitações territoriais e culturais, salvo raríssimas exceções de ambientes digitais enclausurados (o caso chinês). Ao confrontar essa realidade ampla, com a convivência de múltiplos sujeitos, em um ambiente sem vinculação específica a qualquer ordenamento jurídico, o direito estatal mostra-se falho e incapaz de reagir adequadamente.

Nesse sentido, sendo o ambiente digital uma realidade utópica, que foge das fronteiras do mundo físico, o direito estatal de proteger e efetivar direitos humanos dos indivíduos sob sua jurisdição mostra-se incapaz de atuar ou, ao menos, com dificuldades robustas para

promoção de medidas (RONA; AARONS, 2016, p. 5). Sugerem os autores que, diante de uma remodelagem da dinâmica de poderes e a alteração da realidade do exercício da soberania, torna-se necessário impor medidas de tutela dos direitos humanos não mais ligadas aos simples limites territoriais, buscando aplicar a jurisdição de determinado Estado diante de ofensas à dignidade humana por ele promovidas (RONA; AARONS, 2016, p. 8). Portanto, indicam que a tutela de direitos humanos deveria seguir o rastro das ofensas, impondo aplicação dos direitos em questão a todas as ofensas por ele praticadas.

Tal entendimento foi muito bem lastreado em uma decisão do Comitê de Direitos Humanos da ONU (ONU, 2014), que entendeu pela aplicação extraterritorial das normas de proteção de direitos humanos a todas ofensas à dignidade humana promovidas com relação à vigilância digital empreendida pelos Estados Unidos da América (casos denunciados por Edward Snowden, de práticas de vigilância digital empreendidas pela NSA⁴⁵). O referido eixo de pensamento advém diretamente de medidas de tutela de direitos humanos impostas internacionalmente aos Estados, no qual a sujeição de qualquer pessoa ao poder de determinada entidade estatal obriga a garantia dos seus direitos humanos por aquele que exerce o poder, esteja o indivíduo diretamente ou não sob a sua jurisdição.

Enquanto uma diretiva oriunda das normativas de tutela de direitos humanos em conflitos armados e ocupações militares, o exercício do poder sobre os indivíduos é a atividade que vincula o ente estatal ao dever de tutela de direitos, de forma que, ao conceber a realidade virtual que nos cerca e a remodelagem da manifestação do poder, tornou-se possível aproximar tal diretiva para aplicá-la diretamente sobre o ambiente virtual. Semelhantemente, há que se falar em ambientes da *Internet* nos quais há o exercício de poder programacional por parte dos Estados, o que ensejaria a incidência das medidas de tutela de direitos humanos previstas no ordenamento desses países interventores.

Vale citar que o Alto Comissariado da ONU para Direitos Humanos (ONU, 2018) sugeriu a aplicação das normas de direitos humanos sobre quaisquer situações e ambientes sobre os quais exercita o Estado seu poder e o efetivo controle sobre as comunicações digitais e as infraestruturas da rede. Trata-se, portanto, do reconhecimento do exercício do poder na *Internet* como uma faceta da realidade estatal e, assim, exigindo respostas normativas capazes de tutelar os direitos que se encontram afetados pelo exercício de poder e controle.

Trata-se de resposta isotópica para promover a aplicação das normativas internacionais e internas de proteção dos direitos humanos às relações desenvolvidas no ambiente da *Internet*,

⁴⁵ Agência de Segurança Nacional. Trata-se de órgão de inteligência estadunidense.

aplicando analogias, especificamente o exercício do poder e controle, como mecanismos para permitir a incidência de tais normas a uma realidade que dá indícios de expressa divergência do mundo físico. A fundamentação mostra-se coerente e adequada, uma vez que dá respostas isotópicas e pouco atípicas à garantia e tutela dos direitos humanos no ambiente digital, ainda que possuam alguns pontos que ressaltamos que devam ser analisados.

Sob o ponto de vista da aplicação dos direitos humanos estritamente em razão do exercício de poder e controle sobre indivíduos, mostra-se necessário ampliar tal discussão para o âmbito dos agentes privados, que se mostram como agentes dotados de elevado poder na *Internet* e reiterados agentes violadores de direitos humanos.

Os agentes privados, especialmente aqueles que possuem sua atuação voltada à tecnologia da informação, mostram-se como entes poderosos no ambiente digital, possuindo parcela relevante das violações de direitos ocorridas no ambiente da *Internet*. Ainda mais, tratam-se de violações de direitos humanos que não foram, até então, contempladas expressamente nos movimentos atuais de desenvolvimento dos direitos humanos (SHELTON, 2002, p. 279). As normas de direitos humanos centram-se na proteção dos indivíduos face ao Estado, e não na regulação da conduta de agentes privados dotados de poder no ambiente digital, que efetivamente ocupam parte do espaço antes ocupado pelo Estado.

Apesar da ênfase na figura estatal, há que se reconhecer que há quantidade relevante de violações que são empreendidas por agentes privados, citando, como exemplo, as formas de trabalho análogos à escravidão, o que sugere a necessidade de tais protetivas incidirem sobre agentes privados. Para tanto, alguns autores entendem que os instrumentos de proteção de direitos humanos, por possuírem aplicação indireta sobre os entes privados cometedores de violações, também obrigam agentes não estatais (SHELTON, 2002, p. 283), tendo tal fundamento base no preâmbulo da Declaração Universal dos Direitos Humanos, que indica o dever de todos indivíduos e coletividades respeitarem e promoverem direitos humanos.

No sentido da aplicação horizontal dos direitos humanos e a atuação democrática de todos os indivíduos e coletividades na sua garantia e efetivação, há que se falar na possibilidade de incidência dos direitos humanos de determinado ordenamento jurídico em razão de agentes privados, especificamente conglomerados empresariais atuantes nos ramos digitais, promoverem o exercício de poder e controle sobre indivíduos no ambiente digital.

Vale indicar o Guia da OCDE para Empresas Multinacionais (2011, p. 31), que prevê, claramente, o dever de as instituições privadas respeitarem direitos humanos, a elas sendo imposto o dever não só de não infringir, mas de evitar e mitigar efeitos adversos de suas práticas, evitar e mitigar contribuir com atividades que causem impactos sobre a dignidade humana. O

respeito aos direitos humanos é indicado como um ponto necessário dentre as políticas internas das empresas multinacionais sujeitas às regulações da OCDE, devendo constituírem um compromisso formal com a sua proteção. Documentos como o indicado acabam por trazer as corporações para os paradigmas de proteção internacional dos Direitos Humanos, sujeitas aos regimentos internacionais aplicáveis aos locais de sua operação.

É importante considerar que, apesar de não possuir um caráter vinculante à totalidade das empresas, tal prática indica uma diretiva internacional de adoção de padrões de governança corporativa relativa aos direitos humanos, difundida por meio de uma relevante organização internacional.

Há que se considerar a relativa fragilidade das medidas protetivas de direitos humanos oriundas do meio físico, sejam elas originadas da tutela interna ou internacional. Rona e Aarons (2016, p. 17) entendem que as medidas estatais de tutela dos direitos humanos no ambiente digital devem se pautar não somente pela garantia, mas, principalmente, pela efetivação, especialmente considerando a baixa eficácia na condução de medidas positivas voltadas à proteção dos direitos.

Se há espaços sociais cuja realidade vigente cria embaraços à garantia e efetivação dos direitos humanos (SÁNCHEZ-RÚBIO, 2017, p. 27-28), pode-se sugerir que a *Internet* seria um deles, dada sua realidade tecnicamente distinta e a fragilidade inerente para carrear medidas executivas do ambiente físico para o digital. Ao mesmo tempo em que o ambiente digital permitiu uma expansão da capacidade comunicativa, ampliando o conhecimento de violações de direitos humanos, há que se reconhecer o aumento dos poderes disponibilizados pelas tecnologias digitais aos Estados e corporações (PERRY; RODA; 2017, p. 7), ampliando, extensivamente, a capacidade lesiva à dignidade humana.

Haveria, para os seres humanos, na internet, um risco crescente de controle das esferas digitais por corporações, estabelecendo mecanismos de controle e vigilância de difícil escapatória ou repúdio (FLORIDI, 2015, p. 12).

Perry e Roda (2017, p. 2) afirmam que os seres humanos se encontram como caminantes sobre cordas, necessitando, constantemente, equilibrar-se entre a expansão das protetivas de direitos humanos e o surgimento de novas tecnologias informacionais. Portanto, apesar de vários impactos positivos causados pelas novas tecnologias sobre os direitos humanos, como a liberdade de expressão, há que se considerar, também, a grande quantidade de efeitos maléficos por elas trazidos, asseverando a natureza ambivalente da técnica, em seu sentido elluliano.

Por sua vez, sob uma óptica utópica, cumpre levantar a hipótese da reconstrução ou ampliação digital dos mecanismos de garantia dos direitos humanos, demarcando a natureza coletiva da *Internet* e a fragilidade de uma dinâmica puramente isotópica, que meramente importe do mundo físico padrões de dignidade impostos pelo ente Estatal. Torna-se necessário não somente efetivar e garantir direitos no ambiente digital, de forma que é preciso que a própria *Internet* funcione e evolua para defender direitos humanos, de forma nativa e inerente à sua própria realidade (INTERNET GOVERNANCE FORUM, 2015, p. 7). Nesse sentido, sugerem os autores que a *Internet*, sob uma visão horizontal e ampla, deveria estruturar-se com uma governança centrada na tutela e efetivação de direitos, capaz de suprimir as falhas de efetivação existentes na importação isotópica das protetivas da dignidade humana.

Discute-se na temática a relevância jurídica dos direitos que preexistem à era da informação e são incorporados à vivência digital, uma vez que, conforme indicado, há um conjunto de fatores que definem a vivência digital como algo não inerentemente idêntico à vivência física, em especial considerando a realidade de manifestação de poderes e suas externalizações jurídicas. Há que se considerar que há especificidades do ambiente digital que atuam diretamente sobre tensões já existentes, exacerbando-as e instaurando uma realidade de afetações ainda mais marcantes aos Direitos Humanos (RONA; AURONS, 2016, p. 1). A privacidade, exemplo marcante dentro de uma realidade socioeconômica centrada em dados, sofre extensa projeção das suas lesões, que assumem conotações massificadas e constantes (MAARTÍNEZ-BEJAR; BRÄNDLE, 2018, p. 142).

Nesse sentido, entendem Rona e Aurons (2016, p.1) que há a necessidade de uma readaptação das normas de direitos humanos como forma de garantir que essas novas circunstâncias possam ser tuteladas e tenham balizas de dignidade humana garantidas. Ashley Deeks (2015, p. 299-300), sob uma visão utópica, compreende que as atuais circunstâncias da vida digital alcançaram tamanha imersão e projeção, que adaptações e analogias do mundo físico não se mostram mais úteis e eficazes para regular a vivência ali estabelecida.

É necessário compreender a dignidade humana de forma flexível, compatível com as novidades trazidas pela realidade técnica, no entanto, sem significar limitações ou retrocessos às protetivas. Há bases intrínsecas que formam a dignidade humana, no entanto, esta tem parte de suas bases em padrões e valores socialmente vigentes, que definem o que é digno segundo os conceitos de determinada cultura, povo e realidade temporal. Os direitos humanos, dessa forma, devem sempre acompanhar, numa progressão construtiva e não reducionista (RAMOS, 2014, p. 88), a evolução técnica e social que nos cerca, para que a pessoa humana esteja sempre protegida, mesmo defronte à realidade tecnológica.

Um excelente exemplo dessa prática vem da jurisprudência da Suprema Corte Estadunidense, especificamente com relação ao caso paradigma *Kyllo v. United States* (EUA, 2001, p. 35). O caso versa sobre a utilização de tecnologias de rastreamento para finalidades penais, especialmente analisando a relação entre os novos dispositivos de vigilância e a proteção da privacidade doméstica. O ponto central da decisão, o voto unânime da Corte, partiu da necessidade de adequação das protetivas constitucionais de direitos humanos, no caso, o direito à privacidade, à realidade técnica vigente, como forma de evitar que sejam os direitos humanos condicionados aos ditames da técnica. Nesse sentido, seria irrazoável a utilização de mecanismos ultra tecnológicos, que formalmente fugiriam do âmbito de proteção da norma, para empreender violações aos direitos fundamentais, sendo que nenhum avanço da técnica deve sobrepujar a protetiva de direitos.

É necessário conceber os direitos humanos como um processo dinâmico de construção e reconstrução (LAFFER, 1988, p. 134), refletindo concretamente espaços de luta pela dignidade humana. Podemos conceber espaços de luta no ambiente digital pela garantia da dignidade humana, compreendendo-a como uma dignidade isotópica (que se manifesta em ambos os espaços), mas com arestas também que extrapolam a simples correlação átomo bit, demarcando condições ímpares de dignidade que advém da específica vivência digital. Assim, pode-se conceber a *Internet* como um espaço de luta pela dignidade humana, de forma que essa tradução das lutas, como aquelas carregadas por Edward Snowden (2019) e Julian Assange (2013), compõem uma racionalidade de resistência digital.

Apesar das discussões relevantes apontadas na seção anterior, há que se compreender a relevância de uma visão utópica sobre os direitos humanos no ambiente digital, especificamente compreendendo a ascensão de demandas naturais dos utilizadores no ambiente digital. Flávia Piovesan (2006, p. 39) indica a necessidade de se abandonar uma visão genérica sobre os direitos humanos, de forma que se torna necessário identificar o sujeito titular dos direitos e suas particularidades, uma vez que determinados sujeitos de direito, determinadas violações ou ambientes exigem uma resposta específica. Portanto, nesse sentido, entende-se que todas as especificidades da realidade virtual justificam uma visão utópica, que enseja uma resposta específica para as relações humanas existentes no ambiente digital, que se marcam com expressiva distinção da realidade física.

Diante do exposto, vê-se que há uma realidade jurídica distinta daquela usualmente incidente sobre a tutela de direitos humanos no ambiente dos átomos, no qual a dogmática dá indícios de baixa efetividade, incapacidade de regulação das relações massivas e, ainda, desestruturação das bases hierárquicas de poder, projetando um cenário de violação de direitos

humanos, especificamente nos referindo aos direitos de liberdade e privacidade. A realidade da *Internet* demonstra que a massa de utilizadores, que se adensa cada vez mais, passa a sofrer, coletivamente, surtos de violência advindos da atuação dos Estados e instituições privadas, surtos manifestados pelo empreendimento do poder programacional em desfavor dos utilizadores da rede.

Na esteira da construção dos direitos humanos, vê-se que o momento se mostra propício para a afirmação coletiva de direitos humanos que emergem dessa nova realidade, firmando novos padrões de dignidade que se espelham nas práticas violatórias que ascendem à consciência social (COMPARATO, 2010, p. 50).

2.2 Tutela e Garantia da liberdade e da privacidade

Conforme exposto anteriormente, percebe-se um problema inicial afetando as normativas estatais de direitos humanos, enquanto eixo central das protetivas jurídicas à dignidade humana. As normas, enquanto constructos técnicos, dependem de uma regência e atualização conforme os padrões vigentes, como forma de se manterem integradas e capazes de eficientemente compatibilizar os efeitos pretendidos sobre os objetos. Necessita-se, portanto, que as normas jurídicas estejam tecnicamente adequadas ao ambiente de aplicação para que possam, minimamente, surtir efeitos. Tal situação ocorre através de normas atualizadas com frequência, capazes de refletir os avanços técnicos ou por meio da estruturação de normas tecnicamente neutras⁴⁶ (WEITZENBOECK, 2013, p. 294), capazes de se adequarem, ao menos no plano formal, a qualquer realidade emergente.

Com relação às normas não sujeitas a um padrão técnico neutro, a sua adequação à realidade técnica regente depende não de simples atividade hermenêutica dos seus aplicadores, uma vez que as próprias dinâmicas do Direito, centradas em uma realidade material e individualisticamente concebida, impõem barreiras de difícil superação pela hermenêutica. Por sua vez, as normas tecnicamente neutras encontram-se ainda respaldadas em um ordenamento jurídico e um sistema executivo lastreado firmemente sobre bases técnicas, o que enseja uma problemática diferente, porém, com o mesmo efeito prático: ausência de efetividades das medidas normativas positivadas.

⁴⁶ Uma norma tecnicamente neutra pode ser descrita como uma norma que não está presa a padrões técnicos, prevendo seus comandos deontológicos de forma geral, adequada a qualquer realidade técnica aplicável. Tomamos como exemplo o artigo 5º, II da Constituição Federal, que indica que “ninguém será obrigado a fazer ou deixar de fazer senão em virtude da lei”. Nele, não há padrões técnicos que vinculam a norma a circunstâncias específicas, permitindo que seja aplicado tanto para realidade técnicas industriais ou informacionais.

A adoção de uma interpretação teleológica e axiológica, capaz de correlacionar as normas à realidade fundante e suas finalidades (FERRAZ JR, 2001, p. 288), ainda assim refletiria em expressivas limitações à capacidade do direito estatal do mundo físico aplicar-se à realidade digital, considerando, ainda, um ordenamento jurídico pouco adaptado à fluidez do meio digital e sua realidade massificada. Há que se reconhecer que a técnica atua diretamente sobre a realidade socioeconômica e cultural, efetivamente moldando-as conforme seus padrões (CASTELLS, 2013, p. 51). Disso, há que se compreender que o Direito, enquanto uma superestrutura, pauta-se nos padrões técnicos que mediatamente atuaram sobre a realidade socioeconômica, cultural e ideológica (MARX, 2008, p. 47). Tal influência da técnica recai não somente sobre a norma, mas sobre o Direito como um todo, marcando suas estruturas e mecanismo, de uma forma tal que a transição para a técnica informacional pode representar efetiva dificuldade de incidência de efeitos concretos.

Embora considere-se os efeitos construtivos da interpretação sobre as normas de direitos humanos, enquanto aplicação da norma ao caso concreto capaz de adaptar os frios traços da dogmática jurídica para a realidade que cerca o direito (RAMOS, 2014, p. 92), dentro da argumentação trazida, fala-se em certa incompatibilidade entre a Estrutura Jurídica e a técnica fundante. Essa situação sugere, portanto, que não somente a norma sofre com a refração jurídica, mas os próprios instrumentos de operacionalização do Direito também sofrem com tais dificuldades. O Poder Judiciário ou os Tribunais Internacionais, até a hermenêutica jurídica, podem encontrar gravames à sua atuação em razão das alterações paradigmáticas da técnica.

Portanto, as bases do direito, sobre as quais se pautam o ordenamento jurídico, mostram-se incompatíveis com a realidade digital, pendendo uma readaptação técnica das estruturas jurídicas (sob um ponto de vista utópico) ou uma consolidação das normas para que possam, mediante robustas alterações e atividade hermenêutica, produzir efeitos sobre as relações no ambiente virtual.

A dita consolidação das normas apresenta-se como uma medida isotópica de adequação das normas aos problemas inerentes à sua incidência no ambiente virtual da *Internet*, portanto, dotando o Direito e suas estruturas de formas para traduzir ao ambiente digital parcela dos seus efeitos pretendidos. Nesse sentido, percebe-se certa falibilidade desse mecanismo, em razão da sua incapacidade de atualizar os instrumentos jurídicos de aplicação da norma e produção de efeitos, mantendo um mesmo sistema, que não é tecnicamente coerente com a realidade, e, dessa forma, sofre certo desgaste.

As divergências de exequibilidade entre o mundo físico e o mundo digital ainda aprimoram tais impactos, redundando em dificuldades expressivas para que a norma seja

refratada do ambiente físico para o digital, e seja capaz de gerar os efeitos protetivos que dela são esperados.

Apesar da relevância e dos pontos apontados antes, percebe-se que uma dinâmica isotópica de aplicação de direitos humanos no ambiente não se mostra tão adequada e eficiente, sugerindo ser incapaz de promover a devida tutela e efetivação da dignidade humana. A orientação utópica, por outro lado, dá indícios de se adequar a uma construção de direitos humanos pautados na técnica informacional (transcendendo o formalismo e o individualismo do Direito), refletindo demandas coletivas do meio e possuindo eficazes medidas de exequibilidade.

Na etapa da construção dos direitos humanos sob uma nova égide técnica, há que se indicar a necessidade de se traçar bases “homeomórficas” sobre as quais será possível construir planos mútuos de correspondência (PANNIKAR, 2004, p. 209). Por meio de uma base comum, capaz de traçar correlações da dignidade humana entre o meio físico e o digital, torna-se possível adequar até mesmo direitos humanos emergentes de uma realidade utópica à realidade protetiva da dignidade humana que já existe, evidenciando uma natureza humana universal que existe por meios digitais e, assim, um potencial tecnicamente neutro às bases da dignidade humana.

Apesar da universalidade da dignidade humana, a realidade técnica do mundo digital embasa robustas mudanças nas formas pelas quais as demandas coletivas e individuais ocorrem, permitindo a afirmação de que os direitos humanos são digitalmente existentes e não manifestos (não são, simplesmente, reflexos das lutas pela dignidade do mundo físico, possuindo especificidades marcantes).

Assim, busca-se compreender os direitos humanos digitalmente existentes, dada a divergência técnica que os fundaram e as suas especificidades. Parte-se para a análise específica dos direitos de liberdade e privacidade oriundos do ambiente digital, compreendendo as formas pelas quais tais direitos são identificados e divergem das suas versões oriundas da realidade física, além de se debruçar sobre a violação desses direitos e os mecanismos jurídicos usualmente incidentes em face de violações.

Ressalta-se que, adentrando especificamente na dogmática jurídica brasileira, a garantia e tutela dos direitos humanos no ambiente virtual é provida principalmente pela Lei n. 12.965, de 23 de abril de 2014, o Marco Civil da Internet, que projeta as normas de direitos humanos especificamente o ambiente virtual.

2.2.1 Liberdade no ambiente virtual

A *Internet* e as tecnologias digitais possuem como característica, além de carrear inovações massivas junto a determinadas questões, a capacidade de salientar traços da vivência humana e dar a elas roupagens mais robustas e expressivas, permitindo não somente que a vivência humana alcance novas situações, mas que consiga explorar e gerar melhor aproveitamento de situações que já são conhecidas e experienciadas. A visão é muito bem tracejada por Jack Balkin (2004, p. 2), ao indicar as características das liberdades na sociedade da informação.

Nesse sentido, a liberdade atinge uma conotação no ambiente digital que não se marca somente pela inovação relativa às suas dinâmicas já existentes e positivadas nos ordenamentos jurídicos. As liberdades mantêm certos traços-base e adquirem maior expressividade de manifestação, uma vez que os meios digitais passam a permitir uma ampliação quantitativa e qualitativa do seu exercício por intermédio da *Internet* e suas realidades cognatas. Assim como a liberdade mostra-se como o embrião dos direitos humanos (COMPARATO, 2010, p. 23), há que se perceber o afloramento das discussões jurídicas e éticas sobre a *Internet* por meio da liberdade.

Portanto, a *Internet* indica um papel de instrumentalização, de forma mais eficiente e prática, dos diversos aspectos que compõem a liberdade humana. As liberdades objetivas, como a liberdade política, econômica, de expressão e pensamento, ao encontrarem a realidade digital, passam por alterações majoritariamente centradas nas formas pelos quais os padrões de dignidade, manifestos nas modalidades de liberdade, serão alcançados. Como exemplo, seja por meio de um espaço de fala ou mesmo pela manifestação por vias digitais, o padrão de dignidade objetivado pela liberdade de expressão manter-se-ia semelhante, com a inclusão de caminhos mais simplificados e até mesmo mais idôneos.

Luciano Floridi et al (2015, p. 7) ressalta que a liberdade deve ser concebida como um conceito subjetivo, portanto, que decorre das relações humanas entre si, com artefatos tecnológicos e demais manifestações da natureza, de forma que a maior dificuldade atual das dinâmicas político-jurídicas é compreender a descorporificação do ser humano e seus impactos na questão da liberdade

Sob um prisma inicial, haveria uma tendência isotópica justificando tal ponto de vista, uma vez que os padrões de dignidade manter-se-iam semelhantes àqueles perseguidos no mundo dos átomos. No entanto, pontuando rumo a uma diretiva utópica, há que se considerar que até mesmo simplificações e aumentos de eficiência nos caminhos de atingimento da

dignidade humana já se mostram capazes de causar alterações robustas, que, apesar de não alterarem as bases da dignidade, ainda ressignificam os direitos na prática. Se a liberdade de expressão encontra caminhos livres e menos embaraçados para ocorrer por meio de uma específica página da *Internet*, por exemplo, há que se considerar uma adaptação da própria realidade prática, aproximando-se daquelas dinâmicas que se mostram mais eficientes e de fácil acesso à coletividade.

O mundo dos *bits* se comportaria como um meio para que a dignidade humana pudesse ser alcançada por caminhos mais ágeis e menos dificultosos, refletindo em uma própria noção de que tais meios, por serem mais propícios à efetivação dos direitos, consistiriam em efetivos novos traços de dignidade humana. Seria digno, portanto, que os padrões de dignidade fossem mais facilmente alcançáveis e efetiváveis, o que ocorreria no ambiente virtual. Ainda assim, já pontuando, ressalta-se que há que se considerar também a ambivalência da técnica informacional e seu provável efeito lesivo às liberdades.

Nesse ponto, aproxima-se do que fora exposto anteriormente, uma vez que a ampliação das vias lesivas à liberdade por meio da técnica informacional redundaria em espaços reativos da coletividade e dos indivíduos, objetivando a resistência a tais dinâmicas e a construção de novos direitos ascendendo dessa luta, permitindo a construção de direitos na própria realidade digital.

Portanto, sob essa ótica, haveria robustas alterações nos instrumentos de viabilização e instrumentalização, representando uma mudança pujante nas liberdades em razão da era da informação, assumindo uma conotação que, mesmo fosse referenciada aos próprios objetivos, ainda assim teria especificidades capazes de particularizá-las com relação ao mundo dos átomos. Ainda assim, vale notar que, nos termos trazidos na seção anterior, haveria que se considerar o ambiente digital como capaz de ressignificar os padrões de dignidade, que se ampliam sobre novas questões, permitindo criar a hipótese de que há direitos digitalmente existentes e não somente direitos digitalmente manifestados, especialmente considerando a ascensão de novas lutas coletivas e individuais, fruto das práticas lesivas advindas do meio digital.

Nessa dinâmica, haveria que se conceber o papel construtivo dos direitos humanos, especificamente a liberdade, com relação ao ambiente digital, de forma que as novas formas de instrumentalização e a ampliação das concepções de dignidade complementam diretamente as novas realidades de luta pela dignidade humana, efetivadas no meio digital. Conforme traz José Afonso da Silva (2005, p. 232), “o conteúdo de liberdade da liberdade se amplia com a evolução da humanidade. Fortalece-se, estende-se, à medida que a atividade humana se alarga”, o que

significaria a projeção da dignidade humana sobre novas concepções humanas que refletem na vivência.

A liberdade, sob um conceito geral, é descrita como a capacidade humana de manifestar, no mundo externo, as suas vontades interiores (SILVA, 2005, p. 231-232). A liberdade estaria relacionada à autonomia do indivíduo, com vínculo direto com a liberdade pública, fundamento do modelo democrático de governo, que pressupõe a regência por normas que a sociedade mesma estabelece (COMPARATO, 2010, p. 75). Nesse sentido, considerando a realidade do ambiente virtual, permite-se o entendimento de que a realidade virtual que nos cerca compõe um espaço de manifestação das vontades interiores, portanto, um espaço onde pode ocorrer a manifestação da autonomia humana, haja vista a realidade superficial, complexa e mimética que marca o ambiente informacional.

Apesar de ser una, é necessário conceber a sua manifestação em diferentes relações, situação que justifica a sua divisão e classificação conforme a realidade que ela incide (PIMENTA BUENO, 1958, p. 384). Haveria dois conceitos mestres de liberdade, a liberdade sob um ponto de vista negativo, portanto, atrelada à limitação de espaços de interferência, e sob um ponto de vista positivo, como a facilitação ou suporte à habilidade, melhoramento da habilidade, possibilidade e oportunidade de fazer algo (BERLIN, 1958, p. 15).

A liberdade a ser analisada dentro do escopo do trabalho divide-se em liberdade política e liberdade econômica, com cada um dos conjuntos contendo liberdades com conteúdo que se comunica.

A liberdade política seria composta por uma série de direitos que dizem respeito à convivência de um indivíduo no âmbito social, sem qualquer forma de opressão ou coerção ilegítima (MARION YOUNG, 1990, p. 39), o que conflui com a ideia sobre a liberdade apontada por Amartya Sen (2000, p. 83), como a ausência de situações incapacitantes para o indivíduo. Seria ela composta por todas aquelas liberdades civis, que se referenciem à existência do indivíduo no ambiente social, enquanto figura política imersa na coletividade, evidenciando a relação entre a política e a liberdade (ARENDT, 2005, p. 146-147).

A liberdade política seria composta, dentro da dinâmica pretendida para a pesquisa, pela liberdade física (a liberdade de locomoção) e as liberdades de pensamento (opinião, religião, informação, comunicação e expressão), enquanto manifestações desembaraçadas dos interesses humanos. Além das liberdades políticas, entende-se que haveria a liberdade de conteúdo econômico, marcada por um conteúdo patrimonialista aplicado à realidade das liberdades políticas.

Portanto, ambas as formas de liberdade seriam direitos humanos devidamente tutelados pelos ordenamentos jurídicos internos dos países e pelas diretivas internacionais, manifestas como garantias de exercício dos interesses, sem qualquer limitação que se mostre ilegítima. A divisão apontada, seguindo o modelo utilizado por Milton Friedman (2014, p. 16), parte de uma diferença conceitual no objetivo da ação que deverá ser executada e não repreendida pelos agentes do poder. As liberdades políticas, como a liberdade de locomoção e a de livre pensamento, teriam como objetivo a constituição do indivíduo enquanto ser político, imerso no meio social e dotado de autonomia, o que difere da liberdade econômica, que possuiria como direcionamento a tutela suplementar da propriedade privada.

A liberdade de empreendimento, por exemplo, possuiria uma natureza política relacionada aos interesses íntimos do indivíduo dentro de uma ótica social, no entanto, há uma visível manifestação de interesses que desembocam na proteção ampla do direito de propriedade. Ressalta-se que, mesmo com essas diferenças, Milton Friedman (FRIEDMAN, 2014, p. 17) entende que a liberdade econômica e política se encontram entrelaçadas, sendo que aquela mostra-se como fator essencial para a efetivação dos diversos traços da liberdade pessoal, comungando com a ideia de liberdade atrelada ao desenvolvimento trazida por Amartya Sen (2000, p. 17).

Nesse sentido, a liberdade individual, seja ela com conotação política ou econômica, possui uma finalidade que transcende a mera individualidade daquele que a possui, tendo projeção sobre toda a coletividade por meio do desenvolvimento social (SEN, 2000, p. 21), o que permitiria uma abordagem das liberdades não mais como uma dinâmica estritamente individualista.

A autonomia mostra-se como elo essencial na manifestação da liberdade, de forma que pode ser definida como a “capacidade de cada indivíduo viver uma vida seguindo seu próprio senso de valor, evitando ter suas intenções manipuladas, direcionadas, ou obstruídas por forças externas” (BERLE, 2020, p. 59). Trata-se, portanto, da essência sobre a qual se pauta a questão da liberdade, considerando sua importância sobre os valores humanos, por afetar substancialmente as relações humanas.

As liberdades emergem ao contexto jurídico enquanto formas de resistência à tirania dos déspotas, demandando, sob uma ótica positivista, medidas executivas capazes de garantir espaços de atuação negativa do Estado, amarras capazes de impedir interferências estatais sobre o indivíduo (COMPARATO, 2010, p. 76). No entanto, com o avanço das ondas construtivas de direitos, tornou-se visível, sob um ponto de vista coletivo, que a liberdade negativa se mostrava insuficiente para promover a liberação dos indivíduos, demandando que fossem implementadas

medidas positivas de liberação, atuações corretivas do Estado para que os níveis dignos de liberdade fossem atingidos (SILVA, 2005, p. 234).

Essa visão mostra-se importante para compreender a liberdade no ambiente da *Internet*, uma vez que, apesar das atuações opressoras do Estado, existem ainda poderosos agentes privados, capazes de impor limitações à liberdade dos utilizadores da rede e, assim, criar interferências ilegítimas. Manuel García-Pelayo (1967, p. 203) indica que há na história indicações suficientes de que o Estado não é o único agente opressor, compreendendo a existência de atividades coatoras advindas de diversas instituições da sociedade, figurando o Estado, face a essas realidades, como mecanismo capaz de tutelar a liberdade sob uma esfera negativa.

Sob essa abordagem, Molly Land (2009, p. 11) entende que a visão clássica das liberdades civis, como limitações à atuação do Estado, confronta-se com a realidade digital, entendendo que a atuação do Estado nessa esfera seria necessária, sob um ponto de vista ativo, para fazer frente às violações dos direitos dos cidadãos. As regulações privadas, advindas dos próprios agentes privados que atuam no ambiente da *Internet*, ao contrário do que aponta Lessig (2006), seriam insuficientes para regular e tutelar os direitos, considerando sua especial vulnerabilidade às dinâmicas mercadológicas, conforme entende Land (2009, p. 13).

Dessa forma, qualquer modalidade de coação injustificada e ilegítima representaria uma ofensa direta à liberdade, afetando concretamente a dignidade humana. Considerando o ambiente digital e a realidade algorítmica, concebe-se extensas manifestações de ofensas à liberdade por meio de limitações à livre determinação na vivência digital. As liberdades políticas no ambiente digital teriam como preponderantes a liberdade de navegação, a liberdade de pensamento, enquanto esferas de dignidade que sofrem robustas alterações quando comparadas com seus pares do mundo dos átomos.

2.2.1.1 Liberdade de navegação

A liberdade de navegação seria o direito dos indivíduos livremente circularem pelas esferas digitais, comungando, em si, liberdade de informação em uma escala massiva⁴⁷, dada

⁴⁷ Considerando a liberdade de locomoção como uma base para tal pensamento, há que se aplicar sobre ela a devida adaptação técnica, advinda do contexto regente, qual seja, a técnica informacional. Basicamente, as informações compõem o eixo central da nossa realidade socioeconômica, conforme apontado por diversos autores já citados. Nesse sentido, a navegação, em uma clara atividade metafórica ao ato de navegar pelos mares, em uma dinâmica vanguardista, compreenderia o direito de fluir pelos meios e server informações ali existentes/disponíveis. A omnipresença das informações acabaria por impedir que o ato de navegar pela *Internet* viesse conjugado ao conteúdo informacional.

uma dinâmica utópica⁴⁸, tratando-se de um direito com conotações positivas e negativas. Seria a liberdade de fluir e server conhecimento das diversas esferas da *Internet*, considerando-a como um ambiente virtual de ampla comunicação e compartilhamento de informações, livremente acessível a uma grande quantidade de pessoas (PERRY; RODA; 2017, p. 64). Apesar de uma semelhança com a liberdade de ação⁴⁹, fundamento geral e abstrato que compõe a base das liberdades civis, há que se visualizar os impactos da transmutação técnica, na qual a realidade informacional impôs novas dinâmicas à realidade e, por sua vez, permitiu que novas construções de direitos emergissem, considerando a liberdade de navegação como um amálgama forjado sob a técnica informacional entre a liberdade de ação e a liberdade de conhecimento e informação.

A liberdade de navegação é historicamente presente no meio virtual, estando atrelada, diretamente, aos primórdios da *Internet* e à ausência de mecanismos de controle dos fluxos informacionais. Castells (2003, p. 173) entende a liberdade no ambiente virtual relacionada a duas bases originárias, uma base tecnológica, vista a liberdade sob o ponto de vista da incapacidade original de se estabelecer limitações à arquitetura de conexão, e uma base jurídica, tendo a *Internet* surgido sob a proteção constitucional regente nos Estados Unidos da América, o que imporá certas limitações às violações de liberdade.

A circulação pelas vias digitais consistiria nas garantias de utilização desembaraçada e sem restrições dos diversos sítios e aplicações que compõem a rede, independente de limitações geográficas ou de qualquer outra natureza. Se, por um lado, o direito de acesso à *Internet*, compreendido até mesmo pela ONU como um direito humano, decorrente da liberdade de opinião e expressão (ONU, 2011, p. 7), o direito de navegação partiria de uma premissa utópica, considerando o ambiente virtual e sua vivência de forma autônoma do mundo físico. Se a técnica consiste na realização mediata e dotada de menos esforços e dispêndios para a realização de atividades humanas (ORTEGA Y GASSET, 1963, p. 17), pressupõe-se que no ambiente técnico informacional possa-se reconsiderar a locomoção e incluí-la dentro da dinâmica virtualizada.

⁴⁸ A liberdade de navegação demandaria não somente atuações negativas, mas especialmente medidas positivas, capazes de garantir acesso dos indivíduos ao ambiente digital, situação que se aproxima das dinâmicas isotópicas, demandando atuações no mundo dos átomos para que seja viabilizado o acesso ao mundo dos *bits*.

⁴⁹ A liberdade de ação trata-se do fundamento geral das liberdades, constituindo a capacidade do indivíduo agir no mundo, expressando seus interesses sem qualquer opressão ilegítima limitando-o. A liberdade de ação é prevista no artigo 5º, II, da Constituição Federal.

É necessário considerar o conteúdo informacional da liberdade de navegação, atrelado diretamente ao direito de procurar e receber informações e ideias, que é previsto no artigo 19⁵⁰, e o direito de participar livremente da vida cultural da comunidade, fruir das artes e do progresso científico, nos termos do artigo 27⁵¹, ambos da Declaração Universal dos Direitos Humanos. Há na *Internet* e suas vias um enorme potencial de propagação do conhecimento, motivo pelo qual a circulação, pelas vias digitais, passa necessariamente por conteúdos e informações que se mostram relevantes para a formação do indivíduo e garantia da sua dignidade, o que indica um atrelamento entre a circulação na *Internet* e a imersão em informações. Nesse sentido, o direito de informação passaria pelo livre e equitativo acesso ao conhecimento e informações disponibilizadas no ambiente virtual (LAND, 2009, p. 2), um direito de o indivíduo inserir-se e fazer uso da realidade informacional que o cerca, durante a navegação pela *Internet*.

Assim como os demais direitos humanos, há que se ponderar os limites da liberdade de navegação, de forma a compatibilizar com interesses outros legítimos, como o caso da propriedade e da privacidade.

Apesar de não prevista especificamente nos ordenamentos jurídicos positivados, formalmente estaria esta liberdade tutelada de forma genérica, contando com proteção em diversos ordenamentos. Citamos o caso brasileiro, em que a liberdade de navegação é um dos objetivos de proteção da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da *Internet*), prevista nos incisos I e II do artigo 4^{o52}, comungando, ainda, proteção dos artigos 5^o, II⁵³ e 6^{o54}, da Constituição Federal.

A violação da liberdade de navegação consistiria em uma realidade frequente no meio virtual, especialmente manifesta por meio da oposição de barreiras algorítmicas e procedurais

⁵⁰ Artigo 19: Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras.

⁵¹Artigo 27: 1. Todo ser humano tem o direito de participar livremente da vida cultural da comunidade, de fruir as artes e de participar do progresso científico e de seus benefícios. 2. Todo ser humano tem direito à proteção dos interesses morais e materiais decorrentes de qualquer produção científica literária ou artística da qual seja autor.

⁵² Art. 4^o A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos; II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

⁵³ Art. 5^o Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

[...]

II - ninguém será obrigado a fazer ou deixar de fazer alguma coisa senão em virtude de lei;

⁵⁴ Art. 6^o São direitos sociais a educação, a saúde, a alimentação, o trabalho, a moradia, o transporte, o lazer, a segurança, a previdência social, a proteção à maternidade e à infância, a assistência aos desamparados, na forma desta Constituição.

capazes de impedir, de forma automática, a livre circulação pelo meio digital. Reitera-se que se parte de uma análise pautada na dinâmica utópica do direito na *Internet*, o que pressupõe compreender essa realidade como própria e desvincilhada do mundo dos átomos, ao menos sob o ponto de vista superficial e técnico. Nesse sentido, não se encontra, no escopo de análise, aquelas limitações ao direito de navegação advindas do mundo físico, como a incapacidade física de acesso à *Internet*, hipossuficiência informática e outros.

Enquanto normas matematicamente desenvolvidas, os algoritmos objetivam a construção e operacionalização do ambiente digital, procedendo com suas finalidades por meio de uma lógica de entradas (*inputs*) e saídas (*outputs*) codificadas (GILLEPSIE, 2018, p. 1). São diretivas procedimentais, com capacidade regulatória de fato, que modelam concretamente a realidade virtual, sendo a base programacional de todos os constructos virtuais. Ao acessarmos um sítio digital ou mesmo darmos um comando para o envio de uma mensagem eletrônica, estamos, diretamente, em contato com uma série de algoritmos, que estruturam o aspecto visual do sítio, suas funcionalidades, codificam os espaços editáveis e acessíveis aos utilizadores, dentre diversas outras funcionalidades.

Durante a estruturação ou funcionalização da realidade digital, os algoritmos permitem o afastamento do operador humano com relação aos seus efeitos, constituindo um fato essencial na automação de processos e na construção de realidades digitais complexas (GILLEPSIE, 2018). Há que se visualizar o potencial técnico dos algoritmos de estruturarem vias regulatórias eficientes, enquanto mecanismos arquitetônicos emergentes da realidade informacional. Possuem, portanto, adequação técnica ao ambiente digital, o que garante a sua efetiva capacidade regulatória, mostrando-se eficaz para reger as relações humanas ocorridas na *Internet* através de métodos coercitivos automáticos, manifestados de forma negativa.

A liberdade de navegação vê-se frontalmente ameaçada pela algocracia, um fenômeno marcado pelo uso onnipresente de algoritmos para a percepção da realidade e controle, com expressiva capacidade regulatória.

Se, por um lado, a liberdade de circulação é violada por meio da repressão física, manifesta e circunscrita, a liberdade de navegação é suprimida por algoritmos silenciosos e onnipresentes, que ao invés de reprimir, simplesmente não permitem que, dentro dos códigos de funcionamento do sítio ou aplicação digital, o utilizador navegue livremente. Ou seja, o ambiente programado é controlado por limitações às alternativas previamente programadas (ANEESH, 2009, p. 356).

Portanto, enquanto em um modelo panóptico há o controle ativo, demandando sua realização pelo agente de poder, o modelo algocrático marca-se por, simplesmente, negar o

funcionamento de determinado sistema ou impor dificuldades diante de certas circunstâncias, tudo isso pautado em caminhos já programados. Diante disso, dada a regência absoluta dos algoritmos sobre o ambiente virtual, há que considerá-los como práticas que violam a liberdade de navegação dos utilizadores da rede, especialmente tendo em vista os efeitos lesivos da vigilância digital e sua sensação sobre a liberdade humana (HESMONDHALGH, 2006, p. 212-215).

Considerando que todas as práticas no ambiente digital se encontram sujeitas à regência de algoritmos, há que se visualizar a projeção geral dos efeitos lesivos desses sistemas sobre a liberdade de navegação. Ainda assim, cumpre ressaltar os efeitos lesivos da vigilância e afetação da privacidade, que desembocam em efeitos lesivos sobre a liberdade humana, considerando a expressiva existência de dinâmicas de vigilância digital empreendida pelos Estados e por corporações privadas (MÁRTINEZ-BEJAR; BRANDLE, 2018, p. 145).

Face ao exposto, a garantia da liberdade de navegação ocorre, primordialmente, por meio de medidas negativas, com o estabelecimento de espaços de ausência de intervenções estatais na norma constitucional, ausentes medidas mais efetivas para permitir, sob um ponto de vista positivo, o alcance da liberdade em uma dinâmica mais ampla. Há que se ressaltar que há, ainda, uma divisão clara entre a navegação na *Internet* e seu conteúdo informacional. A navegação e sua dinâmica informacional são vistos como direitos humanos somente sob o ponto de isotópico, de acesso à *Internet*, diretamente atrelado ao direito de opinião e livre expressão, nos termos do artigo 19 da Declaração dos Direitos Humanos e a sua compreensão pelo Conselho de Direitos Humanos da ONU.

Portanto, a liberdade de navegação não é compreendida pelos ordenamentos jurídicos e pelos regramentos internacionais sob um ponto de vista uno, além de estar atrelada, na dogmática dos direitos humanos, à liberdade de opinião e expressão, o que sugere uma abordagem isotópica e, portanto, indicando o ambiente virtual como mera ferramenta em função do ambiente físico, não comungando com a ideia de a realidade digital consistir-se em um ambiente de vivência dotado de especificidades.

A tutela das liberdades, por sua vez, ocorreria por meio da atuação responsiva às violações, ou seja, medidas pós-violatórias empreendidas pelas vias judiciais e administrativas para impor sanção àqueles que praticam as lesões e pleitear reparações na esfera civil.

Perpassado o espaço formal de proteção, o ordenamento jurídico seria capaz de promover a tutela somente pela via reparatória, o que dependeria da incidência de mecanismos que não são tecnicamente aptos para compreender as violações de direitos, possuindo ainda menos capacidade de produzir efeitos sob a esfera digital. Especialmente considerando os

algoritmos que regem a vivência digital, percebe-se uma fragilidade executiva das normas que, distante das realidades arquitetônicas tecnicamente aderentes à vivência digital, sofrem com robustas dificuldades de incidência.

Há que se considerar, portanto, uma afetação à liberdade de navegação por parte dos Estados, como evidencia John Laprise (2013) ao abordar o fenômeno da alegabilidade do ambiente virtual, especialmente considerando as práticas de controle e vigilância. Citamos como exemplo marcante da violação da liberdade de navegação o caso da Grande Muralha Chinesa, um *firewall*⁵⁵ adotado para limitar o acesso à *Internet* pelos cidadãos chineses, impedindo concretamente a livre circulação e impondo bloqueio de conteúdo que afeta diretamente o direito de informação dos utilizadores da rede, conforme denotam diversos autores (FEIR, 1997, p. 368-370) (CLAYTON, 2006, p. 21). Trata-se de um modelo de controle de fluxo de informações, medida que ameaça frontalmente a liberdade de navegação, impossibilitando a livre circulação digital e ainda criando embaraços e impossibilidades para o livre acesso à informação.

Scott Feir (1997, p. 361) indica:

No entanto, a tecnologia da *Internet* ameaça comprometer a capacidade da China de controlar a troca de informações. A maior capacidade de comunicação e acesso às informações permite que os cidadãos chineses troquem ideias e informações livremente pela *Internet*. Para restringir essa nova liberdade, a China promulgou as Regras Provisórias de Gerenciamento da *Internet*. Esses regulamentos avisam os utilizadores, provedores de serviços e desenvolvedores de aplicativos sobre os métodos de acesso aprovados pelo governo e o conteúdo permitido de comunicações pela *Internet*. Além de que, conforme esses regulamentos, a China está trabalhando com empresas privadas de tecnologia para limitar fisicamente o acesso de seus cidadãos à *Internet* por vários meios, como filtragem, bloqueio e estabelecimento de uma intranet chinesa proprietária.⁵⁶

Há que se dar atenção especial à afetação à liberdade de navegação promovida por pessoas jurídicas de direito privado e seus prepostos, conforme já apontado, inclusive auxiliando os Estados nas práticas violatórias. Acerca disso, Rodrigues, Marchetto e Barrientos-Parra (2020, p. 509) apontam:

⁵⁵ *Firewall* ou corta-fogo é uma estrutura de *hardwares* e/ou *softwares*, que aplicam filtros e limitações no fluxo de dados.

⁵⁶ “*Yet Internet technology threatens to compromise China's ability to control information exchange. Increased ability to communicate and access information enables Chinese citizens to freely exchange ideas and information over the Internet. To restrict this new found freedom, China enacted the Interim Internet Management Rules. These regulations provide notice to users, service providers, and application developers as to the governmentally approved methods of access and permissible content of Internet communications. In addition to and consistent with these regulations, China is working with private technology companies to physically limit its citizens' access to the Internet by various means such as filtering, blocking, and establishing a proprietary Chinese intranet*” (tradução livre).

É necessário entender que as corporações digitais, enquanto agentes com capacidade técnica e financeira para desenvolver e gerenciar parcelas da rede mundial de computadores e seus mecanismos, possuem expressivo poder dentro da rede, atuando por meio de esferas alegais que mascaram suas atividades ilícitas sobre a privacidade, através de papéis intermediários nos fluxos de informação, enquanto *longa manus* do Estado e de sua regulação, com acesso privilegiado a tais informações, ou mesmo, de forma contumaz, violando a privacidade com o “aval” do Estado, que se utiliza dessa situação de ilegalidade para também ter acesso à esses dados.

Nesses termos, percebe-se a atuação tanto de agentes estatais quanto de agentes privados nas práticas violatórias do direito de navegação. Portanto, tanto as medidas negativas de garantia quanto as práticas positivas de efetivação da liberdade, providas pela dogmática, dão indicativos de incapacidade, especialmente técnica, relacionada à baixa visibilidade das lesões e dificuldades de exequibilidade das medidas no ambiente virtual. As medidas reparatórias, por sua vez, mostram-se também impactadas pela transição técnica, indicando pontos de fragilidade que refletem em reduzida efetividade.

Atentando-se às outras formas de regulação existentes no ambiente virtual, apontadas por Lessig (1998, p. 664), percebe-se certa fragilidade nas medidas usuais capazes de produzir efeitos sobre a tutela e efetivação da liberdade de navegação. Os costumes da rede são marcados pela liberdade de navegação, enquanto uma das bases ideológicas sobre as quais se firmou a utilização civil da *Internet* (CASTELLS, 2003, p. 24), havendo diversos ambientes da *Internet*, que são programados com o intuito de garantir, de forma nativa, o exercício desse direito pelos utilizadores.

Apesar da relevância das normas sociais, conforme denota Lessig, (1998, p. 123), há maior eficácia nas medidas regulatórias advindas das normas estatais, enquanto força regulatória capaz de impactar diretamente sobre as demais. No entanto, conforme apresentado, percebem-se certas condições que impõem dificuldade para que a norma, enquanto força regulatória primordial, produza efeitos concretos sobre a tutela e efetivação do direito à livre navegação na *Internet*.

Adequando-se à realidade informática e cooptando forças arquitetônicas em favor da garantia da liberdade de navegação, há que se ressaltar a possibilidade do empreendimento de medidas tecnicamente adequadas para garantir o exercício da liberdade, como o caso das medidas criptográficas, que permitem a sobreposição de limitações da rede e a blindagem do utilizador frente às medidas de controle (ISHAI et al, 2006, p. 239). Além disso, há que se vislumbrar a ascensão de novos mecanismos capazes de tutelar esses direitos por meio de dinâmicas descentralizadas e viabilizadas pelo consenso coletivo, como o caso das tecnologias relacionadas às *Blockchains* e outras correlações.

2.2.1.2 Liberdade de Pensamento

A liberdade de pensamento na *Internet* alcança uma projeção antes nunca experimentada no ambiente físico, ampliando a níveis massivos a capacidade dos indivíduos, livremente, manterem pensamentos e expressá-los à comunidade, sem qualquer forma de coerção ou embaraço. Nas palavras de Manuel Castells (2003, p. 173), a liberdade de pensamento mostra-se como uma das bases de surgimento da *Internet*, firmando-se como umas ideologias fundantes dos primeiros grupos conectados à rede mundial de computadores, muito antes de sua disponibilização global e da estruturação de vias de acesso facilitada (como o caso do sistema *word wide web*) (CASTELLS, 2003, p. 86).

Considerando a facilidade dos meios digitais e o próprio refluxo informacional (HAN, 2018, p. 37), há que se considerar que a *Internet* permite a expansão da participação cultural dos indivíduos, atingindo níveis muito superiores àqueles existentes em tecnologias anteriores, como o caso da mídia impressa, do rádio e da televisão. Por sua vez, a participação cultural democrática estaria diretamente relacionada à liberdade de pensamento, sendo que a possibilidade de os indivíduos constituírem espaços de fala e expressão, sem oposições coercitivas, é um dos pressupostos para a estruturação de um modelo democrático de direito pautado na dignidade humana. Mais que isso, a *Internet* permite não somente espaço para o exercício da livre expressão, constituindo uma realidade muito mais acessível do que as instâncias tecnológicas de expressão anteriormente existentes, considerando a diminuição dos custos atrelados à expressão e a sua facilidade (BALKIN, 2004, p. 8).

Sob a óptica de Macluhan (1969, p. 37), a *Internet* constituiria um meio de comunicação quente, dada a expressividade dos fluxos informacionais, devendo-se considerar que, além disso, permite-se o alcance de condições benéficas à liberdade de pensamento nunca antes experimentadas pelo ser humano, unindo uma técnica facilitadora e uma dinâmica de acesso massiva, que permite, sob custos reduzidos, um acesso dos indivíduos à possibilidade de gozar de livre expressão e pensamento. Se antes a liberdade de expressão mostrava-se fortemente relacionada à propriedade dos meios de comunicação, agora, por meio da *Internet*, alcança-se uma forma mais igualitária e ampliada de livre expressão (BALKIN, 2004, p. 19).

Conforme expõe John Balkin (2004, p. 2), a liberdade de pensamento não é alterada em seus aspectos fundamentais, ocorrendo, na verdade, um maior esclarecimento de outros vieses por meio das tecnologias digitais, que, diretamente, alteraram as condições sociais de expressão. Portanto, concebendo a liberdade de pensamento na *Internet*, mesmo sob um ponto de vista utópico, há que se considerar sua similaridade com a liberdade de pensamento existente no

mundo dos átomos, marcando-se aquela existente no mundo dos *bits* por novas condições sociais de seu exercício. Ainda assim, há que se considerar que uma visão estritamente isotópica não se mostra coerente com os impactos do ambiente digital, que, apesar de não demarcarem novos aspectos de dignidade, permitem o seu alcance de forma mais facilitada e eficiente, evidenciando distinções suficientes para derrocar uma visão isotópica estrita.

A liberdade de pensamento, em seu sentido lato, consistiria em um aglomerado de liberdades relativas ao conteúdo intelectual e sua projeção para o ambiente social, comungando a liberdade de opinião, enquanto direito de adotar atividade intelectual de forma autônoma (ROBERT, 1977, p. 302), a liberdade de expressão, enquanto direitos relacionados à expressão e difusão de opiniões. Trata-se a liberdade de pensamento de uma liberdade subjetiva, que não possui, necessariamente, uma manifestação externa, há que se conceber maior relevância à liberdade de expressão, que possui natureza objetiva e, de fato, contém diversas especificidades relativas à sua tutela e garantia no ambiente digital. A liberdade de pensamento, apesar da divisão aqui proposta, mantém laços estreitos com a liberdade de navegação, sendo que o direito de pensar livremente na *Internet* estaria associado, diretamente, à possibilidade de livremente fluir pelos meios e sorver conhecimento que se mostre adequado para a construção da personalidade.

A dogmática jurídica, atendo-se à brasileira, possui a previsão jurídica da sua tutela, construindo normativa tecnicamente neutra, capaz de se adequar às novas dinâmicas sociais que marcam a liberdade de expressão na *Internet*. O artigo 5º, IV da Constituição Federal prevê, sob um ponto de vista negativo, a liberdade de manifestação, enquanto norma de eficácia plena (SILVA, 2005, p. 244), tendo sido pormenorizada e tecnicamente direcionada ao âmbito da *Internet* por meio da Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet).

Por sua vez, as normativas internacionais possuem também a aceção desse direito, especificamente indicado no artigo 19 da Declaração Universal dos Direitos Humanos, que conta com um dispositivo tecnicamente neutro, o que permite compreender a possibilidade de sua aplicação no ambiente da *Internet*. A temática é ainda prevista em diversas outras normativas internacionais, como o caso da Convenção Americana de Direitos Humanos de 1969 (artigo 13), pela Convenção Europeia de Direitos Humanos de 1950, pela Carta de Direitos Fundamentais da União Europeia e na Carta Africana de Direitos Humanos e dos Povos de 198.

Sob um ponto de vista positivo, portanto, de medidas afirmativas capazes de efetivar a liberdade de expressão, há indicativos de diretrizes para a atuação do Poder Executivo nas iniciativas de fomento à *Internet* como ferramenta social por meio do Marco Civil da *Internet*,

especificamente no seu Capítulo IV, que contempla os artigos 24 a 28. Nesse sentido, pontua-se que há a necessidade de medidas afirmativas, tanto de caráter isotópico quanto utópico, enquanto medidas adequadas à garantia e efetivação da liberdade de expressão na *Internet*, garantindo não somente o acesso à *Internet* e suas aplicações, mas garantindo espaços de livre expressão e ausência de coerções ilegítimas.

Apesar do disposto, percebe-se a existência de medidas concretas de violação à liberdade de expressão no ambiente da *Internet*, manifestados por meio de espaços com controles algorítmicos ou humanos. Jeffrey Rosen (2012, p. 1537) entende que a proteção da livre expressão no ambiente digital, marcado por grandes corporações digitais regentes, em escala quase monopolista dos espaços de fala massificados, apresenta-se como uma questão de extrema complexidade, dada a não sujeição direta desses entes às vedações constitucionais.

Nesse sentido, a garantia da liberdade de expressão, face às violações promovidas por agentes privados na *Internet*, dependeria não de medidas negativas, de eficácia plena, como ocorre com relação ao Estado, considerando a existência de dúvida tanto acadêmica quanto jurisprudencial acerca da aplicação direta das normas garantidoras de direitos humanos a agentes não estatais (RONA; AARONS, 2016, p. 16). Seriam necessárias, por sua vez, medidas afirmativas, capazes de garantir o direito e reparar eventuais lesões, cabendo ao Estado regular a conduta dos agentes não estatais, forçando-os a cumprir com as normas de direitos humanos.

Dentro da dinâmica atual, caberia ao Estado adotar medidas para apurar a responsabilidade daquele que violou direitos, além de prover meios para a efetivação do direito. No entanto, na visão de Rona e Aarons (2016, p. 31), apesar de haver previsão majoritária dessas medidas na dogmática jurídica e serem elas adequadas à tutela dos direitos humanos, há certas dificuldades de efetivação, especialmente na *Internet*.

Levando em conta a estrutura regulatória do ambiente virtual, proposta por Lessig (2006), Jeffrey Rosen (2012, p. 1536) compreende que a privacidade e a liberdade de expressão possuiriam, no ambiente virtual, um especial envolvimento com as forças regulatórias sociais e arquitetônicas, uma vez que envolvem principalmente a atuação de agentes privados que, como atividade finalística, visam lucro. Tendo como paradigma final o lucro, as empresas do ambiente digital, como Facebook e Google, adotariam padrões de liberdade de expressão condizentes com as demandas sociais de maior expressão na rede, o que pode, por sua vez, refletir em modelos de liberdade limitados por fatores de pouca relevância e inadequados à dignidade humana. Além disso, as medidas arquitetônicas far-se-iam presentes em razão de sua autoexecutividade e eficácia.

Haveria, portanto, um impacto muito maior nas práticas das empresas privadas compreendendo limitações à liberdade de expressão no ambiente virtual, considerando sua atuação frequente, constante, e sem padrões de legitimidade e ponderação.

Especificamente nas mídias sociais, as políticas internas regem a totalidade das vivências ali ocorridas, ditando, por meio de algoritmos, quais falas terão espaço e quais falas censuradas, sendo ausente qualquer indicativo de fundamentação decisória e ausente a possibilidade de questionamento da decisão àquele que a proferiu. Nesse sentido, haveria padrões regulatórios sobre a liberdade de expressão ocultos, que seriam capazes de impor arquétipos de expressão aceitáveis, tudo isso realizado por meio de um sistema autônomo e auto executivo (YEUNG; DIZON-WOODS, 2010, p. 53).

A título de exemplo, vejamos os algoritmos de censura de mídias sociais como Facebook e Twitter, que fazem uso de algoritmos preventivos, pautados na análise massiva de dados para, por meio da formação de padrões, fazer atuações regulatórias por meio de inferências (YEUNG, 2017, p. 509), impondo censura àquelas manifestações que possuem traços, matematicamente definidos com base na análise de padrões, que indicam possibilidade de ser aquela manifestação marcada por ódio contra grupos ou pessoas.

Conforme expõe o Conselho de Direitos Humanos das Nações Unidas (ONU, 2011, p. 6-7) a liberdade de expressão poderá ser limitada mediante a invocação de um motivo legítimo, procedendo com a sua demonstração de forma individualizada e específica, indicando claramente a natureza da ameaça a outro direito, a necessidade da medida e, para tanto, adotando meios proporcionais. Tais exigências não são cumpridas no ambiente virtual, principalmente pelas empresas digitais, que gozam de liberdade ampla para compor suas políticas internas relativas à liberdade de expressão, adotando práticas leoninas e, mais que isso, violatórias de direitos humanos.

Trata-se, portanto, de medidas sem apego aos padrões democráticos e à dignidade humana, lançando robustas violações sobre o direito de expressão. Trata-se de um poder de censura epistêmico, centrado em poucos indivíduos que possuem poder direto sobre as estruturas codificantes, possui, portanto, o “controle sobre o teclado dos programadores”.

Acerca disso, Rosen (2012, p. 1536) expõe:

Até recentemente, a pessoa que possuía poder para determinar quem fala e quem será ouvido no mundo todo não era um presidente, um rei e nem mesmo um tribunal de justiça. Era ela Nicole Wong, que era consultora geral adjunta do Google, até a sua recente demissão. Nicole era conhecida no Google como a “decisora”. Nicole acordava durante a noite e decidia qual conteúdo existiria ou não, não somente no google.com, mas em cada escritório regional do Google em todo mundo, como o

google.fr, google.de, mas também alcançando o Youtube, que foi adquirido pelo Google em 2006.⁵⁷

Nesse sentido, considerando a realidade digital, há que se conceber a primazia das violações da liberdade de expressão por parte de agentes não-estatais, com ênfase em grandes corporações digitais diretamente envolvidas na criação e gerenciamento de redes sociais, ambientes onde, primordialmente, dentro da dinâmica atual, é exercida a liberdade de expressão. As violações de direitos de expressão por parte do Estado, por sua vez, concentrar-se-iam na falência das medidas afirmativas de efetivação dos direitos, não provendo meios materiais para seu exercício e, além disso, não adotando medidas suficientes para barrar a atuação dos agentes privados.

Vale ressaltar que o Relator Especial para a Promoção e Proteção da Liberdade de Expressão e Opinião, David Kayne, indicou uma relação direta entre a violação da livre expressão e as práticas de vigilância, recorrentemente empreendidas no ambiente digital. Além disso, entendeu o Relator que haveria situações de interferência na liberdade de expressão, por meio de limitações ao acesso às tecnologias de anonimização e encriptação (ONU, 2012, p. 2).

Por sua vez, o Relator Especial para a Promoção e Proteção da Liberdade de Expressão e Opinião, Frank La Rue, apresentou, junto ao Conselho de Direitos Humanos das Nações Unidas, o entendimento de que a liberdade de expressão e pensamento, especialmente considerando o ambiente digital, teria como pré-requisitos para seu gozo a existência de meios capazes de tornar a *Internet* um ambiente aberto e seguro (ONU, 2013a, p. 4).

Ressalta-se que a visão empreendida pelo Relator parte de uma premissa relativizada, compreendendo tanto as dinâmicas isotópicas de violação da liberdade de expressão, como o caso de intimidação *off-line*, quanto dinâmicas utópicas, como o caso de limitação ao acesso de tecnologias protetivas da livre expressão.

⁵⁷ *Until recently, the person who had more power to determine who may speak and who may be heard around the world was not a president or king or Supreme Court Justice. She was Nicole Wong, who was deputy general counsel at Google until her recent resignation. Her colleagues called her “the Decider.”. Nicole Wong was the Decider, who was awoken in the middle of the night to decide what content goes up or comes down, not only on Google.com, not only on each of the national Googles that are operated around the world, such as Google.fr, Google.de, but also what goes up or comes down on YouTube, which Google bought in 2006. (Tradução livre)*

2.2.1.3 Liberdade Econômica

A liberdade econômica seria o direito dos utilizadores da *Internet* exercerem livremente seu papel de agente econômico na rede, podendo dispor dos seus recursos⁵⁸ e propriedade sem estarem sujeitos a qualquer forma de coação ilegítima (ROTHBARD, 2008). O conceito da liberdade econômica adequa-se bem à realidade digital, especialmente considerando sua extensão não somente aos termos patrimoniais, concebendo sob o espectro de liberdade do indivíduo todos aqueles recursos, energias, trabalhos e forças que poderão ser livremente alocados, conforme o interesse de seu possuidor.

Exemplificando, um indivíduo que possui capacidades artísticas tem a liberdade econômica para, livremente, alocar suas capacidades artísticas no ambiente digital, seja ela de forma remunerada ou mesmo gratuita, podendo muito bem comercializar suas produções por meio da rede. O mesmo vale para o indivíduo que exerce atividade laborativa por meio da *Internet* ou aquele que empenha essa via para a troca de bens e direitos.

Essa forma de liberdade envolve, necessariamente, a possibilidade de alocar recursos de forma desembaraçada, de forma que não haja condições ilegítimas que impeçam a livre circulação desses recursos, valendo considerar que as facilidades trazidas pela *Internet* possibilitam meios mais simplificados para a livre movimentação de recursos, forças e patrimônio, que passam a fluir de forma ágil e eficiente pela via digital.

A liberdade econômica estaria estritamente relacionada ao direito à propriedade, vinculando-a diretamente à possibilidade dos indivíduos, livremente, exercerem suas vontades centradas na operacionalização econômica de bens por intermédio da realidade informacional da *Internet*. De certa forma, sob uma visão inicial, os bens estariam vinculados à *Internet* somente quando referidos à realidade física, no sentido da desmaterialização da realidade virtual.

Nos termos já apresentados, é necessário repensar as dinâmicas que nos cercam quando visualizadas sob a ótica do ambiente virtual, de forma que a alteração técnica permite que institutos usualmente materiais, como o caso da propriedade, assumam maior relevância na virtualidade. O tema será melhor abordado quando nos depararmos com o direito à propriedade no ambiente da *Internet*. Ainda assim, há que se considerar a existência de propriedade no ambiente virtual e a possibilidade de sua livre disposição, denotando a liberdade econômica.

⁵⁸ Adota-se o sentido amplo de recursos, portanto, nos termos do Dicionário Michaelis *online* (2021): “aptidões naturais ou inatas para fazer algo; meios pecuniários, recursos financeiros, posses”.

A liberdade econômica teria uma conotação social, relacionando-se não somente com o âmbito individual, mas projetando efeitos sobre a coletividade, sendo ela um fator essencial na efetivação de liberdade política, apresentando-se, conforme indicam alguns autores, como um meio de dispersão do poder concentrado (FRIEDMAN, 2014, p. 17).

Especificamente analisando a dogmática jurídica brasileira, a liberdade econômica estaria garantida por meio de normas diretamente relacionadas à propriedade e à livre iniciativa, nos termos dos artigos 1º, IV; artigo 5º, XXII; e artigo 170, *caput*, todos referentes à Constituição Federal. No âmbito da *Internet*, a Lei nº 12.965/2014, o artigo 2º, V, estabelece a livre iniciativa, dentre outros, como um dos fundamentos da *Internet*, sendo seu uso disciplinado, nos termos do artigo 3º, VIII, visando a liberdade dos modelos de negócios ali promovidos. Trata-se, portanto, de um direito manifestado sob a forma de espaços de ausência estatal, limites expressos sobre os quais deve ser omitida a atuação, ressaltando o caráter primordial das violações empreendidas pelo Estado.

Ainda assim, há que se ressaltar a possibilidade de violações à liberdade econômica, tendo como origem agentes privados na *Internet*, especialmente empresas digitais que atuam em caráter anticompetitivo, adotando práticas econômicas que dificultam ou causam embaraço à liberdade econômica dos utilizadores, medidas essas que possuem pouca visibilidade e escassos instrumentos jurídicos adequados à sua garantia.

Exemplos como o Google (CLEMONS; MADHANI, 2010, p. 51) sugerem o enorme poder econômico (e, por consequência, computacional) de companhias digitais, de forma que seu controle sobre o mercado de buscas e publicidade digital poderiam ser empreendidos para violar direitos dos utilizadores da rede, o que demandaria atuações positivas dos Estados para efetivar esses direitos e garantir que agentes econômicos poderosos não façam uso desses atributos para violar a liberdade econômica de utilizadores da *Internet*.

Pensemos em negócios jurídicos legalmente permitidos, que se dão por meio de um sítio digital especializado na intermediação entre compradores e vendedores. Apesar da legalidade do objeto do negócio jurídico, é possível que o sítio, lançando mão de seu poder de codificação e, através de algoritmos, não permita aquela espécie de negócio jurídico sem que existam motivações razoáveis para tanto. Apesar de contrastar com a liberdade econômica do próprio sítio digital, há que se conceber o seu poder econômico e sua utilização de forma abusiva, o que representaria o exercício do poder programacional do sítio digital para violar a liberdade econômica.

Ainda na esfera isotópica, vale citar o caso das corretoras digitais de criptomoedas, que sofreram forte abalo nos seus negócios digitais após terem suas contas em instituições

financeiras ilegalmente encerradas, impedindo o exercício de suas atividades. Trata-se de operação intimamente atrelada à *Internet*, envolvendo criptoativos que, por motivos de exercício de poder, externamente, sofrem expressiva limitação na sua liberdade econômica. Diversos casos foram submetidos à análise judicial nos diversos Estados da União, sendo um dos mais icônicos aquele movido pela empresa Walltime Ltda. em face da Caixa Econômica Federal (BRASIL, 2020), no qual foi reconhecida irregularidade no encerramento das contas bancárias, havendo, inclusive, análise do Conselho Administrativo de Defesa Econômica sobre tais casos (BRASIL, 2018), dada a potencial existência de condutas anticoncorrenciais que, portanto, violam a liberdade econômica dos utilizadores.

Dessa forma, as violações à liberdade econômica teriam forma por meio de medidas estatais ou medidas privadas, de forma que a normativa se mostra mais adequada à conotação negativa, portanto, que visa garantir a liberdade face ao Estado. Sob um prisma positivo, de medidas executivas de viabilização e impedimento às violações promovidas por entes estatais, vê-se uma atuação estritamente centrada em mecanismos isotópicos, portanto, adequados à realidade do mundo dos átomos, inexistindo mecanismos jurídicos aptos a promoverem tal direito no ambiente digital, sob um ponto de vista utópico.

Mais uma vez, relembremos os algoritmos como ponto crucial na falange violadora das liberdades sob um ponto de vista digital, considerando, também, seu impacto sob a realidade econômica. Algoritmos são capazes de produzir lesões consideráveis na liberdade econômica exercida pela via digital, impedindo o exercício de atividades lícitas ou mesmo impondo embaraços pautados em inferências inexatas que, numa óptica imediata e utópica, não são repudiáveis e não se encontram sujeitos a ditames do devido processo legal.

Citamos o exemplo do algoritmo de viés do sítio digital *Youtube*, especializado na disponibilização de vídeos, no qual os algoritmos podem impactar o nível de acesso e disponibilização dos vídeos com base em inferências acerca do seu conteúdo (KIRDEMIR et al, 2021, p. 106). Nesse sentido, a livre alocação de recursos e o exercício de atividades econômicas ficam dificultadas, impondo, portanto, afetação à liberdade econômica. Um determinado indivíduo, que produz vídeos como atividade econômica, pode ver sua liberdade econômica diretamente afetada quando um algoritmo, ao analisar a imensa coletânea de dados que compõem sua produção, retira-o do sítio, alegando possuir conteúdo que viola normas e políticas de utilização da plataforma.

Os autores (KIRDEMIR et al, 2021, p. 116), referindo-se ao algoritmo do sítio *Youtube*, compreendem a existência de algoritmos intensamente marcados por vieses, portanto, predeterminados conforme padrões programados, de forma que atuam sempre tendo um filtro

pré estipulado sobre o qual as saídas (*outputs*) já possuem uma tendência esperada, muito antes do aporte da entrada (*input*). Tal situação pode afetar as atividades econômicas desenvolvidas nessa plataforma, que se veem sujeitas a normas não previsíveis e cuja execução ocorre de forma autônoma e imediata.

Dessa forma, especialmente na era da informação, há que se considerar violações à liberdade econômica especialmente produzidas por agentes privados, com as práticas violadoras alavancando-se pela dificuldade de empreendimento por parte do Estado de medidas afirmativas de liberdade na *Internet*, o que torna tais direitos garantidos sob uma óptica negativa, no entanto, ausente de mecanismos eficientes de efetivação.

2.3 Privacidade no ambiente virtual

A privacidade mostra-se como um dos direitos humanos mais afetados no ambiente digital, especialmente considerando a ampliação dos meios de vigilância digital (SNOWDEN, 2019, p. 99-100) e a absorção social de um padrão comportamental, tipicamente marcados pela transparência (HAN, 2018, p. 88). Inicialmente, há que se considerar que o direito à privacidade aqui abordado se pauta na sua noção lata, portanto, aquela que compreende o direito à privacidade (*stricto sensu*) e o direito à intimidade. Muito embora autores denotem a intimidade como um integrante da própria noção de privacidade, partindo da distinção adotada pela Constituição Federal, opta-se por adotar tal paradigma, compreendendo o direito à privacidade “abarcando todas as manifestações da esfera íntima” (SILVA, 2005, p. 206).

Warren e Brandeis (1890, p. 193) constroem uma definição para a privacidade com base no direito de ser deixado em paz (*right to be alone*), estar tranquilo e só, em uma escala ampla, capaz de albergar todos os aspectos da vida humana que se distinguem da esfera pública e afirmam, portanto, a esfera privada.

É necessário cautela para importar as construções jurídicas do modelo consuetudinário estadunidense, no entanto, as construções dos autores mostraram-se de enorme relevância, partindo, para tanto, de uma análise que fuja de pontos de fragilidade e difícil transposição (ZANINI, 2015). Ressalta-se que a construção dos autores permitiu o entendimento de que o direito à privacidade é autônomo, apesar de manter estrita relação com a ampla proteção do direito de propriedade e a liberdade, conforme bem denotam os autores no seu ensaio teórico. Ainda assim, trata-se de um direito cuja conceituação é marcada por diversas dúvidas e imprecisões.

Pierre Kayser (1984, p. 49), partindo de construções jurisprudenciais da Suprema Corte Estadunidense, compreende o direito de privacidade como o direito de um indivíduo adotar, por si, decisões na esfera da sua vida privada, com a intimidade, por sua vez, centrando-se no direito de o indivíduo reservar informações e segredos que dizem respeito à sua pessoa do conhecimento coletivo, derivando da “*riservatezza*” do direito italiano (DOTTI, 1980, p. 115). Portanto, *lato sensu*, o direito à privacidade seria o direito dos indivíduos gozarem a vida sem qualquer embaraço e distante aos olhos de terceiros, evitando qualquer forma de confusão entre as esferas privada e pública que exponha suas informações.

A visão da privacidade estaria diretamente relacionada à noção de autonomia, que possui reflexos, também, sobre a liberdade econômica, de pensamento e de navegação (além de outras liberdades fora do escopo de trabalho). A autonomia diria respeito ao exercício da reflexão crítica de forma autodeterminante, sendo que medidas coercivas ou deceptivas acabariam por representar situações de perda da determinação do indivíduo, portanto, limitações à sua autonomia, conforme denota Dworkin (1988, p. 14). No contexto da *Internet*, dada *vênia* ao pensamento do autor, há que se considerar um contexto de exercício de poder, que retira quase a totalidade do controle pessoal do indivíduo sobre seus dados, ausentes mecanismos, dentro da óptica do poder informacional, que permitam ao indivíduo exercer controle autônomo (BERLE, 2020, p. 46).

Raymond Wacks (1989, p. 14) parte da noção de que a privacidade está diretamente associada à capacidade de controle do indivíduo sobre suas informações, uma visão que se mantém estritamente relacionada a critérios de propriedade e, portanto, atrelada a uma dinâmica técnica pouco coerente com a era da informação. A visão do autor pouco adequa-se à realidade socioeconômica da era informacional, na qual a visão estrita de propriedade é fragilizada e, além disso, surgem condições sociais, econômicas e jurídicas que alteram totalmente a capacidade dos indivíduos controlarem autonomamente suas informações.

Helen Nissenbaum (2010, p. 70) descreve a privacidade por meio de uma noção contextual de integridade, portanto, que leva em conta a totalidade do ambiente e relações que a cercam. Nesse sentido, a proteção da privacidade seria centrada em evitar que informações íntimas dos indivíduos acessassem as fronteiras externas do contexto socialmente condizente. O que se entende, portanto, é que as informações íntimas teriam sim algum âmbito de circulação fora do controle direto do seu possuidor, como uma questão inerentemente sociológica, constituindo a privacidade o direito de manter essa circulação restrita aos ambientes e/ou círculos socialmente adequados.

Nissenbaum (2010, p. 231) expõe acerca da privacidade:

Nós temos direito à privacidade, mas ele não é um direito de controlar as informações ou o direito de acessar a essas informações restritas. A privacidade trata do direito de viver em um mundo no qual nossas expectativas sobre o fluxo pessoal de informações é, na maior parte, conhecido. Tratam-se de expectativas formadas não somente pela força do hábito ou pela convenção, mas pela confiança geral no suporte mútuo desses fluxos seguindo os princípios-base da vida social, moral e política. Chama-se de integridade contextual, alcançado através do balanço harmônico das regras sociais, normas, valores locais e gerais, finalidades e objetivos.⁵⁹

Um ponto que merece ser analisado é a ideia de que a privacidade serve, exclusivamente, àqueles indivíduos que possuem “algo para esconder”. Trata-se de uma ideia má formada acerca da natureza desse direito e sua utilidade para a afirmação da cidadania. Conforme indica Dan Solove (2011), a privacidade não é sobre esconder coisas ilícitas ou que afetem os indivíduos de qualquer forma, mas sim um mecanismo para o exercício de diversos outros direitos, como o caso da liberdade de expressão, liberdade de associação e etc.

Sob essa ótica, haveria que se considerar o impacto da técnica informacional sob o contexto sociológico, efetivamente instaurando ambientes de vivência virtual que moldam as formas de manifestação das relações humanas. Dada a cultura de massas de relativização da privacidade, com a constante ampliação da transparência na rede (HAN, 2018, p. 108), há que se pontuar a existência de uma retração massiva dos padrões de privacidade, com exposições crescentes que, conforme exposto, servem a finalidade políticas e econômicas, muitas vezes ocultadas do campo de visão dos utilizadores da *Internet*.

Tratando-se de um conceito com diversas concepções, havendo autores que fazem questão de ressaltar o caráter “escorregadio” da privacidade (WHITMAN, 2004, p. 1153). Diante disso, há que se falar na necessidade de reconsiderar as definições de privacidade sob a égide da técnica informacional, averiguando, efetivamente, os pontos sobre os quais se estrutura a esfera privada e sua proteção, ao menos no nível dogmático.

Na visão de Túlio Vianna (2006, p. 73), diante de uma sociedade transparente, como a informacional, há que se reconhecer a privacidade como uma tríade formada pelo direito de não ser monitorado, o direito de não ser registrado e o direito de não ser reconhecido. Finn et al (2013, p. 4) compreende a existência de sete tipos de privacidade, com eles adequados à realidade técnica da era informacional e às novas projeções da intimidade humana. A

⁵⁹ “We have a right to privacy, but it is neither a right to control information nor a right to have access to this information restricted. Instead, it is a right to live in a world in which our expectations about the flow of personal information are, for the most part, met; expectations that are shaped not only by force of habit and convention but a general confidence in the mutual support these flows accord to key organizing principles of social life, including moral and political ones. This is the right I have called contextual integrity, achieved through the harmonious balance of social rules, or norms, with both local and general values, ends and purposes” (tradução livre).

privacidade tomaria a forma tanto da vedação ao acesso às informações sigilosas, assim como o tratamento e a utilização desses dados para finalidades políticas, econômicas, sociais e jurídicas, considerando os traços de violação à esfera privada que assumem forma na realidade informacional (FLORIDI et al, 2015, p. 165).

A privacidade da pessoa relaciona-se diretamente ao direito de o indivíduo manter seu corpo, suas funções e características privadas, tratando-se de faceta do direito diretamente ameaçada por tecnologias de reconhecimento por imagem e mecanismos biométricos. A privacidade de comportamento e ação refere-se ao direito de o indivíduo exercer, livremente, seus comportamentos, ações e hábitos fora da visibilidade pública, encontrando forte oposição por meio das tecnologias de rastreamento e vigilância. A privacidade de comunicação e a privacidade de dados e imagens refere-se diretamente ao conteúdo informacional, portanto, atrelados ao direito de o indivíduo não ter seus dados e telecomunicações interceptados por agentes estatais ou privados.

A privacidade de pensamento, conforme denotam os autores, trata-se de uma faceta da privacidade, cuja protetiva ainda é parcialmente realizada pelas limitações da técnica, tratando-se do direito de reservar seus pensamentos da visibilidade pública. Ainda assim, há que se ressaltar o impacto de tecnologias de inferência e algoritmos de análise, que permitem compreender padrões humanos por meio do processamento e análise de dados.

A privacidade localizacional diz respeito ao direito de acessar locais públicos, semipúblicos e privados sem ser monitorado e controlado. Por fim, a privacidade de associação diz respeito ao direito de se reunir e associar a outros indivíduos sem serem tais comportamentos expostos publicamente, direito que é violado por meio de algoritmos de análise de padrões de massa.

É importante considerar que, tratando-se de uma realidade imersa em dados, grande parte do conteúdo tutelado pelo direito à privacidade encontra-se manifesto sob a forma de dados digitais, *bits*, sejam eles nativos da própria rede ou aportados à rede. A protetiva do direito à privacidade sobre informações é uma questão já estabelecida tanto no domínio teórico quanto dogmático, que decorre da sua própria construção teórica. Warren e Brandeis (1890, p. 200), ao se debruçarem sobre o direito à privacidade, especificamente em resposta ao crescente avanço das mídias jornalísticas, já partia do entendimento de que a tutela da Quarta Emenda à Constituição dos Estados Unidos da América referia-se, efetivamente, ao conteúdo, não dizendo respeito à via de manifestação ou à sua propriedade. O direito à privacidade, portanto, protegeria “pensamentos, emoções e sentimentos”, sejam eles expressados por quaisquer das vias.

Partindo de um exemplo, há que se considerar que o sigilo de correspondência não se refere ao direito de propriedade da carta ou mesmo a tutela dos direitos autorais do subscritor. O que há, na verdade, é a proteção daquele conteúdo ali expresso, que diz respeito ao âmago do indivíduo. Tal situação se transporta com facilidade ao ambiente digital, de forma que os dados, em si, carregam conteúdos, muitas vezes com maior expressividade do que meios físicos de armazenamento e transferência de informações.

Diante disso, considerando a realidade que nos cerca, percebe-se que o escopo de trabalho aqui proposto se coaduna com uma dinâmica marcante, qual seja, a manifestação das informações sob a forma de dados digitais que, ao denotarem informações oriundas de pessoas naturais, assumem a definição de dados pessoais, tomando como base a própria dogmática e a sua disposição nesse sentido⁶⁰. Portanto, a violação de privacidade dentro dos ambientes virtuais ocorre, necessariamente, por meio da obtenção, captura ou processamento de dados pessoais.

Os novos padrões pautados na técnica informacional acabam por definir o ambiente digital como um espaço de transparência, não sob uma visão livre da realidade regulatória que se desdobra, mas sob a visão da existência de robustas medidas de imposição de vigilância, pautado no paradigma técnico e nos modelos socioeconômicos regentes. Acerca disso, expõem Perry e Roda (2017, p. 66):

Regramentos legais internos e externos para a proteção da privacidade encontram enorme dificuldade para seguir os passos do desenvolvimento do setor tecnológico. O uso de sistemas digitais pode engendrar um número grande de ameaças em razão de sua variedade de prolongamentos⁶¹.

Nas palavras de Byung Chul Han (2018, p. 108), trata-se de uma sociedade pautada em um modelo de panóptico digital, que se diferencia por acumular, juntamente ao amplo espectro de visibilidade e limitação da privacidade, a conexão dos indivíduos e a intensa comunicação.

Refletindo em um meio de comunicação marcado por sua densidade quantitativa e expressividade de utilizadores, a hiperconectividade da rede garante padrões de vigilância a níveis nunca antes experimentados, que se desdobram sob a forma de mecanismos de vigilância estatais e privados sobre os indivíduos no ambiente digital. Góis Júnior (2002, p. 95) indica a *Internet* como um ambiente tipicamente marcado pela violação de privacidade, enquanto uma

⁶⁰ A Lei nº 13.709/2018 define, em seu artigo 5º, I, os dados pessoais como toda informação relacionada a pessoa natural identificada ou identificável.

⁶¹ “*National and regional legal frameworks for the protection of privacy have struggled to keep pace with the breakneck rhythm of development in the technology sector. The use of digital systems may engender a number of privacy threats due to a variety of causes*” (tradução livre).

situação nata ao modelo informacional por ela empreendido, estando tal situação ainda atrelada à vastidão dos seus meios, a dificuldade regulatória e o alto grau de anonimato que existe.

Um dos pontos base para a compreensão da violação à privacidade no ambiente virtual é entender a derrocada das balizas diferenciadoras da esfera pública e da esfera privada, inaugurando um ambiente que, por meio da técnica, permitiu a sobreposição de esferas de transparência aos âmbitos de proteção da intimidade. Trata-se de fenômeno decorrente de uma série de questões, dentre elas, questões psicológicas naturais do ser humano, expansão das formas de controle e abdução dos indivíduos pelos padrões culturais massificados, sendo a ascensão da era digital um fenômeno catalisador, que foi possível desenvolver e aplicar “mecanismos cada vez mais capazes de romper as já esmaecidas divisas entre a esfera pública e privada (RODRIGUES; MARCHETTO; BARRIENTOS-PARRA, 2019, p. 507).

Os vanguardistas Warren e Brandeis (1890, p. 195) já compreendiam a expansão dessa dinâmica muito antes da era informacional, propondo teorização sobre o direito à privacidade e intimidade em resposta ao fenômeno da massificação jornalística do fim do século XIX, denotando uma escalada progressiva que, sob a análise proposta, alcança seu ápice junto ao mundo dos *bits*, com violações cada vez mais eficientes e menos visíveis aos utilizadores. Os autores entenderam pela existência de uma relação estrita entre a privacidade e a tecnologia.

As violações à privacidade, portanto, não são uma questão da era informacional, no entanto, assumem notoriedade em razão de seu caráter omnipresente e proeminente, que atinge quase a totalidade dos aspectos da vida humana (BERLE, 2020, p. 41). Paul Armer (1975, p. 13), já na década de 1970 ressaltava a potencialidade dos impactos da violação à privacidade e à liberdade humana em semelhante passo, ao incremento da técnica computacional. Nesse sentido, trazendo a visão icônica de Balkin (2004, p. 2) sobre os impactos do fenômeno da *Internet* sobre as relações socioeconômicas, e, por consequência jurídicas, há que se ver como a tecnologia virtual salienta as violações de privacidade.

Grande parte dos espaços virtuais, sítios e aplicações digitais que compõem a rede mundial de computadores mostram-se ausentes de mecanismos regulatórios eficientes, capazes de executar a garantia e a efetivação da privacidade dos utilizadores (PERRY; RODA, 2017, p. 64). Tal situação se coaduna perfeitamente com os chamados espaços alegais, teorizados por John Laprisse (2013), que denotam ambientes que, em razão da diferenciação técnica e fragilidade dos mecanismos institucionais, sofrem com a ausência de mecanismos de exercício de controle institucionalizado, portanto, ausentes medidas estatais capazes de garantir e efetivar direitos humanos. Abre-se espaço para que os Estados promovam atividades ilícitas de

vigilância e censura, com correlatas atividades por parte dos agentes privados, que promovem violações à privacidade com objetivos econômicos.

Nesse sentido, (MARCHETTO; BARRIENTOS-PARRA; RODRIGUES 2019, p. 512):

A alegabilidade, portanto, denota um domínio digital livre, incapaz de sujeitar-se às dinâmicas diretas de controle do Estado, mas, além disso, conforme denota John Laprise, trata-se de um ambiente no qual o Estado tem a liberdade de agir conforme seus interesses, sem amarras legais que possam impedi-lo de lesionar direitos.

Governos e empresas, conforme indicam diversos autores, possuem uma atuação conjunta para monitorar e realizar controle sobre os utilizadores da rede, exercendo tais práticas de forma oculta, por meio de algoritmos e sistemas camuflados de vigilância⁶². O Estado, na grande maioria das vezes, empreende vigilância com objetivos políticos, especialmente centrados no controle dos indivíduos, prevenção de criminalidade e terrorismo e outras situações relacionadas às suas finalidades precípua⁶³ (chamado de *security tracking*).

A atuação das empresas, por sua vez, é centrada nas questões econômicas, portanto, melhoramento de modelos de negócios, venda de produtos informacionais, vendas de dados e processamento, terceirização de atividades de vigilância estatal, dentre diversos outros (chamados de *comercial tracking*). Shoshana Zuboff (2019, p. 14) indica a ascensão de um modelo capitalista de vigilância pautado na violação da privacidade humana, fazendo o uso de dados humanos “como matérias-primas para a compreensão de comportamentos” e emprego de práticas de mercado.

O acesso às informações dos indivíduos, em dinâmica violatória à privacidade, alcança seu maior nível em toda história humana (CHESTERMAN, 2011, p. 251), sendo elas usadas em constantes medidas orientadas a finalidades políticas e econômicas, de forma que o exercício de poder, por meio da via digital, considerando o poderio informacional desses agentes, excede absurdamente o consentimento público (BERLE, 2020, p. 48).

Narayanan e Shimitov (2009, p. 175-176) indicam uma enorme dificuldade na garantia da privacidade e anonimato na rede diante da presença de dados pessoais no ambiente digital, sugerindo o ambiente digital como propício a ataques à privacidade. Os mesmos autores

⁶² Citamos, como exemplo, o Sistema Pegasus, produzido pela Agência de Inteligência Israelense, recém divulgado pela ONG *Forbidden Memories* e pela Anistia Internacional como um dos casos mais extremos de vigilância digital. Trata-se de um sistema pautado em uma atuação viral, ou seja, infecta dispositivos eletrônicos de forma sorrateira, capotando, ilegalmente, mensagens, fotos, e-mails, além de gravar áudios, enviar alertas e obter imagens, tudo isso sem conhecimento do utilizador (ANISTIA INTERNACIONAL, 2021).

⁶³ Além do caso narrado, podemos trazer à discussão a vigilância empreendida pelos Estados durante o controle da pandemia de COVID-19, na qual foram utilizados diversos mecanismos de afetação à privacidade para controlar a disseminação do vírus e realizar controles sanitários (RODRIGUES; MARCHETTO, 2020).

(NARAYANAN; SHIMITOV, 2008, p. 113-114) indicam a fragilidade do indivíduo no ambiente digital, demonstrando como banco de dados distintos, e sem quantidades massivas de dados pessoais, podem ser cruzados e projetar efeitos expressivos sobre a privacidade dos utilizadores.

Definidas as facetas do direito de privacidade dentro da era da informação e suas principais formas de violação, intermediados pelo ambiente da *Internet*, há que se pontuar as principais origens dessas ameaças, indicando as fontes e os motivos pelos quais o direito de privacidade é afetado digitalmente. Conforme descrevem Perry e Roda (2017, p. 68), a base das violações de privacidade advêm de quatro dinâmicas básicas, sobre as quais podem ser compreendidas a totalidade dessas manifestações no ambiente virtual, fragilidades no gerenciamento de dados, erros humanos e, por fim, ações não autorizadas de coleta e distribuição de dados.

As fragilidades no gerenciamento de dados referem-se às falhas na preservação de informações privadas por parte do indivíduo ou qualquer um que tenha acesso a ela e tenha o dever de garantidor da sua integridade, muitas dessas falhas ligadas a situações de vulnerabilidade dos utilizadores da rede. Especificamente as ações não autorizadas de coletas se referenciam às intrusões, invasões forçadas da privacidade, interceptação de informações, indicam o acesso não autorizado a dados privados por meio de práticas de espionagem (KIZZA, 2017, p. 95-96).

Um ponto que merece atenção, apesar de não compor uma forma direta de violação de privacidade, é o empreendimento de práticas de visibilidade social e auto exposição da vida privada, questões relacionadas, diretamente, à massificação cultural no ambiente da *Internet*, que expõem uma visão considerável acerca da fragilização da privacidade (PERRY; RODA, 2017, p. 76). Falque-Piorretin (2020, p. 9) expõe essa questão com clareza, indicando o empasse entre os benefícios criados pelas redes sociais e os seus malefícios à privacidade:

A influência crescente das tecnologias da informação e da comunicação sobre a organização da sociedade chega ao ponto que a norma do “todos conectados” parece ser irresistível e irreversível. (...) A explosão no uso das redes sociais, que contribuem mais e mais à expressão do indivíduo e, também, são mais e mais consumidoras de dados pessoais.⁶⁴

Diante de uma efetiva revolução social, conforme entende Dominique Cardon (2020, p. 12), os indivíduos veem-se social e culturalmente vinculados a ambientes digitais de exposição,

⁶⁴ (tradução livre).

numa clara dinâmica de transparência, que denota a realidade informacional que nos cerca (HAN, 2018, p. 107). As noções de informação privada assumem conotação demasiadamente etéreas, considerando o estímulo socioeconômico à ampliação das áreas de vasão da intimidade (PERRY; RODA, 2017, p. 76), situação que, por si, impede uma compreensão plena dos valores da privacidade e sua utilidade à dignidade humana.

A afetação à privacidade, por meio da cultura de exposição nascente com a democratização do acesso à *Internet*, decorre não somente de uma vigilância promovida por agentes de poder, mas uma exposição que, em razão dos padrões derrocados de privacidade, pode ser exercida por outros indivíduos. Cardon (2020, p. 13), em referência à icônica ficção de Orwell, indica o fenômeno sociológico da vigilância pelos iguais na era da informática como “*Big Other*” ou vigilância lateral, em um modelo de panóptico digital centrado na hiperconexão.

Os dados assumem cada vez mais valor no contexto da técnica informacional, seja esse valor econômico, político, social ou cultural, de forma que a sua coleta e armazenamento assumem proporções expressivas. Nesse sentido, Berle (2020, p. 44) compreende que a realidade digital instaurou um novo contrato social, que é tipicamente por nós presenciado durante a vivência digital. Conforme descreve o autor, a vida no mundo dos *bits*, dentro do socialmente esperado e adequado aos padrões comuns, depende da cessão, captura, processamento e armazenamento de dados privados.

O modelo jurídico estadunidense de proteção da privacidade pauta-se na voluntariedade das partes, conforme indicam icônicas jurisprudências da Suprema Corte⁶⁵, situação um tanto quanto displicente com relação ao ambiente digital que a sociedade se insere. Dentro de uma sociedade informacional, dotada de mecanismos algorítmicos, procedurais e arquitetônicos de controle e vigilância, sem possibilidades de oposição (auto executivos), não há que se omitir regulação sobre essa técnica e acreditar na voluntariedade das partes em zelar pela sua privacidade, de forma que a auto exposição se apresenta como um fator não jurídico, mas que produz efeitos relevantes na esfera do direito, especialmente considerando as afetações intrincadas à privacidade.

Tal situação traz uma relevante discussão jurídica, especialmente considerando que alguns autores apontam a privacidade, portanto, o conteúdo protetivo do direito à privacidade, como uma questão valorada pelo contexto, não possuindo um valor intrínseco (BERLE, 2020, p. 70). Nesse sentido, a realidade digital imporia circunstâncias diferentes à tutela da privacidade, reduzindo em muito a esfera protetiva, em razão de suposta alteração na noção de

⁶⁵ Katz v. United States (EUA, 1967, p. 361); United States v. Knotts (EUA, 1983, p. 277); Smith v. Maryland (EUA, 1979, p. 736); United States v. Miller (EUA, 1976).

privacidade, podendo considerar, por exemplo, as exposições “voluntárias” dos indivíduos junto à rede. Berle (2020, p. 70) compreende, com razão, a utilidade de um conceito de privacidade útil à realidade jurídica, capaz de identificar casos que efetivamente demandam proteção e, assim, justificam a incidência da protetiva, refletindo na não interferência para a proteção de qualquer evento tido como indesejável.

No entanto, há que se compreender a cooptação da realidade digital pelos agentes de poder, empregando mecanismos efetivos para incentivar indivíduos a, autonomamente, esporem seu âmbito privado, o que indicaria uma possível limitação à noção da privacidade como dotada de relevância conceitual. Rodrigues, Marchetto e Barrientos-Parra (2019, p. 511) compreendem que existem relevantes exposições por parte dos próprios utilizadores da rede que não são autônomas, denominadas pelos autores como exposições “semi-voluntárias”, por envolver uma falsa percepção de liberdade e, ao mesmo tempo, impondo padrões de exposição como condições à utilização de domínios digitais e aplicação. Há que se considerar a existência de termos de uso e políticas de privacidade no ambiente digital que são opressivos à privacidade e segurança dos utilizadores (ZUBOFF, 2019, p. 13), de forma que alguns serviços ou aplicações, usualmente necessárias no atual estágio da vida moderna, têm sua funcionalidade vinculada à aceitação das práticas de vigilância.

Citemos o exemplo de um sítio digital que exija que, para o acesso ao seu conteúdo, o utilizador concorde, expressamente, com termos de uso leoninos, que impõem a captação de dados. Surge para os utilizadores da rede um dilema constante no atual estágio da técnica informacional, a escolha entre ceder informações pessoais ou não as ceder e, por consequência, não obter os serviços, conteúdo ou produtos pretendidos na rede (PENG, 2014, p. 4). Shoshana Zuboff (2019, p. 13) cita o exemplo de um termostato digital vendido para o aquecimento doméstico nos Estados Unidos da América, cuja não aceitação dos termos de processamento dos dados e ausência de conexão com a *Internet* não só impediria o funcionamento normal do aparelho, mas também poderia levar a sérios problemas de funcionamento, portanto, forçando os utilizadores a concordar com tais práticas.

Não somente isso, há que se falar na indisponibilidade dos direitos humanos, de forma que adotar padrões mais permissivos junto à *Internet*, para autorizar ameaças à privacidade dos utilizadores, representaria clara relativização dos direitos e da dignidade humana. Há que se falar, portanto, que, apesar do ambiente digital prover alterações robustas na noção de privacidade, é necessário manter níveis de proteção dos direitos humanos dentro dos padrões de tutela marcados pela indisponibilidade e não retrocesso, concebendo ponderações entre direitos em casos que tal medida se faça necessária e seja legítima.

Especificamente na questão da privacidade, Berle (2020, p. 119) entende que haveria a possibilidade de limitações ao direito de privacidade quando cumpridos alguns requisitos mínimos pelo Estado. Nesse sentido, caberia somente ao Estado promover tal ponderação e adotar medidas de limitação à privacidade, sendo inviável tal medida quando proveniente de agentes privados.

Segundo o autor, a legitimidade de medidas de limitação à privacidade, tipicamente medidas de vigilância e interceptação de dados, seriam viáveis quando existente necessidade devidamente comprovável e proporcionalidade, de forma a evitar medidas intrusivas capazes de reverberar sobre outros direitos humanos. Além disso, haveria que existir medidas adequadas de devido processo legal, haja vista a necessidade de limitações aos direitos ocorrerem por tal via, além da transparência das medidas e estruturação de protetivas contra a reutilização desses dados ou empenho a outras finalidades que não aquelas exasperadas.

Há que se considerar um outro fator a ser levado em conta ao referir-se às dinâmicas básicas, que permitem violações de privacidade no mundo dos *bits*, a vulnerabilidade técnico-informacional. A vulnerabilidade técnico-informacional diria respeito a indivíduos ou grupos que possuem hipossuficiência técnica no ambiente da *Internet*, portanto, não possuindo mecanismos técnicos hábeis para se opor às medidas violadoras engendradas pelos possuidores do poder programacional. O ambiente virtual é composto por sistemas complexos, marcados por constantes transformações, com interações complicadas, o que tira dos utilizadores a sua capacidade de controlar sua própria informação (ROUSSEAU; SAUREL, 2014, p. 77).

Uma diferença básica entre estruturas tecnicamente capazes de engendrar poder por meio de seus aparatos e pessoal autorizado. Trata-se, assim, de uma desigualdade computacional, na qual Estados e grandes empresas contam com um anteparo de poder econômico que os provê expressiva capacidade de estruturar espaços e processos virtuais que sequer são percebidos pela grande massa, que possui reduzido conhecimento computacional e poder econômico abreviados. Pode-se afirmar que seria a referida vulnerabilidade a base sobre a qual se estrutura a algocracia, na qual os avanços tecnológicos são tão expressivos e concentrados nas grandes figuras da *Internet* (Estados e grandes Empresas), que estruturam formas inovadoras de violação à privacidade e, fragilizados, não resta opção aos utilizadores senão sujeitarem-se a essas dinâmicas ou, ainda, nem mesmo tomar conhecimento delas.

Sendo a rede mundial de computadores um espaço que permite a adoção de modelos regulatórios próprios e nativos, fala-se na concentração do poder em estruturas que os utilizam de forma não democrática, com a concentração do poder de gestão e arquitetura da rede em

esparcos agentes, que possuem, assim, o poder para regular o ambiente digital e impor modelos algorítmicos de dominação e violação de privacidade.

Nas palavras do filósofo da técnica Bernard Stiegler (2020, p. 18), a estrutura da técnica algorítmica figura como uma nova forma de governamentalidade, especificamente atenta à dinâmica dos algoritmos, tendo como ponto fundamental a atuação da big data⁶⁶ e seu efeito sobre o indivíduo e sua privacidade. Segundo o autor, a atuação de sistemas robustos de processamento massificado de dados favorece a adoção de uma visão comportamental centrada em números, que permite aos gerenciadores desses sistemas antecipar comportamentos, riscos e oportunidades, criando padrões de vigilância que afetam não só a privacidade dos indivíduos, mas também a sua liberdade de pensamento, econômica e de navegação, isso sem falar nas liberdades consideradas sob a visão isotópica.

Portanto, alguns agentes possuem capacidade e conhecimento para regular e controlar as estruturas da *Internet*. Essa concentração do poder acaba por dar uma vantagem expressiva a tais entes, que fazem tal vigilância quase à total revelia ou submissão dos utilizadores. Não somente isso, há que se considerar também a vulnerabilidade técnica das normativas, que, em sua grande maioria, foram providas antes da ascensão da era da técnica informacional, o que significa que, apesar da neutralidade técnica de grande parte das normas de direitos humanos, existem dificuldades estruturais relevantes que dificultam a tutela e efetivação da privacidade.

Pensemos que a Constituição Federal foi promulgada em 1988, enquanto a Declaração Universal dos Direitos Humanos foi estabelecida em 1948, o que significa que seus meios não se aderem com perfeição aos padrões técnicos atuais, conforme bem indicam Perry e Roda (2017, p. 71). Nas palavras de Berle (2020, p. 45), a maior parte das protetivas legais datam do século XIX e XX, indicando uma incapacidade de responder efetivamente às novas ameaças à privacidade e à nova realidade sociocultural e econômica.

A dificuldade de o direito promover uma tutela efetiva sobre a privacidade na rede, conforme já apontado sob um caráter geral, adviria da questão técnica regente que, ao demandar a aplicação da dogmática sobre determinadas relações regidas por dinâmicas técnicas divergentes, sofre com o fenômeno da refração jurídica.

Ainda que se referindo às normas especificamente dispostas à regulação do ambiente digital, como o caso da Lei nº 12.965 de 2014 e da Lei nº 13.709 de 2018, percebe-se uma relativa adaptação técnica, uma vez que, apesar de prover normas materialmente adequadas às condições técnicas do ambiente virtual, não conta com mecanismos aptos à garantia e efetivação

⁶⁶ Big Data trata-se de um modelo de análises, tratamentos e informação, que se pauta em grupos expressivos de dados, portanto, o tratamento massificado de dados (CHEN et al, 2014, p. 171).

da privacidade na *internet*, dependendo de uma série de condições, estritamente focadas em medidas pós-violatórias, para empreender medidas reparatórias. Portanto, apesar de, sob o ponto de vista material, serem relativamente condizentes, ainda há robustas falhas procedimentais na sua tutela e efetivação.

Portanto, sob essa dinâmica, as normativas, mesmo quando adequadas, sofreriam com certas fragilidades técnicas, o que refletiria na possibilidade de mais violações de direitos humanos na *Internet* e menos medidas de efetivação eficientes. Apesar de existirem normas e sua vinculação, os procedimentos para averiguação, constatação e efetivação dos direitos fica efetivamente inviabilizado pela extensão da rede, massa de utilizadores e, além disso, o empreendimento de espaços tecnicamente adequados e ocultos que impõem afetações aos direitos humanos, em especial a privacidade. Espaços como o da alegabilidade, manifestados em dinâmicas de vigilância adotada por empresas e Estados, permitem a compreensão de que, apesar da dogmática prover mecanismos com determinada adequação técnica, há ainda sérias fragilidades estruturais no ordenamento jurídico, especialmente considerando seus mecanismos de execução.

Ao mesmo tempo em que a norma tutela o sigilo telefônico e impõe diversas exigências para o seu acontecimento, há a adoção massiva de medidas de vigilância por meio de *smartphones*, que possuem total acesso às conversas e demais dados, com conexão quase integral com a rede (MARTÍNEZ-BEJAR; BRÄNDLE, 2018, p. 142). Indo além, ao mesmo tempo que a Lei nº 13.709 de 2018 impõe limitações à captação e utilização de dados pessoais, percebe-se a existência de práticas empresariais e estatais constantes que fogem das dinâmicas de controle e empreendem violações à privacidade digital dos utilizadores.

Ainda assim, há que se reconhecer a existência de medidas isotópicas, portanto, empreendidas no ambiente físico, que promovem reflexos diretos no ambiente digital, especialmente considerando a questão da privacidade. Vale trazer à tona o icônico caso da Ação Direta de Inconstitucionalidade 6.389, movida em face da Medida Provisória nº 954 de 2020, que dispunha sobre a transmissão de dados comunicacionais ao Instituto Brasileiro de Geografia e Estatística (IBGE), na qual foi provida liminar suspendendo sua eficácia, em razão da vagueza da medida e das possíveis implicações desta à privacidade dos utilizadores.

Trata-se de um caso envolvendo a vigilância massiva empreendida pelo Estado através de um ato normativo, situação que, de fato, permitiu maior cognoscibilidade da sociedade e a incidência dos mecanismos jurídicos usuais, situação que se mostra muito diferente àquela constatadas em violações à privacidade pontuais e realizadas por práticas ocultas, como aquelas praticadas por diversos Estados e denunciadas pelos vazamentos do *Wikileaks*, que indicam

práticas ocultas, imperceptíveis e com mínimo potencial de incidência de medidas reparatórias por parte do direito estatal (PELL; SOGHOIAN, 2014, p. 23-26).

Ainda assim, há que se considerar práticas de vigilância institucionalizada pelo Estado e à margem dos liames de dignidade humana, que se assentam sobre o ambiente digital e garantem uma expressiva projeção. Vale trazer o caso norte americano da Corte Estadunidense de Inteligência e Vigilância (FISA), um tribunal, tido por autores como de exceção, que julga, de forma secreta, as situações de vigilância externa dos Estados Unidos da América e expede autorizações. Trata-se de um tribunal com regimentos autônomos e que não atende ao devido processo legal, empreendendo autorizações para vigilância à mercê da proteção da dignidade humana e que não pratica qualquer controle sobre as medidas de vigilância empreendidas pelas diversas agências estatais (MAYER, 2002, p. 250).

Portanto, as autorizações para o empreendimento de medidas de vigilância externa, nos Estados Unidos da América, ocorrem através de um tribunal oculto que, atuando com estrita vinculação ao poder executivo, pode autorizar essas medidas, sem se adequar minimamente aos padrões de devido processo legal e a condições para legitimar a limitação de direitos.

Tal problemática se adensa quando vislumbramos a atuação primária dos mecanismos de vigilância por intermédio da *Internet*, de forma que as violações, mesmo que sujeitas à densidade informacional, que vige no ambiente da *Internet*, não alcançam o conhecimento público e, na sua grande maioria, não produzem efeitos imediatos no ambiente físico. Portanto, as violações tomariam uma forma primordialmente existente no ambiente informacional, sem necessária correspondência no ambiente físico, o que cria, conforme já expressado, um problema de incapacidade e inefetividade do direito estatal, especialmente sua capacidade técnica de garantir sua exequibilidade nas vias digitais.

Nesse sentido, apesar de dogmáticas adequadas e capazes de compreender minimamente a técnica informacional, como o caso da Lei nº 13.709 de 2018, a Lei Geral de Proteção de Dados (LGPD) e a GDPR⁶⁷, no âmbito europeu, normas especificamente voltadas à gestão das medidas de processamento dos dados pessoais, portanto, práticas que efetivamente confrontam o direito à privacidade dos utilizadores. Apesar da coerência e capacidade de produzir efeitos sob a forma de medidas isotópica, ou seja, por meio da atuação sobre o mundo físico de forma a produzir efeitos no ambiente digital, ainda assim há sérias fragilidades quando pensamos na extensão das violações de privacidade que ocorrem à revelia dos utilizadores da rede. Portanto, o direito à privacidade, dentro da dinâmica usual, não contaria com formas de tutela

⁶⁷ Regulamento Geral sobre Proteção de Dados.

especificamente adequadas à realidade digital, depositando suas funcionalidades sobre o funcionamento do sistema jurisdicional e executivo do Estado, tecnicamente adequado a uma dinâmica distinta.

Abordando a Lei nº 13.709 de 2018, percebe-se que, alinhado com as demais normas produzidas para a regência do ambiente virtual, há a adoção de mecanismos jurídicos adequados ao padrão técnico industrial e, portanto, incoerente com uma dinâmica informacional. A norma, de fato, traz uma visão sobre os dados pessoais, objeto material da tutela do direito de privacidade, que indica uma melhor aceção da realidade técnica. Ainda assim, sua estruturação se pauta em modelos pós-violatórios de reparação, com estritos dispositivos regendo a tutela da privacidade de forma nativa ao ambiente digital, estruturando mecanismos de fiscalização e sanção com ditames claramente distantes daqueles reinantes na era informacional. Sugere-se, portanto, uma clara fragilidade frente aos padrões programacionais adotados por agentes privados dotados de poder na rede, indicando a possibilidade das medidas ativas do Estado, na efetivação do direito de privacidade, mostrarem-se inefetivas ou sem eficácia prática, especialmente considerando a dinâmica oculta dos algoritmos.

Ressalta-se que, alinhado à fragilidade da tutela da privacidade por parte do Estado, enquanto garantidor da devida adequação dos agentes privados aos padrões de dignidade normativamente dispostos, percebem-se lacunas graves na imposição de limitações ao Estado, especialmente considerando o caráter abstrato das restrições à sujeição aos termos da norma (dispostas no artigo 4º). Exemplificando, o inciso III do artigo 4º, especificamente nos itens “a” a “d”, estipula os casos de não aplicação das regras de tratamento⁶⁸ de dados pessoais atrelados à segurança pública, segurança do Estado e defesa nacional, situações que são vagas e, conforme indicam diversos autores, são motivos facilmente levantados para justificar invasões ilegítimas à privacidade dos utilizadores da *Internet* (PELL; SOGHOIAN, 2014, p. 27-29); (LIPPERT; NEWELL, 2016, p. 113).

Tratando-se de dados distantes das protetivas de normativas mais estritas, como o caso das normas de tutela do sigilo telefônico ou epistolar, e que estejam fora das já estritas dinâmicas protetivas da legislação de proteção de dados pessoais, há práticas de captação direta de dados e seu processamento pelo Estado, seja por suas agências e órgãos ou mesmo pela atuação de empresas privadas que atuam como *longa manus* das medidas de vigilância

⁶⁸ Tratamento de dados, nos termos do inciso X, do artigo 5º, da Lei nº 13.709/2018, diz respeito a “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração”.

(MÁRTINEZ-BEJAR; BRANDLE, 2018, p. 145). Esses dados, no caso brasileiro, estariam distantes das exigências de devido processo legal para que ocorressem, indicando efetivo abuso do poder programacional exercido pelo Estado, evidenciado na forma de violação ao direito à privacidade.

O que chama a atenção é a disciplina, de forma pouco específica e sem indicativos de aplicação, de medidas nativas à rede para a tutela da privacidade, conforme dispõe o §2º do artigo 46 da LGPD. Trata-se do chamado modelo *privacy by design*⁶⁹, que estipula a necessidade dos sistemas digitais concebidos e executados, já com padrões de privacidade inculcados, portanto, nativos ao seu sistema, que independam de práticas fiscalizatórias e efetivadoras por parte do Estado ou qualquer outro agente. Cita-se, desde já, a adequação da grande maioria das *Blockchains*, sistemas *DLT* e criptoativos aos padrões de privacidade por definição.

Sumarizando, as violações à privacidade ocorreriam através de atuações de entes estatais e privados, empreendendo mecanismos de vigilância digital para a captura de dados pessoais no ambiente virtual, seja por meio de dinâmicas mediadas por atores ou por meio do intermédio de algoritmos. Essas violações tomariam dimensões massivas, considerando a quantidade de utilizadores, as dinâmicas expressivas de captação de processamento de dados, além da facilitação dos mecanismos coletivos de vigilância.

Há que se considerar que a Assembleia Geral da ONU, por meio de uma resolução (ONU, 2014), reconheceu o direito à privacidade como uma ferramenta viabilizadora de outros direitos, especialmente considerando a realidade digital, situação que denota a gravidade das violações sobre esse aspecto da dignidade humana. Nesse sentido, violações à privacidade, além de afetarem diretamente a esfera íntima do indivíduo, imporiam demais impactos sobre a liberdade em todos seus aspectos, o que indica, considerando a majoritária afetação aos direitos de privacidade no ambiente virtual, que se trata de uma ofensa ampla à dignidade humana, alcançando direitos outros.

Em face disso, encontrando uma realidade cujas afetações se estendem sobre diversos direitos humanos, há que se considerar a inadequada atuação dos meios usuais de garantia e tutela dos direitos, que assumem conotação individualizada e não produzem efeitos conjugados e capazes, portanto, de tutelar direitos correlatos simultaneamente de forma eficiente, situação

⁶⁹ Trata-se de um conceito desenvolvido por Ann Cavoukian (2011), Comissária de Informação e Privacidade de Ontário, Canadá. Considerando a previsível expansão dos mecanismos de coleta de dados, entendeu a comissária pela necessidade de imposição de padrões técnicos adequados àqueles meios, para que eles fossem naturalmente tendentes à preservação da privacidade dos utilizadores.

essa alargada pela ausência de uma tutela coletivizada, que se centra em violações singularmente concebidas.

2.4 Conclusões Parciais

Comparada a hipótese primária atribuída a esta seção do trabalho, percebe-se uma relativa aproximação com os objetivos alcançados pela abordagem dedutiva da temática, que foi capaz de direcionar a seção aos objetivos pré-definidos. A hipótese primária indicava o potencial lesionador das diretivas originadas na *Internet* sobre os direitos humanos existentes nesse meio, especialmente atendendo à análise da afetação à liberdade e à privacidade.

Pelas análises teóricas feitas, percebe-se que há efetiva recomposição do ambiente digital, com a estruturação de novas forças motrizes que, por sua vez, regem as dinâmicas regulatórias e também as práticas de vivência humana. Sob a égide de novas formas de manifestação do poder, no caso o poder programacional, percebe-se a ascensão de um modelo jurídico com potenciais robustos de violação à legitimidade do poder, adquirindo conotações de um poder de fato pouco coerente com a tutela dos direitos humanos.

O poder programacional, como aquele regente no espaço da *Internet*, assume uma dinâmica fora da ordem jurídica usual e dos seus liames democráticos, evidentemente marcado por práticas que afetam a dignidade dos utilizadores e, em sua grande maioria, não têm qualquer fundamento na supremacia do povo.

Portanto, o poder programacional nasce como uma força escassa e, principalmente, manifestada junto ao seio econômico e político da sociedade, como uma força que molda sua própria realidade, portanto, tem dinâmicas arquitetônicas sobre a rede, efetivamente estruturando os espaços digitais e as formas pelos quais se dão toda existência virtual. Nesse sentido, seria o poder digital uma força tecnicamente adequada à rede, capaz de projetar sua exequibilidade através de mecanismos próprios da dinâmica virtual, como o caso dos algoritmos auto executivos.

Partindo dessa construção, a realidade virtual teria suas dinâmicas violatórias de direito manifestadas através do exercício do poder programacional, haja vista a estrita relação entre a lesão de direito e o exercício de uma forma de poder. Os Estados ou agentes privados, portanto, atuariam na rede violando direitos humanos dos utilizadores, que, sob um ponto de vista utópico e tecnicamente adequado, existem na rede e não somente se manifestam ali.

Apresentado esse ponto, há que se considerar a fragilidade do direito estatal em regular questões digitais, especialmente abordando as normas de tutela de direitos humanos, seja pela

sua já dificultosa atuação ou seja pela sua marcante distinção técnica, que demarca uma enorme lacuna entre a efetivação de direitos na *Internet* e a positivação de direitos na dogmática. Portanto, haveria normas tecnicamente inadequadas, incapazes de materialmente disciplinar a tutela de direitos, e, além disso, uma marcante inadequação técnica de todo o ordenamento jurídico, demonstrado pela dificultosa ou inexistente exequibilidade digital de suas garantias e efetivações de direitos humanos. Haveria, portanto, um confronto entre o poder regulatório estatal, relativizado e tecnicamente incoerente, e os códigos, normas regentes do ambiente virtual, marcados pela autoexecutoriedade e dificultoso repúdio.

A questão do repúdio à prática normativa, exercida pela arquitetura da rede, demanda maior extensão, dada sua utilidade para compreender o efeito da incapacidade estatal de efetivação de normativas no ambiente virtual. Ao passo que o ambiente físico e a regulação estatal permitem um repúdio às práticas, por meio da atuação controladora e balanceada do judiciário ou de práticas executivas do Estado, o ambiente virtual teria uma regulação silenciosa e oculta ao campo de visão, apesar de ter sua presença reconhecível. Ainda assim, em ambos os casos, falar-se-á de uma atuação pós-violatória, pouco adequada a uma visão preventiva, que se torna ainda mais escassa, considerando as características pouco visíveis das dinâmicas de violação de direitos na *Internet*.

Faz-se questão de indicar que haveria situações marcantes que, em razão de uma capacidade isotópica de afetação, permitiria a incidência do direito estatal sobre o ambiente virtual para a tutela de direitos humanos, tratando-se de situação na qual o poder do Estado se manifesta sob a forma programacional ou é capaz, ainda, de lançar mecanismos e intermediações que garantem alguma forma de exequibilidade.

Portanto, reconhecida a crise de legitimidade na *Internet*, passa-se à discussão da crise de legalidade. É necessário chamar atenção ao fato de que regulações não deixam de incidir sobre a *Internet*, em nenhum momento alcançando um status de “anarquismo absoluto”. A situação que ocorre é uma efetiva redução da capacidade de afetação do direito estatal sobre a *Internet* e, considerando a dinâmica responsiva das forças regulatórias, permite a ascensão de novas modalidades de regulação, como o caso da regulação arquetônica, costumeira ou econômica. Não haveria uma crise de legalidade na *Internet*, mas sim uma crise da legalidade estatal, com as devidas ressalvas à sua extensão, principalmente em razão de contextos isotópicos de aplicabilidade do direito.

A remodelação da legalidade digital e a chamada crise da legitimidade do poder no ambiente digital reascendem a questão da dualidade átomo-bit, permitindo compreender que a garantia e tutela dos direitos humanos marca-se por uma distinção quando transita do espaço

físico para o virtual, denotada, especificamente, pela afetação técnica do direito, seja a dogmática, sua estrutura base do ordenamento e suas dinâmicas de exequibilidade. Nesse sentido, o meio virtual constitui estruturas de poder sem compromisso com a garantia da dignidade humana, estruturando regulações que fogem da hermenêutica constitucional e, ainda mais, atuando efetivamente como mecanismos lesivos.

Foi visto, no decorrer da pesquisa da hipótese inicial, que a crise de legalidade, de fato, não se manifestava como a pesquisa preliminarmente indicava. No entanto, a crise de legitimidade mantém-se e demonstra ser um dos principais problemas causadores da ausente proteção de direitos no meio virtual, enquanto a ausência de estruturas adequadas à tutela dos direitos no ambiente virtual, instaurando uma necessária correlação da vida digital ao mundo físico.

É indicado, considerando a realidade técnica e as construções históricas, o processo de luta para a composição de novos direitos, como o caso da liberdade de navegação, padrão de dignidade humana, que assume especial condição no meio virtual. As demais formas de liberdade e a privacidade, por sua vez, sofrem também com alterações nos seus padrões, considerando o contexto técnico.

Portanto, haveria no ambiente digital uma situação de marcante lesão à privacidade e à liberdade humana, lesões estas que possuem escassas medidas junto à rede, para garantir e efetivá-los, especialmente considerando uma fragilidade do direito estatal e até mesmo do direito internacional protetivo dos direitos humanos, diante de um fenômeno de refração jurídica. As violações aos direitos humanos tomariam, portanto, a forma de práticas de vigilância, com afetação direta à privacidade, e controle, com afetação direta à liberdade, especialmente considerando o efeito sobre os demais direitos.

Cumprе ressaltar que a liberdade e a privacidade estariam intimamente ligadas aos direitos de segunda geração, manifestando-se como forma essencial à efetivação desses direitos relacionados à dinâmica social. Especialmente considerando direitos como a liberdade de navegação, aqui indicada como um amálgama de liberdades manifestas no ambiente da *Internet*, percebe-se a especial relação entre a *Internet*, o direito à educação, considerando o potencial de ampliação da capacidade de sorção de conhecimento de forma gratuita e livre, o direito ao trabalho, direito à saúde e diversos outros direitos.

Haveria, portanto, uma exacerbação de diversos outros direitos no ambiente digital, que também sofreriam com o poder programacional atuando de forma deslegitimada, produzindo lesões a tais direitos, que, dado o escopo do trabalho, não demandam maior explanação.

CAPÍTULO 3 BLOCKCHAINS, CRIPTOATIVOS E TECNOLOGIAS CORRELATAS E SEU PAPEL NA TUTELA E GARANTIA DE DIREITOS

Diante das construções realizadas nas seções anteriores, percebe-se, inicialmente, uma efetiva dinâmica técnica envolvendo o direito e a sua capacidade de regulação do ambiente digital, com especial ênfase à projeção de poder regulatório por meios distintos do direito positivado, considerando uma realidade que, apesar de indicações isotópicas, marca-se por certos aspectos utópicos, sob o ponto de vista jurídico.

Fora apontado que a realidade informacional promove, por intermédio do exercício deslegitimado do poder programacional, efetivas lesões aos direitos humanos, de forma que a tutela, usualmente incidente para garantir e efetivar tais direitos, sofre com diversos problemas de projeção técnica e efetivação, dando indicativos da redução da capacidade regulatória do Estado e da manifestação expressiva de outras dinâmicas normativas.

Enfrentando tal situação, concebe-se a estruturação de mecanismos regulatórios incidentes sobre a esfera digital que sejam capazes de, efetivamente, garantir e tutelar direitos humanos na *Internet*, empreendendo normatização por meio de práticas tecnicamente coerentes com a realidade informacional, que sejam capazes de contornar os pontos de falibilidade apontados na atuação do direito estatal.

A hipótese principal do trabalho é concebida em razão da constatação do poder de exequibilidade, beirando os caminhos da automatização, das tecnologias de registro distribuído, *DLTs*⁷⁰, em particular as chamadas *Blockchains*, criptoativos e demais tecnologias descentralizadas modernas. Esses mecanismos são concebidos com objetivos diversos, no entanto, mostrando-se como tecnicamente adequados para, de forma nativa à rede, produzir efeitos benéficos sobre os direitos humanos ali existentes.

Dessa forma, inicialmente, há que se acentuar sua natureza tecnicamente adequada ao ambiente virtual. Enquanto tecnologias nascentes já em um estágio avançado da era da informação, considerando o nascimento das referidas tecnologias, em 2008, com o *White paper*⁷¹, de Satoshi Nakamoto, acerca do *Bitcoin* (NAKAMOTO, 2008), há que se falar na sua

⁷⁰ *Distributed Ledger Technology (DLT)*. Trata-se de uma base de dados que é distribuída entre diversos utilizadores (institucionais ou utilizadores civis), portanto, não possuindo mecanismos centralizados de registro e processamento de dados. Trata-se de um sistema de registros de informação, pautado no processamento coletivo e no consenso dos utilizadores, pautando uma rede com maior potencial de efetividade e menores riscos sob o ponto de vista de perda de dados (REINO UNIDO, 2016, p. 6). Ressalta-se que a *Blockchain* é uma espécie de rede *DLT*, especificamente o modelo fundante dos sistemas de registro distribuído.

⁷¹ Informativo detalhado, especialmente considerando o ambiente da tecnologia da informação, contendo procedimentos e estruturas algorítmicas de determinadas aplicações, além de fundamentos, motivações e ideias centrais.

estruturação enquanto mecanismos adequados a padrões virtuais de fluxos de dados e relações virtualizadas, que possuem mecanismos codificadores, capazes de produzir efeitos sobre a rede de forma eficiente e com altos níveis de não repúdio, teorizados de forma antecipada por alguns autores como sistemas digitais à prova e interferências (MAY, 1994). Tratam-se de estruturas digitais desenvolvidas já sob uma dinâmica inovadora, pautando-se em modelos descentralizados e na eliminação de pontos de conexão com a realidade física.

Enquanto efeito direto de sua adequação técnica, é possível reconhecer sua capacidade de, nativamente ao meio virtual, estruturar mecanismos capazes de regular relações humanas no ambiente da *Internet* sem a necessidade de recurso aos mecanismos normativos do mundo físico. Pautando-se na visão de Lessig (2006, p. 125), as tecnologias indicadas seriam eficientes mecanismos arquitetônicos da rede, portanto, forças automáticas de regulação capazes de sobrepujar a eficiência do direito estatal dentro da *Internet*. De fato, conforme já apontado na primeira seção, haveria que se questionar até que ponto tais técnicas, dado seu potencial de regência automática e até mesmo oculta, seriam benéficas, especialmente considerando uma possível abordagem fáustica dessas tecnologias. Assim, trata-se de um ponto de deverá ser explicitado com maior expressividade no decorrer da seção.

Uma das bases da hipótese aqui levantada e, portanto, tese que embasa a discussão, é que as tecnologias apontadas operam não somente por uma regência programacional, ou seja, não operam somente pautadas na objetividade e desvinculação de bases estáveis de legitimidade e legalidade. Tratam-se de tecnologias que nascem com uma conotação ideológica e política e, dessa forma, carregam certos elementos, capazes de trazer possível legitimidade a tais meios. Enquanto ponto de partida das tecnologias distribuídas de registro, o *White paper* de Satoshi Nakamoto permite uma clara ideia de, além de estruturar dinâmicas adequadas à realidade do ambiente técnico da *Internet*, busca-se construir uma rede descentralizada, pautada na garantia da privacidade dos utilizadores, transparência e, além disso, tendo como eixo central, raízes de funcionamento democrático, por meio de mecanismos de consenso publicamente compostos.

Ao nos referirmos às normas jurídicas que regulam aspectos do ambiente digital, percebe-se seu atrelamento à existência de agentes intermediários, portanto, agentes que teriam a capacidade de aplicar ou mesmo impor as normas sob o ambiente virtual. Por sua vez, ao adentrarmos a questão dos sistemas descentralizados, tratam-se de estruturas que não possuem agentes intermediários, de forma que sua atuação seria pautada, exclusivamente, em protocolos e códigos programados, sem estruturas de controle (DE FILIPPI; WRIGHT, 2018, p. 4).

Considerando que a norma estatal dependeria de aparatos legais e estruturais para sua exequibilidade (*enforcement*), usualmente relacionados a pontos de apego quanto ao mundo

digital, como agentes intermediários, autores como Karen Yeung (2017, p. 6) apontam que as *Blockchains* e sistemas descentralizados seriam pautados em um “*technological enforcement*”, uma exequibilidade tecnológica, no qual, ao invés de depender da estrutura que rodeia o Direito, as tecnologias em questão estariam pautadas em sistemas tecnológicos de aplicação automatizada.

Sob esse ponto, há que se considerar que, ao contrário do ambiente jurídico, as medidas aplicadas seriam autoritárias, portanto, sem meios para questionar quando a ação violasse direito dos utilizadores, sendo impossível exercitar seu repúdio, seja diretamente ou pelas vias judiciais. Não somente isso, a autora (YEUNG, 2017, p. 7) aponta que a exequibilidade automática, apesar de trazer ganhos de eficiência, não contaria com o mesmo efeito social da aplicação do direito pelo Judiciário, no sentido de reafirmar, socialmente, os valores que envolvem a norma e, em certas condições, até mesmo remodelar interpretações com base no ambiente social.

Um outro ponto que deve ser ressaltado é o potencial de afetação das tecnologias, especialmente considerando sua natureza relativamente acessível aos utilizadores da *Internet* e a dimensão da via digital atualmente, de forma que tais dinâmicas podem alcançar, massivamente, os utilizadores e, dentro da hipótese proposta, indicar caminhos de garantia e efetivação de direitos humanos muito além da atuação pontual e pós-violatória do direito estatal. O potencial de tais tecnologias faria frente a outros constructos digitais, que são responsáveis pelas práticas violadoras de direitos, figurando como uma tecnologia capaz de responder às ofensas à dignidade sob a mesma via e por meio de mecanismos correlatos, valendo-se da realidade técnica que a cerca.

Um ponto que chama atenção é o potencial das tecnologias apontadas implementarem mecanismos de garantia e efetivação apartados de possíveis interferências, ou seja, constroem espaços de privacidade e liberdade, arquitetonicamente estruturados, para que atuações violatórias sejam repelidas em sua essência. Nas palavras de Primavera De Filippi e Aaron Wright (2018, p. 7-8), os criptoativos, as *Blockchains* e as redes *DLT* trariam ao ambiente digital a aplicação de institutos jurídicos usualmente incidentes sobre a realidade física, no entanto, pautando-se em um modelo de regulação arquitetônica, chamada pelos autores de *Lex Cryptographica*.

Distintamente da *Lex Informatica*, preconizada por Reidenberg (1998, p. 555), que se pauta na utilização da tecnologia para a edição de normas estatais, enquanto uma ferramenta política capaz de trazer eficiência para os dispositivos normativos no ambiente digital, a *Lex Cryptographica* mostra-se atrelada diretamente ao ambiente privado, que empreende, por si,

medidas regulatórias, sejam elas benéficas ou mesmo prejudiciais aos indivíduos. Há que se ressaltar que, ao menos no atual estágio, não há indicativos consideráveis do empreendimento de medidas regulatórias pelo Estado por meio de *Blockchains* e tecnologias correlatas

Sob o ponto de vista filosófico do trabalho, há também que se considerar o efeito dual dessas tecnologias, com seus prováveis efeitos maléficos aos direitos dos utilizadores, como a sua cooptação pelos detentores do poder programacional e sua desestruturação em simples estruturas destoadas das dinâmicas políticas que as regiam.

O objetivo aqui proposto pode indicar um efeito negativo de tais tecnologias, havendo a impossibilidade da sobreposição de direitos devidamente ponderados, de forma que haveria constructos que, dentro do mundo dos *bits*, seriam incontornáveis até mesmo à atividade jurisdicional do Estado. Não somente isso, há que se pontuar o potencial efeito remodelador dessas tecnologias sobre a estrutura jurídica moderna, dado o impacto dessas novas tecnologias, que têm redesenhado instituições tradicionais.

Nesse sentido, considerando a quadruple incidência de forças regulatórias no ambiente digital, conforme bem expõe Lessig (2006), propõe-se a hipótese das *Blockchains*, mecanismos *DLT*, criptoativos e outras tecnologias análogas manifestarem-se enquanto mecanismos privados de garantia e efetivação de direitos humanos no ambiente virtual. Nas palavras de Luciano Floridi et al (2015, p.23), haveria a necessidade de se desenhar espaços e tecnologias, assim como políticas aplicadas a tais, como forma de proteger os direitos humanos, e oferecer a criação de um espaço permissivo à democracia.

Antes de tudo, torna-se necessário compreender as respostas anteriores do ambiente virtual frente a tais questões, pontuando as tecnologias existentes antes das referenciadas e suas dinâmicas basilares.

3.1 Respostas do mundo dos bits antes da ascensão das tecnologias descentralizadas ligadas à Blockchain e mecanismos DLT

Antes mesmo da concepção das tecnologias descentralizadas de registro, nascentes no ano de 2008, com a criptomoeda *Bitcoin*, havia instrumentos nativos à própria virtualidade que já se mostravam aptos a produzir efeitos sobre a tutela e efetivação dos direitos dos utilizadores da *Internet*.

As bases da *Internet*, como aponta Manuel Castells (2003, p. 18), marcam-se por sua expansão ao ambiente civil por intermédio de grupos pautados em ideologias de contracultura,

em especial, fortes laços com os ideais libertários, anarquistas e *hackers*⁷². Ao ter seu nascimento atrelado a grupos ideologicamente ligados com a garantia e proteção da liberdade e da privacidade, há a estruturação, desde seus momentos neonatais, de instrumentos aptos a garantir os direitos dos utilizadores em especial atenção às violações empreendidas sob tais circunstâncias.

A liberdade é apontada como um dos fatores essenciais na composição da *Internet*, de forma que a sua recém separação das redes governamentais de comunicações militares (*Arpanet*) demonstrava ser o principal ponto capaz de trazer riscos aos indivíduos ali presentes (CASTELLS, 2003, p. 24). Em um ambiente marcado pela recente “desmilitarização” da *Internet* (ASSANGE, 2013, p. 53), a atuação ideológica e codificadora dos utilizadores da rede envolvia a estruturação de barreiras robustas aos Estados, principal agente capaz de, naquele momento, apresentar riscos à dignidade humana dos utilizadores.

Tal situação é constatada quando se atem às produções político-ideológicas versando sobre a *Internet*, como o manifesto cripto anárquico de Timothy May (1994), o manifesto *cypherpunk* de Eric Hughes (1993) e a declaração de independência do ciberespaço de John Barlow (1996), que se pautam na necessidade de adoção de instrumentos aptos a, por meio do ambiente virtual, fazer frente às dinâmicas lesivas empreendidas pelos Estados. A prática utópica, portanto, estritamente focada na realidade virtual e suas especificidades, adviria da necessidade de estruturar mecanismos, no ambiente em que fossem os Estados mais fragilizados, frente ao exercício de poder pelos indivíduos, em que, apesar de possuírem relevantes instrumentos de poder, haveria ao indivíduo mais possibilidades de oposição por meio de tecnologias capazes de “erodir seus poderes” (MAY, 1994).

Sendo a rede uma forma de fugir da coerção física do Estado (MAY, 1994), atuariam tais comunidades no sentido de estruturar meios nativos ao ambiente digital, para evitar interferências consideradas ilegítimas. Uma das primeiras práticas de garantia de direitos na rede foi a estruturação de mecanismos criptográficos, capazes de codificar e cifrar informações de comunicação, conteúdo de sítios digitais e dados pessoais alocados em servidores ou sistemas de armazenamento.

Vianna (2006, p. 169) descreve a criptografia como “um conjunto de técnicas empregadas para transmitir uma informação de um transmissor para um receptor por meio de

⁷² Opondo-se à uma visão baseada no senso comum, de que *hackers* dizem respeito estritamente a cibercriminosos, o termo *hacker* nasce atrelado a indivíduos com larga experiência na estruturação de programas e aplicações digitais, portanto, programadores experientes que conviviam em comunidades especializadas durante o nascimento da *Internet* (YAGODA, 2014).

códigos secretos que impossibilitam a compreensão por terceiros não autorizados”. Tratam-se, portanto, de mecanismos de segurança informacional, que remontam ao surgimento da comunicação humana, lançando, sobre a era da informação, com estruturas mais robustas de segurança e capazes, portanto, de evitar o conhecimento por parte de terceiros. A criptografia no ambiente digital ganha especial força com o nascimento das comunidades *Cypherpunks*⁷³, no início dos anos de 1990, que se propunham a lançar diversas ferramentas de criptografia para fazer frente à coleta e uso de dados pessoais, empreendida pelos Estados e empresas (HUGHES, 1993).

Ao lançar mão de mecanismos informáticos para o empreendimento de criptografia, garante-se o anonimato de determinado fluxo de dados, marcando-se por sua viabilidade e eficiência (ISHAI et al, 2006, p. 239), especialmente considerando a criptografia assimétrica que, pautando-se em padrões de chaves pública e privada, estrutura-se, facilmente, em diversos aspectos do ambiente virtual. A criptografia, tida como simétrica pauta-se em um modelo ultrapassado de proteção, de forma que os dados cifrados se tornam identificáveis, portanto, passíveis de leitura, visualização, audição ou cópia por meio do aporte de uma senha que é do conhecimento tanto do destinatário quanto do remetente. Trata-se de um sistema frágil, sujeito a interceptações facilitadas e, dessa forma, violações à privacidade por meio do simples conhecimento da chave de encriptação.

No ano de 1976, há a criação da criptografia assimétrica, modelo utilizado até os tempos atuais, dada a sua eficiência e praticidade, lançando-se como uma das bases para a estruturação das assinaturas privadas de autenticação. Trata-se de um sistema pautado na encriptação dos dados e na sua circulação por meio de duas chaves, uma chave pública e uma privada (STALLINGS, 2008, p. 181). Uma chave privada será gerada para cada um dos comunicantes, como uma senha que será agregada à chave pública, que servirá como referência para a comunicação e poderá ser, livremente, divulgada sem riscos. A combinação das chaves, sejam aquelas do destinatário ou do remetente, permitirá a encriptação ou desencriptação do conteúdo (DIFFIE; HELLMAN, 1976, p. 644).

A garantia da sua eficiência vem da produção de chaves através de um algoritmo (algoritmo RSA), que produz chaves públicas e privadas interligadas por meio de cálculos

⁷³ Julian Assange (2013, p. 6) define *Cypherpunk* como indivíduos que defendem a utilização de criptografia e métodos similares como forma de provocar mudanças sociais e políticas. Eric Hughes (1993), um dos fundadores da comunidade, os definem como indivíduos que acreditam que o emprego de tecnologia da informação moderna pode limitar a esfera de privacidade humana, resultando em mecanismos invasivos por parte do Estado e corporações, propondo, como resposta a tais situações, a utilização de tecnologias de encriptação e *peer-to-peer* para conter as erosões à privacidade e liberdade.

matemáticos complexos. Tirando vantagem de peculiaridades matemáticas, torna-se possível divulgar, normalmente, chaves públicas pela rede, em razão de uma suposta impossibilidade, até mesmo para computadores de altíssimo processamento, recuperar as chaves privadas (RIVEST et al, 1978, p. 121-123).

Suponhamos que um indivíduo queira enviar uma mensagem privada a determinada pessoa. Tal situação, ocorrendo por meio de criptografia assimétrica, se dará através da encriptação da mensagem pelo remetente, por meio da chave pública sua e do destinatário. Após tal procedimento, a mensagem poderá ser enviada, independentemente de qualquer interceptação, uma vez que somente a chave privada do destinatário removerá a criptografia sobre a mensagem. A chave pública do remetente, por sua vez, servirá como verificador da origem e garantia de que não houve alteração.

Por meio do sistema de criptografia e assinaturas digitais, verifica-se a possibilidade de garantir o anonimato em comunicações e demais formas de circulação de dados, assim como a privacidade, sendo um método seguro para evitar a circulação de informações além dos planos estipulados. Nesse sentido, o anonimato referir-se-ia à desvinculação do indivíduo dos dados a ele relacionados, enquanto a privacidade seria relacionada ao conteúdo informacional (ISHAI et al, 2006, p. 1).

Portanto, trata-se de um método nativo ao ambiente digital, que é capaz de estruturar, por meio da dinâmica programacional, balizas robustas para evitar a interceptação do Estado ou empresas, que efetivamente redundariam em lesões à privacidade e à liberdade dos utilizadores. Marca-se pela eficiência, pela regência pautada em algoritmos e, assim, a vinculação de suas práticas, de forma que, dentro das possibilidades técnicas, haveria dificuldades para superar as barreiras de acesso ao conteúdo ou informações das partes envolvidas.

A criptografia seria marcada, portanto, pela sua confidencialidade, pela integridade informacional do conteúdo criptografado, a autenticação das partes envolvidas e o não repúdio dos compromissos ou ações (VIANNA, 2006, p. 153-154). Ainda assim, vale ressaltar que a criptografia não é absoluta e pode ser violada.

A criptografia mostra-se, enquanto tecnologia especificamente desenhada para a tutela da privacidade dos utilizadores, considerando todas as circunstâncias técnicas que regem o ambiente informacional, capaz de estabelecer especiais condições para a garantia dos direitos dos utilizadores no ambiente virtual, concretizando espaços livres de interferências, tanto dos Estados quanto de empresas, posicionando-se como eixo central na imposição de limites às práticas de vigilância digital.

A Alemanha possui uma Política de Criptografia desde o ano de 1999, pautando-se no estímulo à sua difusão e utilização e na não erosão do poder de interceptação do Estado, por meio de um esforço para “melhorar a competência técnica do ‘*law enforcement*’ e de agências de segurança” (CEPI, 2021). A legislação alemã foi adaptada à realidade da ampliação do uso de criptografia, adequando-se às políticas públicas diretivas, com uma expansão efetiva de mecanismos legais, capazes de garantir, sob um prisma isotópico, a efetividade do direito estatal no ambiente da *web*. Citamos o caso do *Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens* (Ato de ampliação da efetividade e praticidade no Processo Penal), emenda feita ao Código Processual Alemão, para incluir a possibilidade de uso de tecnologias de descriptação e vigilância legitimada, mediante procedimentos validados pelo devido processo legal e a regulamentação do *government hacking*, invasões cibernéticas promovidas pelo Estado em casos de persecução criminal (ACHARYA et al, 2018, p. 7-9).

Ao mesmo passo em que a Alemanha adota mecanismos tecnicamente adequados para lidar com questões envolvendo o ambiente virtual e sua vivência, há uma visão positiva do Estado acerca da criptografia, entendendo-a como uma prática necessária aos indivíduos e empresas no ambiente virtual, para a garantia da segurança e privacidade (ONU, 2015). O governo Holandês vem adotando semelhante posicionamento, especificamente estimulando a criptografia como medida necessária à garantia da privacidade e da liberdade econômica dos indivíduos, diante de uma economia digitalizada (HOLANDA, 2016, p. 2). A Grécia, por sua vez, adota normativas impondo mecanismos de encriptação para a garantia da confidencialidade das comunicações eletrônicas por meio do Regulamento nº 165/2011, exigindo que tais proteções sejam estabelecidas nativamente pelos provedores de *Internet* e aplicações digitais (GRÉCIA, 2011).

Torna-se necessário considerar que, dada a autoexecutividade dos mecanismos de criptografia, ou seja, a criação de limitações arquitetônicas de difícil superação, há que se falar na estruturação do direito à privacidade como um direito ilimitado, uma vez que, até mesmo sob circunstâncias legítimas de limitação, haveria impedimentos codificados que vedariam a interceptação de dados. Pensemos em um caso que há a prática de crimes no ambiente digital, tornando-se necessária a interceptação de dados. Mesmo lançando mão do édito autorizativo do Magistrado, haveria limitações expressivas à captação desses dados, o que representa, ao mesmo tempo, uma dinâmica de fragilização do caráter sistêmico do ordenamento jurídico.

Vale citar o caso do sigilo criptográfico dos discos rígidos do investigado Daniel Dantas, durante a Operação Satiagraha realizada pela Polícia Federal, no ano de 2008. Mesmo após a autorização judicial, validando o acesso às informações e, assim, justificando a quebra da

privacidade do investigado, o sigilo criptográfico não conseguiu ser quebrado pelo corpo técnico do INC e nem mesmo pelo FBI nos Estados Unidos da América, que se propôs a auxiliar na quebra da criptografia. Em razão da ausência de mecanismos técnicos hábeis a romper a encriptação lançada, permanecem tais dados sob custódia do INC (G1, 2010).

No entanto, mesmo sob esse paradigma, entendem autores que haveria a devida proteção sobre as formas de criptografia, enquanto mecanismo de garantia do direito à privacidade, de modo que qualquer limitação à sua utilização dependeria de medidas legitimamente justificadas (RONA; AARONS, 2016, p. 13). Por outro lado, compreende David Kaye (ONU, 2013b, p. 19), Relator Especial da ONU para a promoção e proteção da liberdade de opinião e expressão, que a criptografia se mostra insuficiente, dado o atual estágio da técnica informacional, para tutelar a privacidade dos utilizadores, especialmente levando em conta o poder de análise dos metadados⁷⁴, que é feita pela *Big Data*. Considerada a capacidade de análise das entrelinhas dos dados, os metadados, e o expressivo poder de processamento e produção de inferências das tecnologias de análise, haveria já certa dificuldade para a tutela da privacidade, estritamente por meio de tecnologias de encriptação.

Entende o Relator que, somente por meio de acesso online anônimo, os indivíduos seriam capazes de proteger seus direitos de privacidade, de forma que qualquer interferência na sua capacidade de acessar a rede de forma anônima representaria uma interferência na privacidade do indivíduo (ONU, 2013b, p. 20). Nas palavras do Relator David Kaye (ONU, 2013b, p. 20), “os indivíduos devem ser livres para usar a tecnologia que escolherem para assegurar suas comunicações. Os Estados devem não interferir no uso de tecnologias de criptografia nem compelir seu uso.”⁷⁵

A utilização constante de mecanismos de vigilância e persecução pelos Estados permite delimitar, com as devidas ressalvas já feitas, a necessidade de pontos de privacidade no ambiente digital, em que, apesar da relevância estar legalmente fundamentada, há ausência de fundamentos de legitimidade. As normas de segurança frente ao terrorismo, como o Ato Patriótico Estadunidense (EUA, 2001) e a Lei de Segurança Interna Francesa (FRANÇA, 2011), estipulam níveis de violação à privacidade que se sobrepõem às necessidades da segurança pública, facilitando o acesso a mecanismos de vigilância informacional pelas

⁷⁴ Metadados são dados que dizem respeito a outros dados, geralmente demarcando informações sobre a origem, data e horário de produção, envio e recebimento, formato, tamanho do arquivo e diversos outros dados que compõem as informações de determinado dado (RILEY, 2017).

⁷⁵ “Individuals should be free to use whatever technology they choose to secure their communications. States should not interfere with the use of encryption technologies, nor compel the provision of encryption keys” (ONU, 2012, p. 20).

instituições de controle e chegando ao ponto de tornar desnecessária a autorização judicial, como faz a norma francesa ao instituir normas rígidas para o controle de fluxo de informações para os agentes intermediários da *Internet*⁷⁶. Diante de situações como essa, percebe-se o potencial, mesmo que limitado pelo avanço do poder programacional do Estado, em garantir a privacidade sob um ponto de vista pré-violatório, ou seja, impedindo que a lesão à dignidade se produza de forma autônoma e auto impositiva.

É importante considerar a relação direta entre a interferência na utilização de tecnologias de anonimato e encriptação, e a tutela da liberdade de expressão e opinião, de forma que tais mecanismos garantem a esfera de privacidade necessária para a livre expressão do indivíduo no ambiente virtual, com também conexões com a liberdade de navegação. Nos termos apresentados por Rona e Aarons (RONA; AARONS, 2016, p. 15), a garantia da encriptação mostra-se como um fator essencial na garantia da liberdade de expressão dos indivíduos, de forma que a tutela pretendida por tais mecanismos acabaria por reforçar vias de proteção de direitos humanos já estabelecidas no mundo *off-line*, como a vedação ao abuso de poder, detenções e esforços punitivos contra a livre expressão dos indivíduos.

Martin Scheinin, Relator da ONU para a promoção e proteção dos direitos humanos em face do combate ao terrorismo, entende que as tecnologias de anonimato e criptografia se mostram necessárias para a efetivação de outros direitos humanos, como o direito de protesto e o direito de resistência a medidas ilícitas e ilegítimas. A garantia de comunicações privadas e reuniões mostra-se como um fator essencial na organização popular face ao Estado, ou mesmo outros atores poderosos, de forma que tais práticas deveriam ser tuteladas também no ambiente virtual (ONU, 2009, p. 14).

Há que se apontar que, apesar do entusiasmo sobre o papel da criptografia na garantia da privacidade, diversos autores, como Narayanan (2013, p. 2) Balfanz et al (2004, p. 19), indicam sua falibilidade frente aos atuais avanços da tecnologia, pontuando que a sua simples utilização teria efeitos muito menores do que aqueles esperados pelos autores ideologicamente exacerbados dos anos 1990 e 2000. Além da existência de erros humanos, desenvolvimento de tecnologias de descriptação ainda mais potentes, haveria que se falar no desincentivo econômico à adoção e produção de tecnologias de criptografia, haja vista uma intensa prática mercadológica de vigilância, de forma que a violação à privacidade dos utilizadores torna-se a engrenagem central da economia digital (NARAYANAN, 2013, p. 4).

⁷⁶ Fornecedores de serviços de *Internet* e telefonia móvel, provedores de *Internet*, gestores de sítios digitais e redes sociais, mecanismos de busca e etc.

Dada a *vênia* aos pontos indicados, percebe-se um potencial mínimo da criptografia auxiliar na garantia de direitos, especificamente a privacidade, a liberdade em todas suas facetas, assim como produzir efeitos diretos sobre outros direitos, como o caso da redução dos mecanismos de censura, que auxilia diretamente na garantia do direito à educação, direito à informação e à participação política.

Além da criptografia, há que se considerar o potencial das tecnologias de rede *peer-to-peer* na garantia de direitos no ambiente virtual, apontadas com um dos eixos centrais para o estabelecimento das tecnologias descentralizadas de segunda geração, como os criptoativos, sistemas *DLT* e *Blockchains*. Redes *peer-to-peer*, ou, traduzindo, redes ponto a ponto, tratam-se de um modelo de funcionamento de redes, por meio do qual o fluxo de informações é realizado através de infraestruturas descentralizadas, no qual cada “nó”⁷⁷ dessa rede é, ao mesmo tempo, fornecedor e consumidor de recursos informacionais (SCHOLLMEIER, 2001, p. 101).

As redes usualmente pautam-se em sistemas centralizados de informação, nos quais o fluxo informacional é unidirecional, indo de nós intermediários, para os nós consumidores, sistemas esses chamados *cliente server* ou servidor cliente (DE FILIPPI; WRIGHT, 2018, p. 16). Exemplificando, um servidor do Google atua somente como fornecedor de informações, centralizando, em si, o papel de direcionar fluxos de informação para todos os nós utilizadores.

Tratou-se do desenvolvimento de uma arquitetura de rede capaz de desatrelar a troca de informações com a atuação de agentes intermediários massivos na rede, especificamente operadores informacionais (DE FILIPPI; WRIGHT, 2018, p. 18). Permitiu-se, portanto, a extinção de mais pontos de intermediação, caminhando rumo à estruturação de uma rede conjugada de comunicação, composta por diversos indivíduos que consomem e contribuem à operação da rede, considerando que se tratam de redes com dificuldades consideráveis de serem derrubadas ou retiradas de funcionamento (CHOI, 2005, p. 394). Essas redes marcam-se pela sua estabilidade, escalabilidade, anonimato e segurança, possuindo mecanismos de controle de acesso que garantem a privacidade dos utilizadores e a autenticidade dos dados circulados pela rede.

Os sistemas *peer-to-peer* ganham popularidade junto a sistemas de difusão de músicas, vídeos e demais conteúdos digitais em violação aos direitos autorais, como o caso do popular *site* Napster, que se propunha a permitir a obtenção gratuita de conteúdo musical sem reconhecimento dos direitos autorais. A segunda geração dos sistemas *peer-to-peer* marca-se

⁷⁷ Nó, *peer* ou *node* podem ser descritos como cada unidade componente de uma rede informacional, possuindo papéis dentro da dinâmica de fluxos.

pela expansão das capacidades das redes, com sua atuação popularizada por meio de aplicações de difusão massiva de informações, como o *Gnutella* e o *BitTorrent*. Basicamente, a nova geração de redes permitiu que as “pessoas difundissem informações sobre arquivos em seus computadores pessoais sem a necessidade de redes centralizadoras” (SAROIU, 2002, p. 69).

O que chama a atenção para tal tecnologia é o seu potencial de iniciar uma desintermediação do ambiente digital, retirando, dos elos de funcionamento da rede, agentes intermediários que, dado seu poder programacional, podem empreender medidas violatórias da liberdade e da privacidade. Nesse sentido, Kubiawicz (2003, p. 33) indica que as tecnologias *peer-to-peer* possuem potencial para garantir liberdade de navegação, a liberdade de expressão e até mesmo a privacidade, por meio da retirada de figuras centralizadoras de poder, redução de espaços de controle e potencial interceptação de dados. O autor fala na tecnologia como um mecanismo que, quando combinado com outras estruturas (como a criptografia), provê garantias aos utilizadores mesmo dentro de uma rede desconfiável, permitindo que pessoas individualmente componham a rede informacional e tenham, dentro dos limites da técnica e da capacidade, algum poder de controle sobre suas atividades virtuais.

É necessário pontuar que Kubiawicz (2003, p. 35-36) sugere que a tecnologia da criptografia, assim como outras, apresentam fragilidades específicas com relação à sua arquitetura e às dinâmicas da técnica informacional, com certas fragilidades superadas pela tecnologia das redes *peer-to-peer*. Ainda assim, entende o autor que haveria a necessidade da adoção de medidas “redundantes” para fazer frente aos riscos da esfera digital, lançando mão de diversas tecnologias combinadas para trazer, aos utilizadores, uma garantia mínima de proteção à sua privacidade e liberdade no ambiente digital.

As redes ponto a ponto, ao indicarem um potencial de desintermediação da rede, permitem um ambiente de projeção da privacidade e da liberdade dos utilizadores, garantindo aos utilizadores, que, ali, transacionando informações, terão condições mínimas de anonimato e possuirão menores riscos de terem suas informações interceptadas. Assim como foi apontado, há que se considerar o potencial de tal tecnologia na garantia de outros direitos, como o direito à educação, informação e o direito à livre associação.

Não se tratando de um mecanismo inerente arquitetônico, ou seja, um algoritmo capaz de engendrar direito de forma autônoma e impedir, de forma fática, violações, há, ainda, que se pontuar o papel relevante dos *softwares* livres na afirmação de direitos no ambiente digital. Os *softwares* são peça chave na estruturação do ambiente digital, compondo não somente sistemas operacionais de aparelhos eletrônicos e aplicações, mas sendo, também, a composição base da estrutura do ambiente informacional, os algoritmos que regem o mundo dos *bits*.

Os *softwares* são, em sua grande maioria, proprietários, ou seja, *softwares* que possuem donos definidos, com direitos autorais devidamente reconhecidos e limitados, o que leva a não divulgação, impossibilidade de adaptação e aplicação para a comunidade da *Internet*. Portanto, a grande maioria dos sítios digitais, aplicações e programas utilizados na *Internet* são proprietários, estando sob controle direto dos seus desenvolvedores ou daqueles com os direitos patrimoniais sobre seu código, que não permitem sua liberalização. Considerando a dinâmica de regência algorítmica já apontada na segunda seção desta pesquisa, e as práticas engendradas pelos agentes privados, há que se levantar a discussão sobre o nível de controle exercido sobre os *softwares* e o seu potencial de limitar ou mesmo violar direitos humanos.

O grupo GNU (GNU, 2021), que milita pela expansão dos *softwares* livres, desenvolveu o famoso sistema operacional *Linux*. O GNU aponta uma clara conexão entre o exercício de controle e os *softwares* proprietários, de forma que o controle sobre os algoritmos e a impossibilidade de conhecimento dos utilizadores sujeita o indivíduo a sérias limitações, indicando que tais *softwares* seriam “um instrumento de poder injusto”.

Seguindo o que já fora apontado, um *software* proprietário denota uma expressão de poder programacional, sob a forma de produção, comercialização e distribuição de sistemas capazes de empreender, sobre os utilizadores, práticas violatórias de direitos. Portanto, seriam mecanismos algorítmicos que, assim como indicado antes, atuariam de forma oculta e promovendo regulação arquitetônica sobre os utilizadores, limitando sua atuação ou projetando os indivíduos rumo a pontos já tracejados pelo programador.

Por sua vez, os *softwares* livres seriam marcados pela transparência de seus códigos, permitindo ao utilizador executar o programa como deseja, conhecer o código-fonte e promover alterações, assim como redistribuir o programa. Quando se fala em *software* livre, fala-se na liberdade de “distribuir, estudar, mudar e melhorá-lo” (GNU, 2021) e não na sua gratuidade, haja vista que podem existir sistemas de código aberto que possuem custos para o utilizador.

Há que se diferenciar os *softwares* livres e os *softwares* de código aberto. Os *softwares* código aberto (*Open Source*) referem-se àqueles programas que possuem, única e exclusivamente, a liberdade do utilizador conhecer seu código fonte, portanto, sabendo o que está sendo feito pela aplicação (KELTY, 2008, p. 2-3). Os *softwares* livres necessitam adequação a quatro princípios basilares: a) liberdade de executar o programa como o utilizador deseja; b) liberdade para analisar os códigos e adaptá-lo; c) liberdade para redistribuir cópias, sejam elas gratuitas ou onerosas; d) liberdade para ceder à comunidade versões modificadas do *software* (GNU, 2021).

Gabriella Coleman (2009, p. 420) indica o papel essencial dos *softwares* livres na remodelação dos padrões de liberdade, propriedade e privacidade no ambiente digital, indicando tal prática como uma resposta efetiva da comunidade virtual para fazer frente às violações de direitos. Portanto, diferente das demais situações antes indicadas, que se referem aos mecanismos com natureza arquitetônica, algorítmica, os *softwares* livres mostram-se como uma prática social que produz efeitos no ambiente digital, por meio da atuação dos utilizadores. Ainda que ausente autoexecutividade e uma dinâmica algorítmica de proteção, há que se visualizar seu valor para a afirmação dos direitos humanos no ambiente virtual.

Referindo-se aos *softwares* livres, haveria o apontamento para o princípio da transparência algorítmica, no sentido de permitir o conhecimento daquelas estruturas que regem o ambiente digital, compreendendo seus traços e suas diretivas, considerando seu poder regulatório.

A possibilidade de conhecer os códigos-fonte que compõem determinado sítio digital ou aplicação mostra-se como fator essencial para garantir a privacidade dos utilizadores, permitindo que se evitem exposições ilícitas. No mesmo sentido, a capacidade de alterar as programações, com a devida ressalva ao conhecimento técnico para tanto, tem potencialidade de auxiliar, diretamente, no enfrentamento das violações de direitos humanos no ambiente virtual, garantindo aos utilizadores a possibilidade de suplantar obstruções arquitetônicas e auto executivas aos seus direitos.

A possibilidade de livremente distribuir *softwares*, com adaptações feitas pelos utilizadores, mostra-se como um fator útil à liberdade econômica no ambiente virtual, permitindo aos indivíduos explorarem atividades econômicas no ambiente virtual sem limitações desnecessárias. Além disso, há que se pontuar o papel essencial desses *softwares* na expansão do direito à informação e do direito à educação, especialmente considerando a educação informática, que se mostra necessária e importante para os utilizadores da rede. Conhecendo os códigos-fonte e sabendo do seu funcionamento, há que se projetar uma melhor percepção dos indivíduos aos riscos que cercam seus direitos, portanto, tornando-os mais aptos para responder a tais situações pelas vias da técnica informacional.

Ainda assim, há que se pontuar que tais tecnologias, isoladamente consideradas, mostram-se sujeitas a alguns pontos de fragilidade, conforme já indicado. A ideia por trás dos criptoativos, *Blockchains* e tecnologias correlatas, é unificar, considerando as especificidades de cada uma das tecnologias e seu potencial, os principais pontos formulados por tais tecnologias para, sob a forma de um amálgama técnico, tentar produzir efeitos com maior amplitude, eficiência e, acima de tudo, com projeção à coletividade digital.

Nesse ambiente das tecnologias que antecedem os criptoativos, *Blockchains* e outras, há que se compreender como ascendem novas demandas de direitos por intermédio de instrumentos técnicos, figurando como respostas dos próprios indivíduos no mundo digital, opondo-se a questões que se mostravam sensíveis. Muito embora se produza a hipótese de que as tecnologias relacionadas às *Blockchains* mostram-se tecnicamente adequadas e capazes de produzir efeitos benéficos aos direitos humanos, as tecnologias predecessoras mostram-se como as bases reflexivas da dignidade humana no ambiente digital, pautando as discussões iniciais que se projetam à discussão em diversos aspectos dos direitos humanos, como a questão da educação, saúde, ampliação das medidas de efetivação de direitos, exercício de direitos políticos e etc.

Ainda que sob um prisma ideológico exacerbado, a ideia composta pelos diversos autores e as técnicas instrumentalizadas pelos utilizadores da rede já demonstravam que o ambiente digital apresentava condições específicas que o delimitavam do mundo físico, produzindo consequentes reflexos jurídicos sobre isso. Não bastasse isso, com questões jurídicas mostrando-se relevantes para a discussão, o utopismo jurídico, advindo das estruturas técnicas do ambiente informacional, passa a dar lugar a espaços de retroflexão, com mecanismos digitais capazes de estruturar uma realidade jurídica nativa e, ao mesmo tempo, capaz produzir efeitos benéficos sobre a realidade física, ampliando os mecanismos de tutela e garantia de direitos humanos sob a égide estatal.

No entanto, mantendo-se alinhado aos objetivos aqui propostos, passa-se à discutir exatamente a questão dos criptoativos, *Blockchains* e tecnologias correlatas, enquanto amálgama técnico que se propõe e fazer frente às falhas marcantes na garantia de direitos no ambiente virtual, demarcando uma natureza coletiva, consensual, algorítmica e tecnicamente resistente a alterações não consensuais, ainda que se pesem condições específicas que impactam sua atuação ou projetem efeitos maléficos sobre os utilizadores.

Robert Herian (2018, p. 131) aponta as *Blockchains* como uma tecnologia capaz de remodelar ou até mesmo substituir o direito, capaz de incidir sobre a forma de percebermos propriedade, liberdade, soberania, governança e regulação, o que fomenta a produção de hipóteses no sentido dos seus impactos diretos sobre a seara dos direitos humanos.

3.2 Características e funcionamento das *Blockchains*, criptoativos e tecnologias correlatas

A pedra de toque para a compreensão do fenômeno das criptomoedas, *Blockchains* e tecnologias correlatas é o ano de 2008 e o lançamento do *White paper* do *Bitcoin* por Satoshi

Nakamoto (2008), pseudônimo de um indivíduo ou grupo que desenvolveu toda a programação atrelada ao funcionamento da criptomoeda, pautando-se estritamente na atuação descentralizada, anônima e virtual do registro de informações em correntes de dados coletivamente certificadas (*Blockchains*). Portanto, a criptomoeda *Bitcoin* nasce no ano de 2008, com a tecnologia *Blockchain* mostrando-se como mero acessório à funcionalização do sistema de circulação virtual de ativos, uma tecnologia cativa que serviria, em um primeiro momento, única e exclusivamente ao registro virtual de transações.

O *Bitcoin* nasce marcado por uma influência *cypherpunk*, centrando-se na estruturação de ativos e, ao mesmo tempo, na formação de mecanismos hábeis para a garantia da privacidade, liberdade e anonimato dos utilizadores, em um primeiro momento, centrada na questão transacional. Diversos teóricos, *hackers* e desenvolvedoras, banhados na mesma fonte ideológica, já haviam tentado, reiteradamente, desenvolver moedas digitais capazes de garantir transferências digitais de valores sem qualquer mecanismo de identificação e, portanto, capaz de preservar a privacidade e a liberdade dos utilizadores. A ideia inicial da construção de uma moeda digital nasce em 1983, com David Chaum (1983), tido pelos teóricos como o pai da tecnologia do dinheiro digital.

Um ano após obter seu Doutorado em Ciências da Computação, pela Universidade Estadual da Califórnia, com a ajuda da recém fundada Associação Internacional para Pesquisa Criptológica⁷⁸, David Chaum (1983) apresenta seu icônico artigo “*Blind signatures for untraceable payments*”, propondo a construção de um sistema digital de transferência de valores que tornaria desnecessária a obtenção de informações das partes. Onze anos após sua teorização, Chaum lança o chamado *Digicash*, aplicando suas teorias a um ativo digital baseado no sistema de assinaturas digitais, sendo esse ativo estruturado sobre um ente central que atuaria como agente de câmbio, realizando a checagem e a verificação das transações. Diversos outros ativos digitais, pautados em agentes centralizados, foram desenvolvidos, como o caso do BitGold (SZABO, 2005) e do B-Money (DAI, 1998).

Dois pontos foram cruciais para o desenvolvimento do *Bitcoin* e, conseqüentemente, de toda a tecnologia de registro distribuída dela advinda, um relacionado à própria dinâmica ideológica dos desenvolvedores e outro de natureza técnica, diretamente atrelada à ciência computacional. Os *cypherpunks*, marcados por uma ideologia anarquista/libertária, passam a ver a necessidade de estabelecer mecanismos de desintermediação das transações econômica, eliminando instâncias intersticiais que, na sua visão, atuavam também como mecanismos de

⁷⁸ *International Association for Cryptologic Research (IACR)*.

controle, efetivos pontos sobre os quais poderiam ser impostas obrigações pelo Estado ou mesmo poderiam ocorrer medidas de vigilância com finalidades econômicas.

Por outro lado, ao se falar em moeda digital, há que se reconhecer que, além da superfície, em seu sentido flusseriano, há apenas um emaranhado de *bits* marcados algorítmicos de registro. Ocorrendo o avanço das ideias, percebeu-se a necessidade de usar mais tecnologias para controlar o fornecimento de moedas e manter níveis de segurança e certeza acerca do seu possuidor. Sendo um recurso digital, haveria a possibilidade de ocorrer a reprodução infinita dessas moedas, o que representaria a derrocada do seu funcionamento e abertura de espaço para a ocorrência de fraudes, ausente agentes intermediários capazes de validar as transações e atualizar os registros (DE FILIPPI, WRIGHT, 2018, p. 19).

A possibilidade de cópia e utilização de um mesmo ativo digital de forma duplicada é chamado pelos teóricos de “*double spending problem*”, ou problema do duplo pagamento ou refluxo monetário. Esse problema exige que cada transação digital “seja checada online em face de uma lista de central de registros” (CHAUM, 1992, p. 96), mostrando-se como um ponto primordial para a estruturação de mecanismos de transação virtual e, mais que isso, mecanismos digitais de registros resistente às alterações. Portanto, qualquer forma de registro digital, ausente de estruturas centralizadas, demanda lidar com a questão do *double spending*, especialmente os sistemas que regem transferências de ativos digitais, como forma de evitar a desvalorização do ativo, evitar emissões desautorizadas e evitar o repúdio⁷⁹ de registros (DE FILIPPI; WRIGHT, 2018, p. 20).

Face ao exposto, o *Bitcoin* nasce, no ano de 2008, como um amálgama de tecnologias, especificamente fundindo, sobre um mesmo algoritmo, os sistemas de chaves assimétricas, assinaturas digitais, *software* aberto e as redes *peer-to-peer*, estruturando a chamada *Blockchain*, responsável, inicialmente, pelo registro das informações transacionais por meio de um sistema descentralizado, que possui estruturas adequadas para evitar a situação de *double spending*. A *Blockchain* mostra-se como uma espécie de rede *DLT* desenvolvida, especificamente, com uma natureza encadeada dos dados (UHDRE, 2021, p. 33), nascendo junto ao *Bitcoin*, sendo elas descritas como (CAMPBELL-VERDUYN, 2018, p. 1) “[Blockchains] são sequências digitais de números codificados em *softwares* de computador

⁷⁹ Repúdio refere-se à rejeição ou negativa sobre a validade de determinado registro.

que permitem a troca segura, registro e divulgação de transações entre indivíduos atuando em qualquer lugar do mundo com acesso à *Internet*.”⁸⁰

Campbell-Verduyn (2018, p. 1) indica que os objetivos principais das *Blockchains* são a obtenção de uma capacidade sem precedentes de monitorar interações, baseadas na realidade informacional, que estariam relacionadas diretamente a indivíduos quase anonimamente indicados, com estes atuando para verificar, registrar e publicizar os registros digitais. Tratar-se-ia de um registro imutável, a menos que haja claro consenso entre os nós para alterá-lo, que demandaria da obtenção do consenso.

O estabelecimento desses protocolos tem como fundamento a garantia da confiança entre nós desconhecidos da rede, garantindo formas de verificação e garantia que, mesmo distante de dinâmicas de controle, seriam capazes de garantir a regularidade dos registros e, por consequência, das transações. As redes *DLT*, com encadeamento de dados, especificamente as *Blockchains*, marcam-se por sua robustez, ou seja, pela sua capacidade de lidar eficientemente com situações excepcionais, medidas que são extremamente necessárias em redes descentralizadas e autônomas, situações que são viabilizadas pelas respostas algorítmicas ao *double spending*, que se baseiam no registro individualizado de transações e na negação de todas as transações que não a primeira que se refira ao mesmo ativo (RAMAMURTHY, 2020, p. 56-57)⁸¹.

Se, ao estabelecermos uma relação comercial física, vislumbra-se a existência de um ente central simbolizante, capaz de garantir a validade daquela transação, a moeda estatal e trazer confiança às partes por meio de um sistema jurídico que a embasa. Portanto, há uma confiança mínima entre desconhecidos que é garantida por um agente central, verticalizado.

Sem um ente central capaz de organizar os registros e validar as transações, o *Bitcoin* estrutura-se em protocolos de consenso capazes de trazer regras específicas para a composição do consenso entre os diversos nós da rede. Trata-se de um sistema aberto e interoperável composto por diversos utilizadores, que executam, individualmente em seus computadores, uma cópia do algoritmo regente (DE FILIPPE; WRIGHT, 2018, p. 21), demandando a existência de um sistema capaz de gerenciar a massa de utilizadores e suas respectivas informações de registro. Nesse sentido, “uma estrutura pautada em um algoritmo democrático

⁸⁰ “*Blockchains are digital sequences of numbers coded into computer software that permit the secure exchange, recording, and broadcasting of transactions between individual users operating anywhere in the world with Internet access*”.

⁸¹ Ao adentrarmos em *Blockchains* de segunda geração, como o caso da Ethereum, percebe-se a utilização de sistemas de evitação do *double spending* mais modernos e eficientes, especificamente, pautando-se na combinação do número da conta e do número global da transação para verificar sua validade frente à corrente de dados e a estampa temporal (BUTERIN, 2013).

dependeria do nível de consenso entre os nós descentralizadas”⁸² (CAMPBELL-VERDUYN, 2018, p. 2).

O consenso em uma rede *Blockchain* é marcado pelo uso de protocolos seguros e predefinidos, validação de transação e blocos, verificação da viabilidade de recursos, a execução e confirmação de transações. Nesse sentido, uma cadeia de blocos de registro singular, com dados consistentes, mostra como aquela que será consensualmente definida pelo protocolo com a vigente, portanto, aquela que será distribuída à rede e referida como a válida. A cada inclusão de blocos na corrente aumenta-se o nível de segurança e confiança na rede, uma vez que o consenso, acumulado para validar e confirmar cada um dos blocos, torna dificultosa a alteração e expressivamente desvantajosa.

O instrumento de consenso da grande maioria dos criptoativos pauta-se no chamado consenso distribuído⁸³, que compreende a existência de diversos nós da rede compondo um registro conjugado, que deve passar por testes robustos de validação, verificação e confirmação à rede (NARAYANAN et al, 2016, p. 53). Pensemos os nós como cartórios de escrituração, considerando que, entre eles, há uma rede descentralizada, portanto, um registro comum, que deve ser construído conjuntamente por todos, mantendo a segurança da rede e garantindo o não repúdio das informações ali constantes. A garantia de uniformidade dos registros ocorre por meio do chamado *proof of work*, prova de trabalho, algoritmo disponibilizado no sistema *Blockchain* que, após resolvido, permitirá ao registrador gerar um número de registro válido (no caso das transações escritas na *Blockchain*, são os chamados *hashs*) e permitirá aos demais nós verificarem a conformidade com os registros anteriores (DE FILIPPI, WRIGHT, 2018, p. 23), portanto, o mecanismo que efetivamente controla a informação que poderá ser adicionada aos repositórios.

Acerca disso, expõe Jan Ziegeldorf (2018, p. 451):

Todas as transferências são agrupadas em blocos e gravadas em um registro público, a *Blockchain*, que contém a história completa das transações aceitas envolvendo *Bitcoins*. A *Blockchain* é constantemente validada pelos participantes. Adicionar um novo bloco à *Blockchain* requer uma *proof-of work*, uma prova de trabalho, no qual aquelas divergências com relação à *Blockchain* requerem, em um pequeno tempo, uma nova realização do *proof-of-work* para os blocos sucessores. Trata-se de uma proteção contra interferências e o problema de dispêndio em dobro (*double spending*) de *Bitcoins*, desde que a maior parte do poder de computação seja contribuído por nós honestos e que não colidam com a maioria.⁸⁴

⁸² “A democratic algorithm structure depends on the consensus level of decentralized nodes”.

⁸³ *Distributed consensus*.

⁸⁴ “All transfers are grouped into blocks and recorded in a public ledger, the blockchain, which thus contains the complete history of accepted Bitcoin transactions. The blockchain is constantly validated by the Bitcoin participants. Adding a new block to the blockchain requires a prior proof-of-work such that diverging from the

Primavera De Filippi e Aaron Wright (2018, p. 42) descrevem a *Blockchain* e as demais redes descentralizadas como sistemas capazes de coordenar atividades sociais e auxiliar pessoas a chegarem a um consenso em determinada questão, o que denotaria sua função que extrapola sua utilização inicial para fins econômicos.

Acerca disso, expõe Primavera De Filippi (2015):

*A Blockchain é uma tecnologia interessante nesta questão, enquanto uma tecnologia que facilita o estabelecimento de um novo modelo de governança que é mais plano, mais transparente e potencialmente permite mais democracia e participação na tomada de decisões. Na minha visão, um dos benefícios chave da Blockchain é que ela reduz (ou mesmo elimina) a necessidade de intermediários ou agentes. Por meio da incorporação de regras específicas de governança junto à Blockchain, torna-se possível às comunidades se auto-organizarem e gerenciarem, transacionando diretamente com outro sem a necessidade de confiar em qualquer autoridade centralizada.*⁸⁵

Dessa forma, o consenso é obtido através da prova de trabalho no caso da *Blockchain*, um mecanismo que depende da realização de extensos cálculos matemáticos e consumo de vastos recursos computacionais. Em termos técnicos, a prova de trabalho fornecerá um número de *hash* válido para um bloco de registro de transações, com esse número possuindo uma estampa temporal (marcas de hora e data de registro, *timestamp*) e uma conexão direta com o número de *hash* do bloco anterior. Portanto, sendo a *Blockchain* uma cadeia de blocos, o número de *hash* obtido pela prova de trabalho deverá levar em conta o *hash* anterior, e assim formando um círculo virtuoso que garante a validade dos registros ali incluídos. Havendo a prova de trabalho e a validação de um bloco, ele será incluído e comunicado a toda a rede descentralizada, no qual tal cadeia de blocos passará pela validação pelos demais nós, será confirmado e, cumulando consenso de 50% mais um da totalidade dos nós, haverá a adoção daquela cadeia de transações como a base para as seguintes.

Dessa forma, as *Blockchains* garantiriam por meio de seus protocolos uma maior confiança aos utilizadores, que basicamente migrariam de agentes centralizados para uma rede descentralizada, no qual os utilizadores interagem entre si por meio dos modelos estabelecidos (CAMPBELL-VERDUYN, 2018, p.3). Tratar-se-ia de um sistema pautado na auto governança

blockchain at an earlier point in time would require redoing all proof-of-works for the successor blocks. This protects against tampering and rules out double-spending of Bitcoins as long as the majority of computation power is contributed by honest non-colluding participants” (tradução livre).

⁸⁵ “*Blockchain is an interesting technology in that regard, as it facilitates the establishment of new governance models which are flatter, more transparent and potentially allow for more democratic and participatory decision-making. In my view, one of the key benefits of the blockchain is that it reduces (or even eliminates) the need for an intermediary or a middle-man. By incorporating specific governance rules directly into the blockchain, it becomes possible for communities to self-organize and self-manage themselves, transacting directly with one another without the need to rely on any centralized (trusted) authority*” (tradução livre).

e na sua sustentabilidade interna, tendo seu funcionamento autonomamente garantido, independentemente de qualquer instituição social, uma rede gerida por seu próprio algoritmo na qual a integram somente aqueles que concordam com seu modelo (DE FILIPPI; LOVALUCK, 2016, p. 10).

Portanto, as transações realizadas em *Bitcoin* ou qualquer outra moeda que adote similar sistema, assim como registros em geral lançados nas *Blockchains* são registradas de forma anônima, tendo por base o sistema de chaves públicas e privadas. No entanto, ainda assim, há a abertura da rede e dos registros a todos aqueles que queiram conhecê-los, demarcando um certo nível de transparência (DE FILIPPI, WRIGHT, 2018, p.22).

Basicamente, as *Blockchains* podem ser de natureza pública, no qual a atuação como parte da rede, no caso como mineradores, seria livremente exercida por qualquer indivíduo, que teria acesso aos protocolos e *softwares* necessários para a sua operacionalização. As redes públicas, por serem de fato redes descentralizadas com caráter massivo, teriam que arcar com mecanismos de consenso mais estrito, como forma de garantir que os diversos nós da rede concordem com os registros efetivados. Haveria também as *Blockchains* privadas, no qual o acesso é limitado a partes específicas, marcadas pela ausência de transparência.

Por outro lado, haveria as *Blockchains* permissionárias, no qual são constituídos um consórcio de nós especificamente designados para proceder com os registros, validações e verificações dos dados aportados, facilitando a sua gerência e contingenciamento. Trata-se de um modelo de rede marcada por uma semi descentralização, de forma que haveria um ente central que confiaria aos nós a função (RODRIGUES et al, 2021, p.65), possuindo os benefícios de rede pública com a velocidade e eficiência advindas de uma seletiva de utilizadores que poderão promover as validações e registros.

Citamos como exemplo a rede da criptomoeda Libra, que adota como nós da rede de validação apenas empresas que tenham contribuído monetariamente para o projeto, de forma que somente os validadores possuem acesso aos registros e conseguem efetivamente proceder com as verificações e registros.

Havendo nós designados e, portanto, confiados para exercer as atividades da rede, não haveria a necessidade de métodos robustos de garantia do consenso, provendo maior agilidade nos registros. Por sua vez, haveria que se considerar suas fragilidades, como o caso do monopólio do poder sobre a rede, o que poderia representar no empreendimento da rede para finalidades específicas, inclusive opostas à dignidade dos utilizadores, fazendo uso dela conforme os interesses de um seletivo grupo de validadores possuidores do poder de fato sobre

os registros ou mesmo possuindo mais pontos de fragilidade frente a possibilidade de invasão e afetação por *hackers* (RODRIGUES et al, 2021, p.66).

Na visão de Primavera De Filippi e Aaron Wright (2008, p.31) apesar das facilidades atreladas à validação e aprovação, as redes permissionárias e privadas contariam com problemas relativos à confiança, residindo sua base sobre poucos nós, que podem facilmente se corromper, além de tal situação importar em uma alteração massiva da natureza ideológica trazida pela *Blockchain*, que se pauta no consenso democraticamente composto.

Vale ressaltar que tecnologias *DLT* correlatas marcam-se pela adoção de modelos distintos de garantia do consenso descentralizado, que se adequam a necessidades específicas, embora mantenham quase a totalidade das dinâmicas trazidas pela *Blockchain*. A chamada segunda geração de *Blockchains* marca-se pela ascensão de modelos pautados em redes descentralizadas formada por nós autorizados, reduzindo os dispêndios energéticos do *proof of work* e as largas etapas de verificação e confirmação (RODRIGUES et al, 2021, p. 65). Citamos como exemplo o modelo de verificação de consenso por meio do mecanismo de falha Bizantina⁸⁶, que se pauta na identificação de padrões de falha que serão comunicados e verificados antes da averiguação dos pontos corretamente identificados nos registros, portanto, tratando-se de um modelo de consenso que tolera em certos momentos erros nos registros (LAMPORT et al, 1982, p.382). A criptomoeda Libra é um exemplo que adota a falha Bizantina e o modelo autorizado para registrar transações de forma descentralizada.

Dessa forma, as transações são armazenadas em correntes de blocos (*Blockchains*), com cada um deles sequencialmente alinhados, sendo os blocos marcados por uma estampa temporal e um *hash*. No caso do *Bitcoin* e das demais tecnologias que adotam a *Blockchain* em seu estado primordial, a inclusão de novos blocos na corrente demanda o *proof of work*, que se marca pelo aporte de recursos físicos à rede para prover a adição, verificação e validação dos blocos. Os agentes atuam coletivamente no esforço, com cada um deles sendo remunerado com um prêmio do sistema, com um claro incentivo econômico para que os indivíduos atuem a favor da rede e do consenso coletivo (DE FILIPPI; WRIGHT, 2018, p.26).

Portanto, trata-se de um sistema que encoraja os interesses individuais dos utilizadores em nome de contribuições para o melhor benefício da coletividade, com indivíduos atuando dentro da sua singularidade e produzindo resultados úteis a toda rede (SWAN, 2015, p. 3-4). Vale considerar as relevantes críticas a tal situação que criaria uma visão de “cidadãos-

⁸⁶ *Byzantine Fault Test* (BFT).

consumidores” ao se referir aos utilizadores das redes descentralizadas, uma visão privatista que traria prejuízos à questão da dignidade humana carreada por tais tecnologias.

Cada *hash* criado para um novo bloco de transações será recompensado com uma quantidade específica de criptoativos, o chamado *block reward*, que é entregue àqueles que efetivamente auxiliaram fornecendo recursos computacionais para a resolução da equação matemática. Trata-se de uma atuação centrada na “verificação e divulgação à rede das transações registradas, competindo para criar um bloco que será validado e confirmado pelos demais utilizadores”⁸⁷. A atividade de fornecimento de poder computacional à rede *Blockchain* é usualmente chamada de mineração, estando presente em todas as *Blockchains* que possuam natureza pública, ou seja, fundamentam-se no funcionamento descentralizado pautado em nós que podem livremente operar o algoritmo que rege o sistema.

A utilização de *Blockchains* atreladas diretamente a criptomoedas e, portanto, questão econômicas, apesar de indicarem um potencial de não alterarem a relação dessas tecnologias com a produção de efeitos jurídicos, há que se reconhecer o papel essencial da estabilização da rede de registros por meio dos mecanismos econômicos a elas atrelados. Basicamente, a garantia de inalterabilidade dos registros e, portanto, todas as garantias atreladas ao seu uso dependem de um uso maior da rede, com mais e mais nós integrando os sistemas de validação e verificação. A atratividade econômica serve para incentivar a participação de agentes em ceder poder de processamento e, portanto, contribuir com o objetivo coletivo da rede, aumentando a sua resistência e tornando mais eficiente sua utilização e efeitos.

Acerca disso, expõem CARLSTEN et al (2016, p.155):

Basicamente, se o custo para realizar registros aumentar (como é esperado que ocorra, uma vez que o protocolo *Bitcoin* parará de emitir recompensas), a troca de *Bitcoins* pode se tornar mais caro, fazendo com que menos pessoas confiem na rede, mostrando-se mais próximas de alternativas centralizadas, fazendo com que o interesse em *Bitcoin* minguie.⁸⁸

Um passo primordial para a compreensão do papel das referidas tecnologias sobre a questão dos direitos humanos é visualizar a sua projeção muito além das questões estritamente econômicas que envolvem as transações de criptomoedas, que, de fato, deram origem às *Blockchains*. Campbell-Verduyn (2018, p. 6), ao se referir ao impacto direto das criptomoedas

⁸⁷ Fala da Doutora Bina Ramamurty no Curso “*Blockchain Basics*”, *State University of New York*, 06 maio 2020.

⁸⁸ “*Conversely, if Bitcoin’s transactions fees increase (as they are expected to do once the Bitcoin protocol stop issuing block rewards) sending Bitcoins may become expensive, making it less likely that people will choose to rely on this network, as opposes to more centralized alternatives, thereby causing interest in Bitcoin wane*”. (Tradução livre).

e *Blockchain* na governança, indica que as tecnologias, independente da fonte, teriam aplicações distantes daquelas advindas de seu propósito inicial, com as tecnologias atreladas às *Blockchains* tidas como de segunda geração, sistemas que se estruturam com novidades em relação ao modelo primordial, a *Blockchain* de Satoshi Nakamoto. Essas tecnologias teriam um impacto amplo, que excederia a limitação do seu uso econômico e, portanto, alcançariam questões jurídicas e de governança.

As *Blockchains* marcam-se, sob uma análise geral, pelo seu pseudo anonimato, portanto, registros que não revelam a real identidade dos utilizadores de forma imediata, indicando somente as chaves públicas daqueles indivíduos envolvidos, com a devida assinatura digital, capaz de garantir a fidedignidade daquele que efetivou a transação. Trata-se, portanto, de um sistema de registro e verificação permanente que não revela, precisamente, quem e o que estaria envolvido naqueles registros (CAMPBELL-VERDUYN, 2018, p. 1).

Pautando-se no que fora iniciado pela *Blockchain*, o sistema de registros mostra-se como uma “trilha auditável da atividade da rede, que embora estejam as informações criptografadas e indiquem somente dados públicos, é possível para averiguação por qualquer um” (DE FILIPPI; WRIGHT, 2018, p. 38), tendo conhecimento do valor transacionado e da chave pública dos envolvidos. Algumas redes tidas como de segunda geração (*ZCash* e *Monero*) adotam modelos que divergem das bases da *Blockchain*, ao adotar o chamado *zero-knowledge proofs* e a *ring signatures*⁸⁹, que ampliam a esfera de privacidade e rompem com a abertura trazida pelas redes de pseudoanonimato (SASSON, 2014, p. 460) (MACKENZIE, 2015).

Há que se considerar que o pseudoanonimato, como uma decorrência da técnica informacional, mostra-se como um incentivo à realização de atividades sociais e econômicas, como a ampliação da esfera de direitos (DE FILIPPI; WRIGHT, 2018, p.38), ao mesmo tempo que pode incentivar práticas ilícitas, como a evasão fiscal, lavagem de dinheiro e o tráfico ilícito de armas e drogas (OMRI, 2013, p.39-40).

É importante considerar que a tecnologia Bitcoin, portanto, pautada no sistema *Blockchain*, embora possua efeitos sobre a questão dos direitos humanos, apresenta algumas limitações de utilidade, nas quais a sua estrutura permite a sua utilização, estritamente dentro dos objetivos para os quais foi criada (DE FILIPPI; WRIGHT, 2018, p. 27). Trata-se de uma rede que possui certas limitações com relação às informações registradas e ao tempo de registro, motivos pelos quais há o surgimento de diversos novos projetos baseados no modelo

⁸⁹ *Zero-knowledge proofs*, provas de conhecimento zero, e *ring signatures*, assinaturas em anel, tratam-se de sistemas adotados por algumas *Blockchains* e criptoativos para esconder informações acerca da fonte, destinação e quantidade das transações registradas.

Blockchain para superar esses limites, lançando a base para a construção de sistemas descentralizados, objetivando superar esses limites e ampliar a utilidade dessas tecnologias.

Basicamente, em razão da natureza livre dos *softwares* e protocolos relacionados à *Blockchain*, a sua ideia inicial passou a ser replicada e melhorada, motivo pelo qual os sistemas *DLT*, marcados pelo encadeamento de dados, são chamados também de *Blockchains*. Conforme expõe Campbell-Verduyn (2018, p. 2), as diversas replicações e adaptações da *Blockchain* são usadas não somente para criptoativos, mas também servindo para o registro de diversos tipos de informações, citando o autor, como exemplo, o registro de questões contratuais, votos e informações públicas.

Nesse paradigma, há que se falar que, com a expansão das utilidades das tecnologias relacionados às *Blockchains* e correlatas, há uma efetiva expansão da capacidade de tutela e efetividade dos direitos humanos no ambiente virtual, que vai além das simples bases traçadas por Satoshi Nakamoto, em 2008. Ainda assim, há que se pontuar que as bases trazidas pela *Blockchain* e pelo *Bitcoin* são capazes de tutelar a questão da privacidade e liberdade no meio informacional, sendo a segunda geração de *Blockchains* responsável por ampliar e diversificar as medidas de garantia e efetivação, ampliando-se, também, para outros âmbitos de dignidade.

A segunda geração de criptoativos e *Blockchains* surge com protocolos que vão muito além do poder de registro e da utilidade do modelo inicial, utilizando-a para outros fins que não a simples circulação de criptoativos, que projeta efeitos marcantes sobre a questão dos direitos humanos. É necessário considerar a enorme inovação trazida pela primeira das *Blockchains* tidas como de segunda geração, o *Ethereum*, que se pauta nos mesmos fundamentos da *Blockchain* e fazendo uso de um novo modelo de *state-transition system*⁹⁰, e o incremento de uma nova camada de algoritmos atrelados ao sistema de registros, capaz de incluir mais informações além daquelas usualmente registradas. A nova geração de *Blockchains* marca-se, portanto, pela inclusão das *overlay networks*, ou redes de sobreposição, novas camadas de protocolos que passam a ser atreladas aos sistemas de registros já existentes para transmitir dados adicionais.

A inclusão de uma nova camada de registro para dados, especificamente no caso da *Ethereum* o chamado sistema *Solidity*, permitiu a inclusão e funcionalização de novas aplicações por meio da rede descentralizada, como o caso dos chamados *smartcontracts*⁹¹,

⁹⁰ *State-transition system* ou sistema de estado de transição, trata-se do protocolo de atualização das redes *DLT*, referente à inclusão de um novo bloco de dados da corrente de dados. Portanto, resumindo, trata-se do modelo que vai reger o tempo de atualização da rede e inclusão de novos dados nos registros.

⁹¹ Os contratos inteligentes operam como um agente autônomo, automaticamente reagindo aos *inputs* recebidos por contas externas ou outros contratos inteligentes executados na rede, permitindo às partes realizar transações,

contratos inteligentes, que se pautam na operacionalização automática, sem a necessidade de atuação das partes para efetivar pagamentos, garantindo a realização de transações econômicas com baixos custos, alta garantia e velocidade (DE FILIPPI; WRIGHT, 2018, p. 29).

Um ponto que merece ser indicado é a questão dos *forks*, partições na rede em razão de dissenso acerca de determinado protocolo. Referindo-se, especificamente, às *Blockchains* públicas, como é o caso da *Blockchain*, em razão da ausência de estruturas intermediadas, a adoção de determinado protocolo acerca do registro, validação e verificação das informações depende também do consenso da rede, com a necessidade de que os nós da rede aceitem tal alteração e, de forma fática, adotem tal protocolo junto aos sistemas em operação. Nesse ponto, pode ocorrer de parte dos nós optar por não adotar o protocolo, optando por manterem funcionalizando a rede, dentro dos padrões anteriormente vigentes (DE FILIPPI; WRIGHT, 2018, p. 35). A situação em questão pauta-se estritamente na natureza descentralizada, consensual e democrática da rede, permitindo que os utilizadores livremente obtenham o consenso para estruturar o sistema que lhes convém.

Ainda que pese a importância da utilização dos criptoativos para finalidades econômicas, há que se ressaltar que o escopo aqui pretendido se pauta na importância da tecnologia e suas consequências sobre a questão jurídica, especificamente sobre a tutela e garantia de direitos humanos no ambiente virtual, sem focar estritamente no seu funcionamento financeiro. Dessa forma, os criptoativos mostram-se como o ponto de início e o modelo que viabilizou a expansão da tecnologia, rumo aos modelos mais avançados de registro descentralizado.

Ao passo que uma segunda geração de *Blockchains* seria marcada pela aposição de camadas de metadados, atrelados às informações providas pelos blocos, alguns autores abordam uma suposta terceira geração, que passa a ser desvinculada, efetivamente, de criptoativos, e atentam-se, especificamente, à gestão de registros e funções em geral, como é o caso da icônica *Linux Foundation's Hyperledger* (2018), que passa a empregar a tecnologia para o gerenciamento industrial, e da *Vechain*, utilizada por diversos conglomerados industriais e comerciais para o gerenciamento logístico de produtos e sua origem (VECHAIN FOUNDATION, 2015).

A segunda geração, portanto, marca-se por fugir da simplicidade do registro de informações de processamento, assumindo as *Blockchains* funcionalidades que fogem da mera acessoriedade aos criptoativos, estabelecendo um verdadeiro ecossistema digital. Passa a ser

sem a necessidade de intermediários e contando com procedimentos seguros para sua efetivação, evitar mora ou o inadimplemento (BUTERIN, 2013, p. 13).

possível o estabelecimento de aplicativos e protocolos baseados em algoritmos em *Blockchains*, permitindo que aplicações, jogos, cadeias de gerenciamento, registro e *websites* tenham suas funcionalidades baseadas em mecanismos descentralizados (LEDGER, 2021).

Uma terceira geração de *Blockchains*, tida por alguns autores (LEDGER, 2021), baseia-se em uma gama ainda maior de utilidades para os sistemas de registro distribuído, especialmente não relacionados diretamente aos criptoativos. O ponto essencial dessa nova geração seria o estabelecimento de um protocolo de consenso *proof-of-stake*, que se baseia não na realização de uma prova de trabalho energeticamente dispendiosa, mas sim na demonstração do nó registrador à coletividade, de que possui acesso a uma quantidade de criptoativos (SALEH, 2021, p. 1162). Trata-se de um ponto essencial para a garantia da sustentabilidade das redes descentralizadas, especialmente considerando o expressivo gasto energético e a pegada de carbono que vêm atreladas ao *proof-of-work* das *Blockchains* de primeira e segunda geração⁹².

Além disso, outro ponto crucial nas *Blockchains* de terceira geração é a sua escalabilidade e interoperabilidade, permitindo que sejam utilizadas massivamente sem perdas de eficiência e, além disso, que sejam estruturados sistemas cooperativos envolvendo outras redes descentralizadas ou até mesmo redes centralizadas, facilitando a transferência de informações além da rede (LEDGER, 2021).

Dessa forma, percebe-se que o potencial de utilidade das *Blockchains* de primeira geração, apesar de possuírem projeção sobre outras searas, resumir-se-iam à questão da liberdade econômica, visto que estão atreladas diretamente à questão de gerenciamento de informações transacionais envolvendo criptoativos. As *Blockchains* de segunda e terceira geração, por sua vez, possuiriam uma gama mais ampla de aplicações, possuindo projeção, considerando os objetivos do trabalho, à questão da privacidade e da liberdade dos utilizadores, não se resumindo a tais questões.

É necessário considerar os diversos ativos que estruturam tais redes e mostram-se diretamente atrelados ao funcionamento desses sistemas de registros. A tecnologia das *Blockchains* nasce como mecanismo de viabilização do *Bitcoin*, projetando sua importância para diversos outros ativos ligados a tais tecnologias descentralizadas. Campbell-Verduyn (2018, p. 48) indica que as criptomoedas possuem especial relevância no ambiente dessas

⁹² Krause e Tolaymat (2018) procederam pesquisas com relação a quatro *Blockchains* de primeira e segunda geração (*Bitcoin*, *Ethereum*, *Litecoin* e *Monero*), sugerindo que a pegada de carbono somente dessas quatro *Blockchains*, entre janeiro de 2016 e junho de 2018, correspondeu a quase 15 milhões de toneladas de gás-carbônico.

tecnologias, por serem os primeiros empreendimentos/organizações a utilizarem efetivamente, e com relevância, as tecnologias *Blockchain*.

Don Tapscott e Alex Tapscott (2016) compreendem que existem pelo menos sete tipos de criptoativos, com cada um deles desenvolvido para certa finalidade. Inicialmente, haveria as criptomoedas, ativos utilizados como mecanismos de pagamento virtual, que se marcam por possuírem uma circulação facilitada (RODRIGUES, 2018, p. 21). Basicamente, ativos lastreados no aporte de confiança junto às *Blockchains*, especificamente sob a forma de entrega de poder de processamento à rede. Tratam-se de ativos digitais que possuem valor econômico e apresentam-se como mecanismos viabilizadores do desenvolvimento de técnicas e novas modalidades de redes *DLT*.

Tratam-se de ativos com circulação irreversível e pautadas nos mecanismos *DLT* para a averiguação e constatação da propriedade de determinado indivíduo sobre determinado ativo (devidamente individualizado, com um número de *hash* especificamente relacionado a ele, seu possuidor, transações e estampas temporais) (FOBE, 2016, p. 23).

Ainda que já reticentemente apontado na academia (RODRIGUES, 2018), há que se considerar o intuito marcante do *Bitcoin* e diversas outras criptomoedas atuarem como moedas no ambiente virtual, ainda que estas não contem com éditos de reconhecimento e imposição de circulação pelos Estados, e mostrem robustas lacunas nas suas características econômicas (YERMACK, 2015, p. 34). Algumas criptomoedas possuem atributos econômicos favoráveis à sua monetarização, apesar de existirem robustas objeções por parte dos Estados, o que por si, diante do atual estágio de política econômica tida como usual, sugere a inviabilidade do seu uso para esse fim (RODRIGUES et al, 2021, p. 74). Ainda assim, é importante considerar a relevância de se pensar na confiança atrelada à moeda, não somente sob um ponto de vista hierárquico (atrelado ao *ius imperi*), mas, especialmente, como uma forma horizontal, atrelada ao consenso social advindo da aceitação de seu uso (AGLIETTA, 2002, p. 34).

Além das criptomoedas, ativos criptografados de maior difusão, há que se pontuar também os (i) ativos de protocolo (*protocol tokens*), especificamente desenvolvidos para garantir o registro de informações em uma *Blockchain*; (ii) ativos de utilidade (*utility tokens*) ativos programáveis que se mostram necessários para interagir com determinado aspecto da rede; (iii) ativos securitários criptografados (*security tokens*), representações criptografadas e registradas em *Blockchains* de ativos mobiliários; (iv) ativos naturais criptografados (*commodity tokens*), ativos vinculados a bens naturais do mundo dos átomos; (v) ativos colecionáveis (*crypto collectibles*), ativos criptografados, que representam bens únicos ou escassos do mundo dos átomos, com natureza artística ou artes criadas no mundo virtual

também com únicos ou escassos; (vi) criptomoedas estáveis ou moedas fiduciárias criptografadas (*crypto fiat currencies* e *Stablecoins*), ativos criptografados criados ou suportados por governos ou empresas, cujo valor é vinculado com lastro em ativos ou moedas do mundo dos átomos (UHDRE, 2021, p. 66).

Michèle Finck (2019, p. 16) compreende que todas as divisões apontadas para a classificação de criptoativos poderiam ser resumidas a dois grupos gerais, os *Tokens* e as criptomoedas. Os *Tokens* seriam “essencialmente, um ativo digital que é artificialmente feito escasso e rastreado por meio de uma *Blockchain* ou tecnologia correlata”. Alguns autores sugerem que, entre os diversos tipos de *tokens*, pode haver certa fluidez, de forma que a utilidade de cada um dos tipos pode variar constantemente (HACKER; TOMALE, 2015, p. 12). Os autores fazem questão de trazer robustas indicações, apontando, por exemplo, que *tokens* utilitários podem ter componentes de investimento, indicando uma fluidez entre os gêneros distintivos de criptoativos.

Há que se indicar o papel essencial dos criptoativos na efetivação dos objetivos que envolvem a tecnologia das *Blockchains*, marcando-se como instrumentos de viabilização econômica de projetos, garantia de transações sem intermediários e desburocratizada, especulação financeira, registro de informações e viabilização de aplicações.

Portanto, as *Blockchains* mostram-se como tecnologias marcadas pela desintermediação das relações e registros, pautando-se em um modelo resistente às alterações e centrado na obtenção do consenso coletivo da rede, sob uma análise geral. Os criptoativos, em todas suas formas e as demais tecnologias *DLT* correlatas, inserem-se diretamente nessa dinâmica, lançando-se sobre as mesmas bases de funcionamento e instrumentalização, com a respectiva produção de efeitos sobre a sociedade.

Os pontos primordiais que garantem a projeção de efeitos sobre a realidade jurídica são, dentre outros, a natureza criptografada e descentralizada, garantindo a privacidade das informações e, ao mesmo tempo, lançando mão de mecanismos de transparência através da utilização do sistema de assinaturas e chaves digitais. O consenso, a prova de trabalho e as dinâmicas algorítmicas, por sua vez, garantem a imutabilidade da rede, a garantia de alterações devidamente acordadas pela maioria e, além disso, a evitação de práticas forçadas de afetação à privacidade.

3.3 Criptoativos e Tecnologias correlatas enquanto mecanismos privados de tutela e garantia de Direitos Humanos

Considerando o exposto, é perceptível a ascensão de um modelo de governança descentralizado, com indicativos técnicos, mercadológicos e acadêmicos de que os avanços da *Internet*, atrelados às redes *DLT* e criptoativos, serão maiores que os avanços singularmente concebidos da *Internet* (RAMAMURTHY, 2020, p. 293). Trata-se, portanto, da criação de uma nova espécie de circulação de informação, uma efetiva readequação da técnica informacional, especialmente desenvolvida para lidar com os problemas advindos de autoridades centrais controlando dados e seus fluxos.

Michael Abramowicz (2016, p. 359-360) descreve os sistemas pautados em *Blockchains* como fundações para os mais variados tipos de tomada de decisão, permitindo a criação de instituições jurídicas sem a votação ou o *design* de uma entidade central. Sem a possibilidade do direito estatal ser aplicado, eficientemente, no ambiente virtual, as normativas advindas da realidade técnica da *Internet* e, portanto, advindas da chamada *lex cryptographica*, acabaria por afastar de cena a lei estatal (DE FILIPPI; WRIGHT, 2018, p. 52), permitindo a instrumentação de vias adequadas à condição regente, especialmente tendo a ideia do papel vanguardista das *Blockchains* e demais tecnologias no âmbito da era informacional.

Nesse paradigma, Mellanie Swan (2015, p. 8) descreve as *Blockchains* como a Magna Carta e a Pedra de Rosetta para o ambiente informacional, provendo potencial expressivo de remodelação das atividades humanas, com especial indicativo do seu potencial jurídico. É importante citar que Lawrence Lessig, em entrevista ao *Australian Financial Review*, declarou, expressamente, que as *Blockchains* consistiriam nas mais importantes inovações do ambiente virtual desde o seu surgimento, sugerindo seu potencial enorme para aumentar eficiência produtiva e informática, além de promover direitos (EYERS, 2015).

Haveria que se falar em tais tecnologias como medidas de proteção legal por *design* (*legal protection by design*), enquanto articulações de direitos fundamentais dentro de estruturas de tecnologia da informação e comunicação, regidas por processos automatizados. A realidade não-linear do ambiente digital acabaria por desconsiderar a lei escrita e o seu potencial regulatório, demandando a adoção de vias capazes de regular eficientemente tal ambiência (FLORIDI et al, 2015, p. 170).

Analisando os diversos *White papers* de criptoativos, *Blockchains* e sistemas *DLT*, percebe-se que grande parte destes possui uma carga ideológica massiva, reiterando aquele

padrão já inicialmente feito por Satoshi Nakamoto (2008). Dessa forma, é visível o papel dessas tecnologias como formas de conter a expansão da vigilância estatal e corporativa, além de propiciar expansão dos modelos de liberdade (CAMPBELL-VERDUYN, 2018, p. 3-4). Nesses termos, as tecnologias seriam “um fenômeno social sustentado diretamente ideologias e ideias com poder de implantar e incentivar os utilizadores a agirem”⁹³ (tradução livre) ou permitir sua atuação de determinada maneira.

Portanto, ao abordarmos as referidas tecnologias, é necessário ter em mente seu papel central nas questões de governança e jurídica que envolvem a atual realidade técnica, considerando o papel da tecnologia como uma força poderosa, capaz de redefinir as atividades e seu significado (WINNER, 1986, p. 6).

Partindo da visão muito bem estabelecida por Lawrence Lessig (2006) acerca da composição das forças normativas sobre o ambiente virtual, parte-se do entendimento de que as *Blockchains*, criptoativos e tecnologias *DLT* estariam diretamente dispostas como formas normativas do ambiente digital, regulando, de fato, diversas questões, visão esta que é compartilhada tanto por Campbell-Verduyn (2018, p. 4), quanto por Primavera De Filippi e Aaron Wright (2018, p. 193). Compondo-se de força normativa, de fato, no ambiente virtual, portanto, dotado de poder informacional para dispor códigos e reger as dinâmicas do mundo dos *bits*, por meio de uma atuação arquitetônica, compreende-se a possibilidade de tais tecnologias servirem como mecanismos de garantia e tutela de direitos humanos, dada suas especificidades.

Dispondo-se como mecanismos com potencial de produção de efeitos sobre a privacidade, liberdade e outros direitos dos indivíduos, o poder organizacional de tais tecnologias é marcante, vista a sua capacidade de influenciar sobre o comportamento individual (JOHNSON, 1985, p. 65), especialmente considerando seu papel arquitetônico e, portanto, cogente aos indivíduos sujeitos à realidade virtual que se mostra afetada por tais técnicas.

Primavera De Filippi e Samer Hassan (2016, p. 1-2) compreendem que a tecnologia das *Blockchains* e outras mais teriam um enorme potencial de assumir as funcionalidades das normas legais, considerando sua natureza auto executiva e sua correlação direta a uma série de consequências decorrentes do seu baseamento na rede *Blockchain* (garantia à privacidade, liberdade, governança democrática e aberta). No entanto, considerando o exposto, é possível projetar um potencial ainda maior a tais tecnologias, levando em conta sua natureza técnica, enquanto “normas tecnicamente adequadas” (DE FILIPPI, HASSAN, 2016, p. 3), o que garante

⁹³ “Technologies as deeply social phenomena that are underpinned by specific ideologies and ideas with the power to constitute the interests and incentives of their users” (tradução livre).

mecanismos mais eficientes de efetivação e, além disso, ainda aponta para características mínimas, capazes de garantir a legitimidade de tais meios.

Alguns autores apontam os prováveis malefícios da ascensão dessas tecnologias no ambiente digital, sugerindo que a sua natureza tecnicamente adequada ao meio digital levaria à formação de um “Tecno-leviatã” (CAMPBELL-VERDUYN, 2018, p. 8), com uma capacidade impressionante de impor padrões aos indivíduos regulados. Nesse ponto, apesar de reconhecer a dualidade da técnica e seus efeitos sobre todas suas manifestações, há que se pontuar o papel inovador de tais tecnologias dentro da realidade do poder informacional, contando com mecanismos, nunca antes vistos, para garantir uma mínima proteção aos utilizadores, como a própria questão da dinâmica democrática da rede.

Há que se considerar que a emergência dessas novas tecnologias representa uma alteração nos paradigmas de poder, marcando uma efetiva remodelagem na forma pelo qual o poder informacional pode ser exercido, passando de uma realidade epistocrática para uma realidade com mais traços democráticos. Nesse sentido, Campbell-Verduyn (2018, p. 8-9) compreendem que as *Blockchains* e tecnologias correlatas fazem emergir novos atores de poder ao mesmo tempo que fragiliza alguns. Haveria, assim, uma dinâmica de maior concentração de poder junto a agentes não estatais, auxiliando-os a adquirir uma maior capacidade de interação e efetividade de suas intenções no ambiente virtual.

Haveria, nesse sentido, um desempoderamento de atores, usualmente detentores de poder programacional, especialmente aqueles agentes privados, permitindo uma maior dissolução do poder frente à coletividade de utilizadores e à uma expansão da dignidade dos utilizadores no ambiente virtual. Diversos autores reafirmam o papel primordial dessas novas tecnologias na ampliação dos poderes dos indivíduos e redução da capacidade de intervenção de agentes poderosos (SIMSER, 2015, p. 158) (PIETERSE, 2012). Portanto, há que se visualizar o papel de tais tecnologias na afirmação de direitos humanos, em especial, considerando o impacto dessas tecnologias sobre a privacidade e sobre a liberdade humana, elos centrais que, inclusive, fizeram parte do substrato ideológico que fundou o *Bitcoin* e a sua *Blockchain*.

Além de seu impacto geral sobre os utilizadores, haveria que se considerar o impacto dessas sobre diversos grupos humanos, historicamente lesionados (CAMPBELL-VERDUYN, 2018, p. 8-9), garantindo a esses mecanismos adequados para a tutela de seus direitos, dentro da dinâmica informacional. Sob um aspecto geral, as referidas tecnologias teriam papel essencial na limitação e responsabilização de atores poderosos do ambiente virtual (AMMOUS,

2015, p. 19-20), (ATHEY, 2015). Trata-se, nas palavras de Bina Ramamurthy (2020, p. 105), da democratização da privacidade.

As redes *Blockchain* seriam marcadas por um modelo de igualdade por design (AL-SAQAF; SEIDLER, 2017, p. 343-344), no qual o seu estabelecimento sobre códigos de fontes abertas (livres e *open source*) garantiria a ausência de mecanismos de diferenciação entre os nós, pautados em qualquer característica não técnica. Portanto, não é possível estruturar privilégios ou impor condições inferiores aos nós, permitindo a estruturação de um sistema neutro, no qual os nós “são tratados igualmente, e não são abusados por um elemento central ou poderoso”⁹⁴ (tradução livre). O que surge, por sua vez, é um acesso não paritário dos indivíduos aos meios que propiciam tais tecnologias, quais sejam, *Internet* acessível e estável, assim como *hardwares* com capacidades de processamento mínimo, um problema que pode minar o potencial efetivo dessa tecnologia atingir os indivíduos, especialmente considerando fragilidades de telecomunicação e acesso a bens de informática em países subdesenvolvidos (AL-SAQAF; SEIDLER, 2017, p. 345).

Portanto, os criptoativos, *Blockchains* e tecnologias correlatas trazem um modelo de governança pautado na *Lex cryptographica*, uma resposta que se mostra tecnicamente adequada para enfrentar as novas ameaças aos direitos humanos, advindas do manejo ilegítimo do poder programacional. *Pari passu* ao poder de violação de direitos humanos, advindo das práticas de vigilância e controle empreendidas por meio de protocolos e algoritmos, as referidas tecnologias emprenderiam barreiras robustas, auto executáveis e que não dependeriam diretamente da tutela estatal (DE FILIPPI; WRIGHT, 2018, p. 95). Haveria que se falar, portanto, na ascensão de um modelo tecnocrata, que opera por meio de estruturas técnicas baseadas em códigos e algoritmos.

Dessa forma, haveria que se visualizar a possibilidade dos utilizadores de criptoativos ou mesmo utilizadores de sistemas, pautados em *Blockchain*, de possuírem uma tutela de fato sobre a sua privacidade e liberdade, a partir do momento em que estivessem vinculados ao anonimato/pseudoanonimato dos registros envolvendo tais tecnologias, isso ampliado pela ausência de um controle centralizado. Os riscos advindos de uma realidade descentralizada de governança caem por terra diante das *Blockchains* (especialmente as de natureza pública), em razão da liberdade de participação da rede e a procedência das medidas na rede sob a regência de uma ordem democrática, que depende do consenso, livremente obtido, para proceder com alterações.

⁹⁴ *This neutrality ensures that] all are treated equally and are not abused by a central or more powerful element.*

A atuação dessas tecnologias, na tutela de direitos, tomaria a forma de uma ação social individualizada, na qual a atuação conjunta de diversos indivíduos, sem um controle centralizado, permite um direcionamento desejável do grupo, rumo a um objetivo específico, tendo como base os protocolos que o estruturam e definem os direcionamentos possíveis. Dessa forma, a atuação individual dos utilizadores de *Blockchains* e outras tecnologias, direcionando-se ou efetivamente à tutela dos direitos ou objetivando realização de meras operações comerciais (como exemplo, o minerador, que não busca privacidade diretamente, mas, sim, recompensas econômicas do sistema) permite a construção de uma tutela coletiva, que desencadeia uma maior robustez do sistema na garantia do anonimato ou pseudoanonimato, ao passo que há incremento na democraticidade dos mecanismos de consenso, especialmente considerando a estrita relação entre o aumento da descentralização e o aumento da resiliência da rede.

Um ponto que merece atenção é o desvirtuamento das redes descentralizadas por meio de aglomerações de poder de processamento,⁹⁵ em um número reduzido de agentes com capacidade de controle, o que refletiria no manejo das redes por menos participantes, especificamente aqueles que controlam maior poder de processamento de dados (DE FILIPPI; WRIGHT, 2018, p. 40). Apesar da insegurança trazida por esse controle, ressalta-se que ele não tem impacto direto sobre a privacidade dos dados registrados e, indiretamente, não haveria vantagem econômica em promover alterações robustas que desvirtuassem a rede e pudessem afetar a liberdade dos utilizadores atreladas à sua utilização. Apesar da problemática, há indicativos de que as redes possuem capacidade de manejo dessa situação.

Um ponto que merece atenção é a limitação de acesso dos indivíduos a tais tecnologias, que se mostram diretamente vinculadas a custos econômicos de utilização, o que, apesar de trazer benefícios consideráveis à dignidade humana, pode limitar seu espectro de atuação. Apesar da expansão das vias digitais e um considerável crescimento de acesso dos indivíduos à *Internet* e suas aplicações, há que se considerar um acesso ainda sujeito a algumas restrições, quando pensamos na utilização de criptoativos, *Blockchains* e tecnologias correlatas.

A composição de uma rede sólida e capaz produzir os efeitos esperados sobre a privacidade humana e a liberdade depende, conforme já indicado, da existência de um vasto número de nós validando registros e, portanto, caracterizados mecanismos mínimos de controle democrático do consenso. Nesse sentido, apesar da possibilidade de os indivíduos, livremente,

⁹⁵ Refere-se aos chamados *mining pools*, agrupamento de estruturas de processamento, que são estruturados para ganhar vantagem competitiva nas atividades de mineração e, por consequência, obter rendimentos com essa atividade.

programarem redes e construïrem protocolos de *Blockchains*, que ainda é especialmente limitado pelo baixo nível de instrução técnica informacional geral da sociedade, tais redes não contariam com robustez suficiente para fazer frente às dinâmicas violatórias do poder programacional.

Somente as *Blockchains* públicas, com algumas ressalvas a certas permissionárias, possuiriam capacidade de, efetivamente, prover os benefícios ora analisados à dignidade humana, de forma que a participação nessas redes, seja como nós ou tendo seus dados/transações registrados, depende de custos diretos ou indiretos. Custos de processamentos, custos de registro (usualmente chamados de taxas de registro *fees* ou *gas fees*) devem ser considerados, uma vez que, ao menos em um primeiro momento, não se vislumbra o fomento ou produção dessas tecnologias totalmente abertas aos indivíduos, com custos subsidiados ou mesmo providos, totalmente, pelo Estado, organizações ou pela própria sociedade coletivamente concebida.

Além disso, há que se pontuar, conforme expressa Campbell-Verduyn (2018, p. 25), o expressivo impacto da exacerbada carga de utilização econômica dos criptoativos, especialmente para finalidades de especulação, medida que acaba cooptando a *Blockchain* para finalidades que não aquelas capazes de projetar efeitos sobre a dignidade humana. Citamos o exemplo clássico da *Bitcoin*, que nasce como uma tecnologia relacionada à supressão de esferas intermediárias e tutela da privacidade por meio de transações virtuais, no entanto, passa por uma desvirtuação, sendo integrada à economia formal como ativo especulativo, sem projeções relevantes como moeda.

Ainda assim, há que se considerar sua relevância, demonstrando-se como tecnologias capazes de fazer frente às violações promovidas pelo poder programacional e tendo origem e funcionamento distintos da regulação jurídica estatal, indicando-se como um meio tecnicamente adequado e provindo do ambiente privado. Portanto, ainda em seus momentos pós natais, ainda há consideráveis limitações à expansão massiva da sua utilização, no entanto, é necessário já ponderar as suas qualidades, efeitos e possíveis projeções.

Um ponto que merece ser destacado é a inexistência de uma dinâmica disruptiva quanto à tutela jurídica dos direitos humanos quando pensamos nas *Blockchains*, criptoativos e tecnologias correlatas. Conforme muito bem demonstrado por Campbell-Verduyn (2018, p. 31), uma visão inicial das criptomoedas e seus sistemas indicava uma posição de rompimento com a realidade vigente, especialmente considerando as questões de soberania e moeda, visão que é totalmente superada após uma concepção mais madura dessas tecnologias e seus efeitos. Nos termos já previstos por Lawrence Lessig (2006, p. 666), a regulação *cryptographica* dos

direitos humanos mostra-se apenas como mais uma força deontológica dentro do ambiente virtual, não excluindo a incidência das normas jurídicas e, ao mesmo tempo, firmando apenas mais uma via para se atingir os semelhantes fins, tendo a via aqui abordada maior apego à realidade técnica circundante.

Nesse sentido, é necessário considerar que as tecnologias apontadas podem existir paralelamente à tutela jurídica provida pelo Estado, mostrando-se sujeitas às condições ali impostas e, assim, adequadas a um sistema jurídico. Isso significa que, apesar da atuação auto executória e da efetividade das suas práticas, tais tecnologias e sua atuação não poderiam ser excluídas da apreciação jurisdicional, até mesmo como medida capaz de garantir a fidedignidade dos resultados ao ordenamento jurídico e evitar produção de efeitos maléficos à integralidade do ordenamento jurídico.

Para tanto, cumpre indicar, especificamente, o impacto das referidas tecnologias na tutela e efetivação da privacidade e da liberdade no ambiente virtual, apontando em qual medida e como tais tecnologias possuiriam condições técnicas para empreender a tutela da dignidade humana no espaço virtual. As tecnologias em questão teriam uma projeção sobre diversas searas, não se limitando mais ao registro de criptoativos e suas transações, mostrando-se como um modelo arquitetônico capaz de embasar *websites*, algoritmos de gestão de dados, *softwares* e outros mais, isso sem contar na possibilidade de assimilação dessa tecnologia pelo Estado, como de fato vem ocorrendo, sendo utilizada para autenticação de documentos (RUBINSTEINN, 2021) ou mesmo para um sistema de voto eletrônico (NIWA, 2019).

A Organização das Nações Unidas, desde o ano de 2016, compreende a utilidade de tais tecnologias aos seus programas e painéis relacionados aos direitos humanos, tendo sido criado, no ano de 2016, um programa de engajamento das Nações Unidas à tecnologia das *Blockchains* (VEIT, 2019, p. 31-32), assim como um grupo de especialistas multidisciplinares para a proposição de soluções envolvendo as tecnologias (ONU, 2020). Vale, ainda, citar a Comissão relacionada às *Blockchains* para o desenvolvimento sustentável, que, desde o ano de 2017, busca desenvolver aplicações das tecnologias voltadas aos benefícios coletivos de tais tecnologias (ONU, 2021).

3.3.1 Privacidade

A privacidade nativa é considerada a melhor resposta operacional para proteger os direitos fundamentais de proteção de dados e, ainda, garantir as dinâmicas e fluxos informacionais (ROUSSEAU; SAUREL, 2014, p. 78), mostrando como uma resposta à

garantia da privacidade dos utilizadores da rede, embebida nas fontes da técnica informacional, comungando uma base ideológica que, dentro da dinâmica programada, regerá a relação *input* e *output*, para que chegue a um resultado favorável aos utilizadores.

Portanto, ao concebermos o papel de tecnologias *DLT*, como o caso da *Blockchain* e diversos outros mecanismos atrelados a criptoativos, percebe-se que a composição algorítmica, a base matemática sobre a qual será estruturado o seu funcionamento, tem um paradigma subjetivo que regerá os resultados da sua atuação. Portanto, além da simples objetividade dos paradigmas matemáticos, haveria uma determinação da comunidade desenvolvedora/mantenedora para que toda a estrutura algorítmica não permita violações à privacidade, estruturando barreiras resistentes a tais práticas. E, em grande parte da comunidade, tais paradigmas adviriam de medidas democráticas de composição, formadas pelos diversos nós formadores da rede distribuída.

Fala-se em *Privacy by Design* como uma forma de embeber o direito da técnica vigente, dotando mecanismos protetivos de direito das capacidades regulatórias pautadas no poder programacional e na eficiência dos algoritmos (GREER, 2011, p. 146-147). Assim, há a estruturação de elementos capazes de proteger direitos humanos na técnica vigente, garantindo meios facilitados de execução e até mesmo situações de impossibilidade de condutas lesivas, que fujam do padrão imposto pelo mecanismo lógico-matemático. Sob esse paradigma, é necessário pontuar a utilidade das novas tecnologias na proteção da privacidade, especialmente considerando a falibilidade do modelo tradicional de tutela pelo ordenamento jurídico, que depende de estruturas com modelos temporalmente extensos e não possuem qualquer escalabilidade em face do contexto do *Big Data* (GASSER, 2016, p. 67).

Mais do que tecnologias que são desenhadas sob o prisma da privacidade, há que se identificar os criptoativos, tecnologias *DLT* e *Blockchains* como tecnologias que realçam a privacidade (*Private Enhancing Technologies*), garantem o anonimato e a confidencialidade das informações, sem estabelecerem suas bases sobre sistemas centralizados e estruturando mecanismos que previnem a exposição (PERRY; RODA, 2017, p. 78). Enquanto as tecnologias de privacidade por *design* estruturam-se sobre sistemas que evitam o tratamento de dados não autorizado, em sua grande maioria, pautados em mecanismos e aplicações que promovem adequação às normas de proteção de dados pessoais, impedindo exposições por meio de um controle centralizado do desenvolvedor/gerenciador. Ou seja, a privacidade é protegida sob a forma da confiança de que determinada entidade gestora dos dados não possui estruturas algorítmicas ou práticas que revelarão aqueles dados protegidos.

As tecnologias que realçam a privacidade, por sua vez, marcam-se por uma dinâmica ativa na sua garantia, estruturando um ambiente com tecnologias conjugadas que garantem a intimidade, o anonimato dos utilizadores e a não exposição de conteúdos sob um ponto de vista descentralizado, portanto, independente da confiança para com intermediários (PENG, 2014, p. 16-17). Ou seja, a privacidade aqui é protegida sem a necessidade de confiar informações a um terceiro, uma vez que a tecnologia se pauta na composição de uma rede descentralizada, na qual cada um dos nós da rede é tecnicamente impossibilitado de violar a privacidade e, conjuntamente, não seria do interesse dos nós promover tal violação.

Barrientos-Parra (2011, p. 65) indica que o aumento na eficácia dos sistemas passa a exigir uma maior centralização sobre informações e dados, medida esta que seria diretamente relacionada ao aumento das práticas de controle e vigilância. Diante do exposto, percebe-se que há potencial de utilidade das tecnologias em questão para empreender tutela sobre os direitos humanos, especialmente considerando a sua descentralização e, assim, ruptura com uma dinâmica que promove lesões à privacidade dos utilizadores da rede.

Ao abordar a utilização de tecnologias *Blockchain* e outras correlatas, à garantia do direito à privacidade, busca-se alcançar a máxima de proteção à privacidade por meio de medidas de automatizadas, que não exijam ações dos utilizadores ou mesmo do Estado, de forma que o próprio sistema é capaz de proteger a privacidade do utilizador por meio da estrutura algorítmica.

A privacidade deve estar estruturada dentro dos sistemas de informação e das práticas negociais, não sendo simples adições ou construção anexas, conforme indicam Rousseaux e Saurel (2014, p. 78). É necessário que a arquitetura dos sistemas tenha a proteção da privacidade como um elemento essencial, uma parte integral e nativa àquela estrutura virtual.

Quando falamos em tecnologias de máscaras de identidade ou pseudoanonimato, falamos em “válvulas digitais”, que permitem o fornecimento de dados, mas ainda preservando a privacidade, como o caso da *Blockchain*, que, amparada na criptografia, permite informar dados, mas sem comprometer dados sensíveis de utilizadores, embora muitos autores discordem disso e apontem as *Blockchains* como capazes de, mesmo sob essas “máscaras”, informar dados sensíveis (PERRY; RODA, 2017, p. 78). As estruturas como as *Blockchains* pautam-se nas chamadas provas de conhecimento zero, limiares informativos que permitem o registro de informações, sua circulação e compreensão de sua origem e autenticidade sem, no entanto, identificar o indivíduo ou seus dados sensíveis.

Satoshi Nakamoto (2008, p. 6) expõe em seu *paper* o nível de privacidade oferecido pela *Blockchain Bitcoin*, indicando que o fluxo de informações é limitado por meio da

imposição de anonimato das chaves públicas envolvendo os registros. Basicamente, torna-se possível garantir dados de acesso público, como a existência de uma transação e a quantidade transacionada, mas ausente de qualquer informação que relacione aquele registro a uma pessoa. Ainda que pese o valor da medida de pseudoanonimato garantida pela rede, há que se ressaltar a possibilidade de rastreamento e interligação das transações com os indivíduos, o que sugeriria a capacidade de relativização da privacidade em *Blockchains* que adotam o modelo de pseudoanonimato, medidas que poderiam ser empreendidas pelo Estado, mediante a incidência de práticas sobre agentes intermediários, como o caso das casas de câmbio de criptoativos (*Exchanges*) (CAZABET et al, 2017, p. 169-172).

Tratam-se de esquemas que tornam anônimos os dados pessoais, ao mesmo tempo em que mecanismos para averiguação da autenticidade da fonte e, sob algumas circunstâncias, até mesmo permitir o acesso à identidade real dos utilizadores e demais dados necessários ao interesse público. Esse nível de transparência mostra-se incapaz de lesionar a privacidade e, além disso, marca-se pela sua utilidade aos sistemas descentralizados. Conforme preceitua Mozorov (2013, p. 16), a privacidade para as sociedades deve ser necessária para garantir um modelo democrático e, ao mesmo tempo, não ser tão expressiva que sufoque a circulação de informações necessárias para a valoração de políticas, formação de opiniões e garantia dos demais direitos humanos.

O nível de pseudoanonimato oferecido pelos criptoativos, *Blockchains* e tecnologias correlatas indica um grau de privacidade que coaduna com o exposto pelo autor, garantindo proteção aos utilizadores, ao mesmo tempo em que não promove, torna o direito à privacidade um direito absoluto. Ainda assim, ressalta-se que Primavera De Filippi e Aaron Wright (2018, p. 68) entendem que a transparência, oferecida pelo pseudoanonimato das *Blockchains*, permite novas formas de vigilância por parte dos Estados e organizações privadas, fazendo uso de metadados e técnicas de controle e rastreamento capazes de violar mesmo a privacidade dos dados registrados nos sistemas descentralizados.

Ainda assim, é necessário pensar que, dentro da estrutura jurídica, passa a ser necessária a imposição de limites e ponderações aos direitos, enquanto um pressuposto básico de harmonização da dignidade humana coletivamente concebida, o que dependeria da capacidade do Estado, quando dotado dos procedimentos formais para tanto, possuir mecanismos que permitam adentrar, legitimamente, sobre a esfera da privacidade dos indivíduos em nome do interesse coletivo.

Os criptoativos, nas palavras de Puzis et al (2019, p. 194), possuiriam capacidades expressivas para preservar a privacidade dos utilizadores, especialmente considerando sua auto

executoriedade, o que indica o autor ser semelhante ao *enforcement* (executoriedade) das normas jurídicas. A capacidade de tutela da privacidade atingiria níveis ainda mais absolutos ao se referir a criptoativos e *Blockchains*, especializados na proteção das exposições, como o caso da *Blockchain* Monero, que possui métodos ainda mais eficientes para preservar os dados registrados, evitando exposições até mesmo de informações tidas como públicas em outras *Blockchains*, como o caso de informações transacionais básicas, como o valor e chave pública dos envolvidos (PUZIS et al, 2019, p. 184).

Ressalta-se que a possibilidade de uso dessas tecnologias, para a garantia da privacidade no ambiente digital, mostra-se capaz de, ao incorporar uma realidade tecnicamente adequada, empreender mecanismos eficientes e massificados de tutela, independentemente de práticas pós-violatórias usualmente relacionadas. Nos termos abordados anteriormente, fica visível que os empreendimentos algorítmicos, típicos das *Blockchains* e das tecnologias correlatas, seriam capazes de trazer, aos seus utilizadores, um nível alto de proteção da privacidade no ambiente digital, demarcando-se como um mecanismo com indícios de efetivação da dignidade humana.

Os dados registrados em *Blockchains* e tecnologias correlatas, sejam eles quais forem ou qual seja sua finalidade, estariam adstritos ao seu possuidor, considerando a criptografia que reina sobre os dados e, sobretudo, a sua proteção por algoritmos seguros, sob o ponto de vista cibernético, de difícil acesso por terceiros. A sua natureza descentralizada evitaria seu acesso por parte de agentes tipicamente marcados por práticas de vigilância, como Estados e corporações do mundo digital, eliminando um elo que se mostra central nas práticas de violações à privacidade dos utilizadores da *Internet*. Ao passo que os dados estejam em registros descentralizados, devidamente criptografados, garante-se o pseudo-anonimato das informações, o que garantiria a impossibilidade de utilização direta dos dados para vinculação com pessoas físicas.

Apesar do modelo adotado geralmente pautar-se no pseudo-anonimato, as redes se estruturam para proteger a privacidade dos utilizadores e dos dados ali registrados, sejam esses dados escolhidos pelos utilizadores ou mesmo dados de transações atrelados a criptoativos (GUPTA, 2020, p. 2015).

Dessa forma, o elo central da garantia à privacidade, pelas tecnologias em questão, encontra-se na criptografia atrelada aos dados registrados das *Blockchains* e demais *DLTs*, juntamente com sua natureza descentralizada, e o pseudo-anonimato que marca os registros. O que denota, portanto, uma realidade de efetivação da privacidade por instrumentos arquitetônicos, efetivamente manejando estruturas impossíveis ou de difícil sobreposição ou ultrapassagem para garantir espaços privados.

Nos termos indicados na secção anterior, as características das tecnologias, em especial, sua auto exequibilidade e independência com relação à dinâmica do mundo dos átomos demarcariam uma aderência ímpar desse mecanismo de garantia da dignidade, sob uma ótica preventiva, o que seria improvável de se visualizar em uma dinâmica ordinária de tutela e efetivação da privacidade, realizada pelo Estado.

Apesar da natureza ímpar de proteção provida à privacidade por meio das referidas tecnologias, alguns autores ressaltam a incompatibilidade dos sistemas de pseudoanonimato com as normativas estatais, especialmente considerando a capacidade de efetivação do interesse público e as dificuldades de adequação dessas estruturas às exigências das normas de proteção de dados pessoais (MILLARD, 2018, p. 845). Gasser (2016, p. 66) sugere que as tecnologias mais recentes, no ambiente da proteção da privacidade, têm se mostrado capazes de entrar em consonância com o ordenamento jurídico, estruturando-se como sistemas responsivos aos diferentes tipos de riscos advindos dos dados protegidos, situação que poderia, ou mesmo já estaria, ser incorporada às tecnologias descentralizadas, especialmente considerando a dinâmica regulatória que passa a incidir sobre as *Blockchains* e criptoativos.

Diversas tecnologias já apontadas mostram-se incapazes de lidar com essa situação intersticial, apontando para caminhos extremos de tutela da privacidade, como o caso das práticas de encriptação isoladas e o anonimato, que permitem a proteção da privacidade e, ao mesmo tempo, garantem condições mínimas para a sua ponderação, caso tal situação chegue ao Poder Judiciário.

Um ponto que merece atenção é o embate entre as normas protetivas de dados pessoais e as atividades promovidas pelas *Blockchains* e outras tecnologias semelhantes, especialmente considerando a inexistência de entes centralizados, motivo pelo qual alguns autores referem-se como o ponto primordial de incompatibilidade entre a norma estatal e as *Blockchains* (MILLARD, 2018, p. 844). Ainda que preze a relevância das normas de proteção dos dados pessoais, a dependência de estruturas centralizadas abre um espaço massivo para a realização de violações à privacidade, adentrando na mesma questão anteriormente disposta, qual seja, a existência de elos centrais sujeitos à incidência normativa ou mesmo incidência do poder programacional, que poderia resultar em práticas de vigilância capazes de lesionar o utilizador.

Mesmo diante da legitimidade dos interesses públicos envolvidos na atividade Estatal, considerando as reiteradas práticas de vigilância, é necessário perceber a existência de uma visão marcante dos autores de que a privacidade é garantida por meio das *Blockchains*, ou outros meios que garantam a descentralização e desintermediação das atividades, em especial

pela suscetibilidade a ataques ou mesmo mau uso daqueles dados confiados a agentes intermediários (ZYSKIND et al, 2015, p. 184).

Nas palavras de Gurses et al (2016, p. 11), o fenômeno da adoção da *Lex Cryptographica*, como resposta às práticas violatórias da privacidade dos utilizadores da *Internet*, marca-se por uma profunda despolitização, em especial, fruto das exposições dos esquemas de vigilância massiva feitas por Edward Snowden. Ainda assim, é necessário considerar a possibilidade de tutela da privacidade através das tecnologias aqui apresentadas, sendo empreendidas no ambiente digital por parte do Estado, adotando medidas autoexecutivas sem necessidade de socorrer-se ao ambiente físico e ao poder de fato, sugerindo um “relacionamento mutualmente produtivo” entre as ferramentas de privacidade e o ordenamento jurídico, permitindo uma atuação estratégica e capaz de, efetivamente, responder à escalabilidade da vigilância empreendida na era do *Big Data* (GASSER, 2016, p. 67).

Trata-se, aqui, do empreendimento de um modelo híbrido de tutela da privacidade (NISSSIM et al, 2018, p. 711), fazendo uso de tecnologias descentralizadas, devidamente compatibilizadas com o ordenamento jurídico, fornecendo ao direito estruturas tecnicamente adequadas para responder às violações empreendidas na rede e garantindo a integração do ordenamento ao ambiente digital sem limitações à sua exequibilidade, garantindo a estruturação de um “sistema de governança” que, por meio da integração tecnológica às forças regulatórias, promove a tutela, de forma eficiente, da privacidade online (MAYER-SCHÖNBERGER, 2011, p. 1882).

Nesse sentido, expõe Gasser (2016, p. 69):

Re-imaginando a relação entre tecnologia e lei relativa à privacidade na era digital, essa deve ser vista como um componente-chave de um esforço maior que visa abordar a atual crise de privacidade digital de forma mais holística. Sob as condições contemporâneas de complexidade e incerteza, o espaço de solução para os desafios multifacetados da privacidade de nosso tempo precisa fazer mais do que tratar os sintomas dos males de privacidade discretos. Ele precisa combinar abordagens, estratégias e instrumentos que abrangem todos os modos de regulação disponíveis no espaço digital, incluindo tecnologia, mercados, normas sociais e a lei.⁹⁶

⁹⁶ “*Reimagining the relationship between technology and privacy law in the digital age should be seen as a key component of a larger effort aimed at addressing the current digital privacy crisis more holistically. Under contemporary conditions of complexity and uncertainty, the solution space for the multifaceted privacy challenges of our time needs to do more than treat the symptoms of discrete privacy ills. It needs to combine approaches, strategies, and instruments that span all available modes of regulation in the digital space, including technology, markets, social norms, and the law*” (tradução livre).

É importante ressaltar que o ritmo das inovações avança além daquele assimilado pela seara jurídica, o que reflete em uma dinâmica muito mais ágil de resposta a eventuais falhas e problemas na efetivação da privacidade.

O que merece ser ressaltado, atendendo à própria base filosófica que ordena a pesquisa, seria a projeção de efeitos maléficos decorrentes da técnica das *Blockchains* e tecnologias correlatas sobre a privacidade, especialmente entendendo que essas tecnologias se pautam em uma cadeia de blocos que se acrescentam, sem potencial de destruição de dados e, portanto, estruturando um sistema de registros “eternos” (GUPTA, 2020, p. 217-218). Nesse sentido, haveria o risco de, superadas as barreiras criptográficas que evitam as exposições de dados nas *Blockchains*, públicas ou permissionárias, ocorrerem exposições de informações privadas, situação que, apesar de ser remota, em razão da constante atualização dos protocolos dos sistemas, devem ser consideradas.

Apesar de algumas possíveis falhas e espaços para vazamentos (GUPTA, 2020, p. 2015-218), especialmente aqueles relacionados ao pseudo-anonimato (TIANJIAO; CHUNJIE, 2019, p. 2046-2048), nos termos anteriormente já trazidos, tratam-se de tecnologias que possuem potencial de utilização para fins de garantia e efetivação do direito à privacidade na *Internet*. Os mecanismos apontados como falhas seriam, sob os pontos indicados, espaços de abertura para ponderação dos sistemas, que se pautam em modelos arquitetônicos de efetivação da privacidade, permitindo espaços de abertura para integração com o ordenamento jurídico.

3.3.2 *Liberdade*

A efetivação dos diversos aspectos da liberdade humana na *Internet*, por meio dos criptoativos, *Blockchains* e tecnologias correlatas, correlaciona-se, diretamente, com a capacidade dessas tecnologias promoverem espaços de privacidade, considerando a relação direta entre esses dois direitos. Não somente isso, há que se considerar, também, os impactos autônomos das tecnologias sobre a questão da liberdade, especialmente relacionada às características essenciais que marcam o seu funcionamento.

A descentralização da rede e seu modelo pautado na inexistência de autoridades centrais mostra-se como um fator essencial para a garantia da liberdade dos utilizadores, seja a liberdade de pensamento e expressão, a liberdade econômica ou até mesmo a liberdade de navegação, quando pensamos na possibilidade de padronização de *websites* e navegadores de *Internet* centrados na tecnologia distribuída. A utilização desses *softwares* ou mesmo a estruturação da arquitetura da rede, com base em tecnologias descentralizadas, garantiria a existência de

sistemas autônomos, por meio dos quais seria possível realizar transações ou mesmo registrar informações digitais com garantia e velocidade, reduzindo ou mesmo suprimindo a necessidade de supervisão humana (DE FILIPPI; WRIGTH, 2018, p. 44).

A supressão ou, ao menos, redução dos níveis de intermediação no ambiente digital acabaria por reduzir espaços para a imposição de medidas violatórias de direitos, seja pelo Estado ou pelo próprio elo intermediário, de forma que se garantiriam menos hipóteses de interferências sobre os indivíduos no ambiente digital. Apesar de alguns autores sugerirem o papel institucional de agentes intermediários na efetivação da liberdade na *Internet* (MONTERO; ENIS, 2011, p. 22), atuando como elos centrais para a incidência do ordenamento jurídico no ambiente virtual, há que se pontuar a expansão da alegabilidade e das reiteradas práticas de violação da liberdade na *Internet*, como muito bem indica Julian Assange (2013, p. 121), e as diversas delações trazidas pelo site *Wikileaks*, especialmente centradas no ocultamento das práticas, o que, por si, já traria dificuldades robustas ao emprego da norma e do sistema judiciário para a tutela de tais violações.

Hughes et al (2018, p. 65) apontam a tecnologia *Blockchain* como uma resposta tecnológica capaz de garantir a liberdade individual face à realidade algorítmica que rege o ambiente virtual. Através do seu potencial de empoderamento, as *Blockchain* teriam a capacidade de aumentar a autonomia individual na *Internet* e a confiança entre os indivíduos, o que produz efeitos sobre a liberdade socialmente concebida. Nesse ponto, o impacto das *Blockchains* seria ainda maior, considerando Estados com reiterada prática de censura e um ambiente virtual tido como pouco livre (FRENI et al, 2020, p. 179).

A liberdade de navegação, usualmente violada por bloqueios no acesso a *websites*, aplicações digitais e conteúdos digitais empreendidos por medidas executivas (algoritmos), intermediários da rede ou pelos próprios Estados, mostra-se como uma prática usualmente aplicada no ambiente virtual, especialmente em regimes com baixo apego democrático, como o caso da China e Rússia (TAPSCOTT; TAPSCOTT, 2016, p. 223). Especificamente quanto à liberdade de navegação, percebe-se um relacionamento mais estrito dessas práticas com as figuras estatais, apesar de existirem medidas dessas espécies oriundas de agentes privados, como o caso de redes sociais. Os referidos autores ressaltam que as *Blockchains* e tecnologias correlatas teriam papel essencial para se opor a tais medidas, abrindo espaço para a estruturação de *websites* e aplicações descentralizados, impossíveis de serem suprimidos, tirados do ar ou alterados, incentivando a liberdade de navegação e expressão por meio de registros incapazes de serem destruídos ou suprimidos por Estados e corporações.

A resistência das *Blockchains* a alterações que não advenham do consenso da rede acaba por permitir um acesso constante e seguro a informações armazenadas, desde que o indivíduo tenha acesso à chave criptográfica para obter a informação armazenada. O direito dos indivíduos, livremente, conhecerem e obterem informações, relacionado ao que pontuamos como liberdade de navegação, passa a ter especial mecanismo de efetivação junto às tecnologias em questão, garantidos meios materiais para que o indivíduo possa efetivar essa faceta da sua dignidade no ambiente virtual.

É necessário pontuar que, apesar da sua relevância, há que se conceber o potencial ilícito de utilização dessas tecnologias, seja para a divulgação de conteúdos ilícitos ou mesmo empreendimento de atividades ilegais. No aspecto da liberdade de navegação, citamos, como exemplo, a divulgação de obras de cunho racista, xenofóbico e antidemocrático por intermédio de redes descentralizadas, valendo-se dos seus atributos para fugir de limitações e até mesmo perseguições penais. Dessa forma, a estruturação de redes, baseadas em pseudo-anonimato, mostra-se necessária e útil para a sua integração ao ordenamento jurídico, permitindo que, em situações esporádicas, como o caso de ilicitudes, seja possível romper o anonimato da rede para alcançar os indivíduos.

Nesse ponto, há que se ressaltar que já houve práticas dos Estados, no sentido de adentrar a questão do pseudo-anonimato, para empreender investigações com indivíduos cometendo crimes, como o caso do *website Silk Road* (SIMSER, 2015, p. 164), que realizava a venda de produtos ilícitos na *Internet* através de negociações com *Bitcoins*. Dessa forma, fica visível que, apesar da garantia de um certo grau de anonimato, que produza efeitos benéficos aos utilizadores, haveria formas de rastreamento que garantiriam mecanismos para que o Estado, na integração do ordenamento e aplicação, pudesse empreender controle.

Diante de uma *Blockchain* pública, acessível por qualquer um, haveria que se visualizar a eliminação das estruturas centralizadoras como um rearranjo dos poderes na rede, eliminando a demanda por entidades centrais de gerenciamento de dados e, por isso, reduzindo sua esfera de atuação e controle (AL-SAQAF; SEIDLER, 2017, p. 343). Dessa forma, por meio de uma *Blockchain*, é possível que os indivíduos, livremente, exponham e recebam dados e informações, estruturando uma rede que, nas palavras de Al-Saqaf e Seidler, seriam a primeira forma de rede efetivamente horizontal, sem elos hierarquicamente superiores.

Nesse mesmo aspecto, a liberdade de informação, que foi indicada, antes, como uma faceta da liberdade de navegação, mostra-se especialmente marcada pela expansão das vias digitais descentralizadas, considerando a maior capacidade de projeção das informações além das instâncias de controle e, dessa forma, efetivamente garantindo o direito dos utilizadores da

rede. Meredith Veit (2019, p. 40) aponta as *Blockchains* como elos essenciais para garantir a liberdade de informação, considerando seu especial papel de fugir das instâncias intermediárias e, assim, evitar censura e conflitos de interesses, que poderiam afetar a exposição da verdade jornalística pelas vias usuais, como sítios digitais de grandes tabloides e mídias sociais. A autora cita o caso da *Civil Media Company*, um jornal que se pauta na divulgação por meio de *Blockchain*, centrando-se na independência.

A liberdade de pensamento e expressão, que possui fortes laços com o ambiente virtual, também possui projeção por meio das *Blockchains* e tecnologias correlatas, de forma que a realidade descentralizada e sem intermediários permitiria a criação de ambientes virtuais de vedação às práticas de censura e controle, impondo barreiras a tais práticas. Não somente isso, a proteção sobre a privacidade resvalaria na questão, considerando a necessidade de espaços reservados para que o indivíduo, autonomamente, opte por expor seus pensamentos e livremente se manifestar.

As *Blockchains* públicas seriam capazes de produzir efeitos, na garantia da liberdade de expressão, por meio de um “ambiente efetivo em termo de custos” (ALSARSOUR, 2020, p. 33), no qual haja a garantia de não alteração dos registros e a ausência de centralização direta, fornecidas a um custo relativamente baixo, quando comparado com outras estruturas. Portanto, essas tecnologias, pautadas tanto no *proof-of-work* quanto no *proof-of-stake* estruturariam redes com dados não removíveis e não modificáveis, de forma que a proteção à liberdade de expressão pode ser mais facilmente garantida, contornando estruturas de controle e censura que fujam do consenso democrático dos protocolos.

Vale trazer como exemplo a adoção massiva da *Blockchain Ethereum* no ano de 2020, para que denunciante do governo chinês e pesquisadores perseguidos politicamente expusessem suas opiniões além dos limites da censura, expondo informações controladas acerca da pandemia de Coronavírus e das medidas adotadas pelo Governo Chinês (ALLEN et al, 2020, p. 128).

Nesse sentido, seria possível atrelar, diretamente, o uso das referidas tecnologias à efetivação, sob uma dinâmica arquetônica, da liberdade de navegação dos utilizadores da *Internet*, de forma que a liberdade poderia ser garantida em uma dinâmica imediata ou mediata, sendo que a preservação da privacidade se mostra como um elo central na garantia da auto determinação dos indivíduos na realidade digital. Ao passo que eventuais lesões à liberdade de navegação dos indivíduos dependeriam da possibilidade de trazer, à esfera jurisdicional, tal situação, e promover uma dinâmica reparatória, as tecnologias abordadas permitiriam estruturar espaços de isenção material, arquetonicamente construídos, impedindo intervenções.

Em que pese a relevância da liberdade ao indivíduo e à coletividade, há que se ponderar a liberdade disponibilizada aos utilizadores de *Blockchains* e tecnologias correlatas, medidas que devem estar atreladas aos seus protocolos, enquanto necessidade para garantir um modelo juridicamente adequado ao ordenamento e à multiplicidade de direitos fundamentalmente tutelados.

A utilização de tecnologias descentralizadas e desintermediadas acabaria por remover os riscos atrelados à liberdade de expressão e também à liberdade de navegação, uma vez que se torna mais difícil a prática de censura e limitação de acesso (ARTICLE 19, 2019, p. 20). No entanto, a ressalva feita pela organização *Article 19* merece ser apontada, indicando a organização, que os eventuais impactos positivos das *Blockchains* sobre as liberdades humanas não podem ser interpretados como uma perda de responsabilidade dos Estados, não devendo eles abdicarem da sua responsabilidade de zelar pelos direitos em nome de suposto efeito útil da tecnologia. Indo além, a adoção desses mecanismos, pelo Estado, poderia se mostrar útil e capaz de ampliar seus efeitos benéficos, permitindo a projeção do seu uso.

Essas tecnologias possuiriam como diferencial, com relação a outras capazes de engendrar formas de efetivação da liberdade, a dinâmica democrática, que não estaria presente normalmente em plataformas privadas, que possuiriam baixo apego democrático e ligado à transparência das dinâmicas de governança (KLONICK, 2018, p. 1665). Ao menos sob uma dinâmica ideológica, as *Blockchains* possuiriam características democráticas, pautadas na transparência aos utilizadores dos protocolos e medidas ali adotadas, o que garantia que a liberdade usufruída alcançasse uma maior amplitude do que aquela tida por utilizadores em plataformas digitais, como o caso de redes sociais.

Sob a óptica econômica, a liberdade estaria diretamente atrelada à seara dos criptoativos, em especial aqueles que possuiriam potencial de empoderar indivíduos economicamente e, dessa forma, garantir sua autonomia financeira frente aos bancos e modelos economicamente centralizados e onerosos (SCOTT, 2016, p. 5). Os criptoativos, portanto, possuiriam um papel importante nas relações econômicas entre os indivíduos, estabelecendo vias facilitadas e seguras para transações, o que refletiria, diretamente, na livre disposição da propriedade pelos indivíduos, seja no mundo dos átomos ou no mundo dos *bits*, o que marca a liberdade econômica.

Cita-se, como exemplo, o caso do *M-Pesa* e do *Bitcoin*, que são usados, massivamente, em países economicamente fragilizados, como o Quênia e Venezuela, trazendo meios seguros, menos custosos e ágeis para realizar transações e transferir valores (CAWREY, 2013) (MARINHO, 2020). Seriam, portanto, tecnologias capazes de criar inclusão financeira a um

nível nunca antes visto (SCOTT, 2016, p. 11), que seria capaz de, ao permitir a utilização dessas tecnologias pelos indivíduos, projetar efeitos benéficos sobre outras searas da liberdade e, também, sobre a privacidade.

Aproximando-se das tecnologias decorrentes de uma segunda geração de *Blockchains* e seu uso, haveria que se ressaltar, também, o papel essencial dos contratos inteligentes na garantia da liberdade econômica dos utilizadores, mostrando-se como mecanismos hábeis para a redução de custos operacionais e capazes de, por meio de uma realidade descentralizada, serem estruturados conforme o interesse dos contratantes, garantindo uma adequação às necessidades das partes e uma exequibilidade ímpar das obrigações (DE FILIPPI; WRIGHT, 2018, p. 80).

Além disso, a questão de registro de dados em *Blockchains* também teria relevância direta à liberdade econômica, considerando o registro de informações transacionais, dados que são massivamente explorados por empresas para finalidades diversas, como medidas de controle e proteção do crédito e até mesmo publicidade (DENG et al, 2015, p. 256), e também por Estados para finalidades não legítimas. Dessa forma, a existência de um pseudo-anonimato sobre os dados transacionais, envolvendo criptomoedas ou mesmo novos serviços financeiros descentralizados, como o caso do Libra⁹⁷ (RODRIGUES; MARCHETTO; SILVA, 2021), permitiria uma maior liberdade econômica aos indivíduos, de forma que seus dados estariam afastados de elos centralizados, pautando-se, unicamente, em registros criptografados, realizados de forma descentralizada.

Considerando a prevalência de modelos pautados no pseudo-anonimato, haveria privacidade sobre os dados pessoais dos indivíduos que realizaram as transações, sendo acessíveis, publicamente, suas chaves públicas e também os valores transacionados, tendo como modelo uma *Blockchain* de primeira ou segunda geração. Sob esse aspecto, utilizando-se de práticas de conhecimento do consumidor (*Know your customer* - KYC), seria possível realizar cruzamento de dados para que, sob situações legítimas, pudesse o Estado ter acesso às informações dentro do limite da sua utilidade.

Dessa forma, quando se mostrasse necessário, poderia o Estado, dentro das bases do devido processo legal, adotar medidas para conhecer os valores transacionados e as partes, para que possa, por exemplo, empreender tributação ou mesmo investigações criminais. Portanto, o pseudo-anonimato traria a privacidade necessária à garantia da liberdade econômica dos

⁹⁷ Com as devidas ressalvas em razão do seu maior nível de centralização, que pode indicar uma possível recentralização, adotando um modelo de *Blockchain* permissionária com entes definidos, empresas de grande porte.

utilizadores, prevendo, em si, mecanismos semipermissivos ao acesso de informações, o que reflete em maiores dificuldades para o empreendimento de controle.

Diante dessa dinâmica, há que se conceber que a liberdade econômica e também política, propiciadas pela utilização de criptoativos e *Blockchains*, possuiria, em si, um efeito coletivo, de forma que a promoção da liberdade, em nível individual, refletiria, diretamente, no desenvolvimento social, como bem expõe Amartya Sen (2000, p. 19). A vida social mostra-se intimamente relacionada à capacidade dos indivíduos acessarem o mercado de uma forma livre e autônoma, uma vez que o bem estar coletivo, e a própria reafirmação das liberdades humanas estariam intimamente relacionadas a esse paradigma econômico. Portanto, apesar de apontar rumo a uma individualidade, há que se conceber o potencial de efeito das *Blockchains* e tecnologias correlatas sobre a coletividade, instrumentalizando efeitos sociais rumo ao desenvolvimento humano.

Torna-se perceptível uma dinâmica dos Estados que, acreditando que todo conteúdo ideológico dos criptoativos teria fundamento e respaldo, passam a temer privações à sua soberania, dinâmica especialmente verificada em Estados com baixo apego democrático e à tutela dos direitos humanos. Basta observar o caso do Estado Chinês que, em 24 de setembro de 2021, optou por banir toda e qualquer operação envolvendo criptoativos (INFOMONEY, 2021), lançando fundamentação com base na sua soberania monetária. Enquanto uma questão já muito bem analisada na academia (RODRIGUES, 2018), criptoativos não possuiriam natureza monetária, aproximando-se mais de um arranjo de pagamento ou mesmo um bem móvel, situação que permite vislumbrar que medidas, como aquelas adotadas pela China, não possuiriam efeito restrito à dinâmica econômica envolvendo as tecnologias em questão, mas produzindo efeitos também sobre a dignidade dos utilizadores, que passam a não dispor de tais meios e seus impactos.

No âmbito da liberdade e da autonomia, apesar dos pontos indicados, Primavera De Filippi e Aaron Wright (2018, p. 207) apontam que é necessária ponderação nas utilizações das tecnologias automatizadas para a garantia da liberdade, porque, apesar da sua eficiência, elas podem vir acompanhadas de efeitos maléficos sobre os direitos humanos, indicando uma dinâmica fáustica sobre a técnica. Apontam os autores que a liberdade e autonomia, assim como os demais direitos tutelados pelas tecnologias analisadas, mostrar-se-iam tecnicamente mais eficientes que o modelo do devido processo legal. No entanto, um abuso na liberdade por tais métodos pode vir acompanhado de um controle ainda maior pelos algoritmos e codificações autônomas.

Segundo apontam os autores, é necessário que haja uma melhor compreensão pela tecnologia dos impactos da *Lex Cryptographica* sobre a sociedade, em especial, considerando a ambivalência da técnica, ideia central do paradigma filosófico que embasa a pesquisa. Conforme expos Lawrence Lessig⁹⁸, a dispersão total das estruturas do Estado, em nome da liberdade, não representa a ascensão de um modelo prometeico, uma vez que o vacúolo de poder passaria a ser ocupado por outras entidades, situação muito bem percebida na questão da *Internet* e o poder programacional. Nesse sentido, a liberdade propiciada pelas *Blockchains* e tecnologias correlatas deve se pautar em um modelo ponderado, capaz de admitir limitações, especialmente em nome do devido processo legal, a ser exercido pelo Estado, por vias legítimas e democraticamente válidas.

Há indicativos diretos que a disrupção das estruturas de poder não é uma prática que tenha conseguido ser implantada pela revolução tecnológica das *Blockchains* e criptoativos (CAMPBELL-VERDUYN, 2018, p. 11). Mais que isso, é necessário conceber a utilização prudente e ponderada dessas tecnologias para a garantia da liberdade dos utilizadores, sem exceder estruturas que já existem e apresentam relevância social, como o caso do Estado e seus mecanismos de tutela de direitos humanos. Não se fala, portanto, na derrocada de um modelo e ascensão de outro, mas, sim, na assimilação tecnológica pelo Estado de tais vias, que são mais eficientes que as usuais e podem, ao serem empregadas para a sociedade por meio de políticas públicas, produzir efeitos melhores.

Primavera De Filippi e Aaron Wright (2018, p. 208):

No fim, portanto, a tecnologia *Blockchain* não encaminha ao fim do devido processo legal como conhecemos. Mesmo em um mundo com uso disperso de *Blockchains*, os governos permanecem retendo as suas quatro forças regulatórias, normas, códigos, forças do mercado e normas sociais, as quais podem ser utilizadas direta ou indiretamente para regular essa nova tecnologia.⁹⁹

Diante do exposto, dedutivamente, concebe-se que as liberdades humanas, em especial a liberdade de navegação, liberdade de pensamento e expressão, assim como a liberdade econômica, possuiriam relação direta com as tecnologias *Blockchain* e derivados, uma vez que as características desses sistemas teriam especial projeção sobre a faceta desses direitos no ambiente virtual e, em casos estritos, projetando-se também sobre o mundo dos átomos.

⁹⁸ Discurso de Lawrence Lessig no evento “*One Planet, One Net*”, ocorrido em 10 de outubro de 1998.

⁹⁹ “*In the end, however, Blockchain technology does not spell the end of the rule of law, as we know it. Even in a world with widespread use of Blockchains, governments still remain their four regulatory levers – laws, code, market forces and social norms – which could be used to either directly or indirectly regulate this new technology*”. (tradução livre).

A descentralização das redes, funcionamento pautado em mecanismos de consenso coletivo e pseudo-anonimato, estariam diretamente atrelados à efetivação da liberdade humana no ambiente virtual, especialmente considerando as violações promovidas por intermédio do chamado poder programacional. Por meio dos pontos indicados, haveria a possibilidade de se instituir mecanismos de efetivação algorítmica da liberdade humana, impedindo medidas violatórias em sua essência e, assim, não se pautando em práticas pós-violatórias. Faz-se, ainda, as devidas ressalvas aos pontos indicados, de forma que as tecnologias indicadas devem ser integradas ao ordenamento jurídico e não atuarem como técnicas disruptivas, capazes de desestruturar o Estado e o seu poder legitimamente constituído.

CONCLUSÃO

A pesquisa foi desenvolvida com base em uma metodologia hipotético-dedutiva, buscando-se testar hipóteses previamente levantadas por meio de uma análise dedutiva de materiais multidisciplinares adequados à temática proposta. São apresentadas duas hipóteses primárias a serem testadas, cada uma delas dentro de uma das seções do trabalho, com cada uma delas tendo seu resultado indicado a um dos objetivos propostos.

O objetivo central do trabalho foi demonstrar uma correlação entre a utilização de criptoativos, *Blockchains* e tecnologias correlatas, enquanto estruturas nativas do mundo digital, como mecanismos de tutelas de direito digitalmente existentes ou manifestados por essa via. Enquanto vias para o alcance do objetivo central, foram estruturados dois objetivos específicos, quais sejam, compreender as dinâmicas de poder na rede, compreender a manifestação de direitos na *Internet* e as fragilidades das estruturas institucionalizadas e das estruturas não ortodoxas de regulação do ambiente virtual.

A hipótese central do trabalho se comunica com o objetivo primário, pautando-se na utilização de criptoativos, *Blockchains* e tecnologias correlatas enquanto mecanismos aptos à tutela, por intermédio de estruturas privadas descentralizadas, dos direitos de liberdade e privacidade dos utilizadores da rede, mostrando-se como um mecanismo nativo à rede e que não dependeria de recursos ao mundo dos átomos para produzir efeitos. Para se chegar à testagem dedutiva da hipótese em questão, fixou-se um caminho metodológico que percorre hipóteses iniciais, com cada uma delas estruturadas em seções separadas da dissertação.

A primeira seção da dissertação se ateu à formação da base filosófica sobre a qual seria estruturado o trabalho dentro da metodologia optada e a introdução dos temas iniciais acerca da relação entre o direito e a técnica informacional. Enquanto base filosófica e sociológica que se constrói o trabalho, há a adoção de um paradigma dos estudos da técnica, tendo como referencial teórico os autores Jacques Ellul (1968), Hermínio Martins (2012), Ortega y Gasset (1963) e Vilém Fluesser (2013; 2019).

A técnica mostra-se como um fenômeno humano de rejeição ao natural e promoção de alterações estruturais em seus diversos aspectos de vivência, estando, em si, embebida de uma dinâmica de simplificação através de práticas mediadas, ou seja, não diretamente empreendida pela ação humana. Adequando ao esquadro de trabalho, fez-se necessário indicar a ascensão da técnica informacional como uma realidade fluida e não-objetificada, apontando como essa realidade foi capaz de remodelar as questões socioeconômicas, culturais e jurídicas das

sociedades humanas, colocando a informação como ponto de referência para o ambiente técnico.

A técnica computacional serviria como ambiente de transição entre uma técnica industrial e uma técnica informacional, permitindo a estruturação de uma realidade comunicacional. Essa realidade, sob um ponto de vista gnóstico, concorreria diretamente com a vivência física, cooptando a vivência dos indivíduos rumo ao ambiente digital, tipicamente mais seguro e ágil, tendo como seu expoente a *Internet*.

Sob esse paradigma, o direito estaria diretamente imerso nas questões técnicas, embebendo-se da realidade de sua estruturação, para empreender regulação sobre a vivência humana. Nesse sentido, fala-se na transição de um direito tipicamente pautado na técnica industrial, materialista, para um ambiente fluido e sensível ao toque, dando origem ao fenômeno intitulado refração jurídica, relacionado à incidência de normas típicas de uma realidade técnica sobre outra.

A primeira hipótese foi definida como a existência de uma realidade digital que se distingue da realidade física, com projeção direta dessa questão sobre a incidência do direito e demais formas regulatórias, hipótese que foi testada na primeira seção do trabalho, especialmente centrada na manifestação digital do direito e na hipotética dicotomia Átomo-Bit. Realizada a testagem dedutiva da hipótese, foi verificada a existência de dois paradigmas teóricos acerca da incidência do direito sobre o ambiente digital, o utópico e o isotópico, com cada um deles indicando pontos dedutivamente testados como plausíveis e, portanto, indicando um rompimento com uma necessária dicotomia entre o átomo e o *bit*, de forma que as forças regulatórias, usualmente incidentes sobre o mundo físico, teriam certa incidência ao ambiente virtual.

Foram constatadas certas fragilidades técnicas na incidência das estruturas jurídicas ordinárias, tipicamente atreladas à técnica industrial, divergente daquela sobre a qual se estrutura toda a vivência cibernética atual. Portanto, testada a hipótese, passou-se a adotar uma diretiva utópica relativizada para o encaminhamento da pesquisa, fazendo sempre as devidas ressalvas à validade e testagem, inclusive no âmbito do trabalho, da aplicabilidade de uma visão isotópica. Nesse sentido, percebe-se que o resultado, obtido por meio da testagem dedutiva, aproximou-se da hipótese indicada e, além disso, aproximou-se do objetivo especificamente traçado para a seção da dissertação. Isso, portanto, sugeriria a validade da hipótese e, diante da sua testagem, por meio de um direcionamento metodológico, centrado no modelo dedutivo, mostrou-se cabível a adoção dos resultados indicados para o prosseguimento do caminho metodológico.

A segunda hipótese da pesquisa centrou-se na existência de direitos ou meras manifestações de direitos no ambiente virtual, além da existência de fragilidade nas respostas das estruturas institucionalizadas frente às violações de direitos humanos e aptidão técnica das estruturas nativas ao ambiente informacional. Por meio da testagem dedutiva, constatou-se que houve, no ambiente digital, uma remodelação das forças incidentes, alterando a estrutura de regulação e as práticas e vivência humana diante dessa nova realidade.

Tendo sido tomada como base a visão utópica para as testagens das hipóteses propostas após a primeira seção da pesquisa, construiu-se o entendimento de que haveria direitos decorrentes do ambiente informacional, e não meras manifestações de direitos que existiriam no mundo dos átomos. A base dessa concepção partiu da existência de robustas divergências técnicas entre o mundo dos átomos e o mundo dos *bits*, motivos pelos quais o ambiente socioeconômico, cultural e jurídico atual acabaria por ressignificar a dignidade humana, de forma que as demandas ali nascentes, sejam elas individuais ou coletivas, possuiriam a conotação de efetivos direitos. Os direitos nasceriam como uma construção coletiva do ambiente da *Internet*, especificamente respondendo a demandas e exigências oriundas da experiência digital, possuindo uma conotação que, por si, já traria uma menor adesão do pensamento isotópico.

Dessa forma, aquelas realidades de vivência, ainda que não física, possuiriam especificidades que se permitiriam a ascensão de direitos especificamente relacionados a elas. Ainda que não se fale, necessariamente, na estruturação de direitos referentes a novos aspectos de dignidade humana antes não tutelados, há que se conceber a reestruturação de padrões de dignidade e também a reestruturação dos mecanismos de tutela e garantia, que, por si, já permitiram compreender uma nova realidade envolvendo os direitos humanos sob seu aspecto informacional.

Haveria que se considerar a ascensão de novos processos de luta para a composição de direitos humanos, construção que seria marcadamente histórica e relacionada às novas tendências técnicas, afetando a dignidade humana. Nesse aspecto, pontua-se a ascensão de um padrão de dignidade humana especial, estritamente relacionado ao ambiente virtual, a liberdade de navegação, capaz de comungar a livre circulação pelos ambientes informacionais e a possibilidade de assimilar e ter acesso às informações que se mostrem úteis ou necessárias ao indivíduo, assim como compartilhar e livremente transmiti-las na rede. As demais formas de liberdade e a privacidade teriam passado por alterações robustas nos seus padrões, dada a alteração do contexto técnico, situação que permitiu pensar nesses direitos como oriundos de contexto de afirmação do próprio ambiente virtual.

Esse novo modelo de forças, pautado na regência do poder programacional, assume padrões que fogem da dinâmica jurídica usual e, além disso, subtrai-se dos moldes democráticos que devem reger as atividades regulatórias. Sob esse novo paradigma, haveria adequação técnica para que as forças regulatórias, oriundas do poder programacional, projetassem exequibilidade nativa à própria rede, portanto, mecanismos regulatórios embebidos já em mecanismos de exercício do poder de fato, lançando mão de padrões arquitetônicos de regulação.

Nesse sentido, foi apontado que as dinâmicas violatórias de direitos humanos, na realidade virtual, estariam pautadas na atuação de agentes dotados de poder programacional, haja vista a estrita relação entre a lesão de direitos e o exercício de formas de poder. O poder programacional seria visualizado, majoritariamente, no Estado e corporações com braços de atuação digital, portanto, estando essa manifestação de poder diretamente relacionada ou à capacidade de cooptação do poder técnico-estrutural do Estado e/ou do próprio poder econômico.

Sob esse aspecto, haveria que se considerar as reiteradas práticas alegais, portanto, pautadas em ambientes não regulados e sob a ausência da efetividade normativa, que estariam sendo empreendidas pelo Estado e pelas corporações digitais, diretamente afetando os direitos humanos dos utilizadores da *Internet*, por meio de reiteradas medidas de controle e vigilância. Nesse aspecto, considerando a atuação ilegal do Estado e a ascensão de figuras privadas, dotadas de poder de fato, há que se conceber a existência de uma crise de legitimidade afetando o poder na *Internet*, de forma que ele estaria sendo empreendido, massivamente, além dos limites do que é legítimo e esperado dentro do Estado Democrático de Direito.

O ambiente informacional seria marcado pelo empreendimento de práticas violatórias decorrentes do exercício do poder programacional e, ao mesmo tempo, pela ausência de adaptabilidade técnica do direito estatal às questões digitais, especialmente considerando a tutela e efetivação de direitos humanos. As normas jurídicas não seriam tecnicamente adequadas à realidade informacional, sem apego material à tutela de direitos e com escassos mecanismos de exequibilidade e garantia dos direitos humanos. Na prática, tratar-se-ia de o direito estatal dispor de mecanismos analógicos e não informatizados, em sua essência, para regular códigos e protocolos, já inseridos na fluidez do ambiente digital, isso sem contar com a já difícil tutela dos direitos humanos pelo Estado, que se pauta em uma dinâmica pós-violatória.

Não se fala na incapacidade de o Estado incidir regulação sobre a questão dos direitos humanos, envolvendo o ambiente digital, haja vista a necessidade de se reconhecer a existência

de espaços de aplicação isotópica do direito estatal, no qual haveria pontos de ancoragem do ambiente virtual que permitiriam ao Estado impor medidas de controle e, assim, garantir sua exequibilidade. Além disso, a própria adoção do poder programacional pelo Estado permitiria a incidência regulatória sobre a dignidade humana no ambiente virtual, no entanto, tratando-se de um paradigma escassamente empreendido pelo Estado.

Conforme já havia sido apontado, na esfera digital, passa a assumir notoriedade a força regulatória dos códigos, marcando-se pela relevância e adequação técnica, assim como sua autoexecutoriedade e dificultoso repúdio pelas vias ordinárias. A regulação passaria a ter maior eficiência ao não depender de outros fatores para garantir sua exequibilidade, o que refletiria no enfraquecimento ou menor atuação da via estatal. Sob esse aspecto, concluiu-se que não haveria na *Internet* uma crise de legalidade, mas, sim, uma crise na legalidade estatal. Preliminarmente, havia-se estabelecido que não haveria, no ambiente, uma crise de legalidade, tendente ao anarquismo absoluto, hipótese que fora testada e os resultados se coadunam com o proposto.

Nesse sentido, haveria, no ambiente digital, considerando a ascensão do poder programacional e suas dinâmicas ilegítimas, marcantes lesões à privacidade e à liberdade humana, lesões que se dariam tanto por práticas estatais de vigilância e controle quanto por medidas de agentes privados. Sob esse aspecto, o direito estatal e até mesmo o direito internacional possuiriam restritos mecanismos de tutela e efetivação, ao passo que as forças regulatórias, nativas ao ambiente informacional, possuiriam aderência à realidade técnica e teriam especial caráter autoexecutivo.

A segunda hipótese foi testada e coadunou com os objetivos traçados, dando indicativos de que haveria direitos decorrentes da realidade digital, haveria certas fragilidades na atuação de instâncias jurídicas usuais e, por sua vez, as estruturas nativas se mostrariam com vantagens comparativas exacerbadas.

Testadas ambas as hipóteses primárias e obtidos resultados condizentes com os objetivos definidos, passou-se à discussão da hipótese central da dissertação. Percebida a existência de uma realidade digital atrelada à técnica, um ambiente marcado por reiteradas práticas violatórias de direitos e a fragilidade das respostas jurídicas usuais, passou-se a discutir a capacidade do emprego das vias tecnológicas para garantir e efetivar direitos no ambiente digital, especialmente as tecnologias atreladas aos criptoativos, *Blockchains* e tecnologias correlatas.

A adoção desses mecanismos seria pautada na utilização de vias automáticas de regulação, mecanismos arquitetônicos, que seriam capazes de produzir efeitos consideráveis

sobre a tutela dos direitos humanos no ambiente digital. Uma hipótese que se levanta nesta seção é que as tecnologias relacionadas não seriam estritamente centradas em uma regência programacional, desvinculada de bases estáveis de legitimidade, hipótese que é testada e traz indicativos diretos de que a tecnologia das *Blockchains* e outras correlatas seriam embebidas em bases ideológicas e políticas, motivos pelos quais grande parte das suas manifestações estariam atreladas a um modelo de regência democrática, de forma que todo poder programacional, sobre o qual se estruturam tais sistemas, estaria pautado em modelos de consenso coletivo, além de trazer formas de transparência capazes de garantir o acesso (ao menos no caso das *Blockchains* públicas) parcial às informações.

Foi demonstrado que as tecnologias digitais, que antecedem as *Blockchains* e correlatas, apesar de possuírem relevância e utilidade marcante na tutela dos direitos humanos, no ambiente digital, quando concebidas, singularmente, possuiriam pontos de fragilidade capazes de minar seus efeitos. Portanto, apesar da sua relevância e potencial de produção de efeitos sobre a tutela dos direitos humanos, tecnologias como a criptografia, as redes *peer-to-peer* e os *softwares* livres, ou de códigos abertos, possuiriam uma atuação que, embora tecnicamente adequada, sofreria com restrições na produção de efeitos, seja em razão da ineficiência do emprego isolado de uma das técnicas ou mesmo pelo seu baixo apego às questões da legitimidade e seu conteúdo democrático.

Por outro lado, as *Blockchains* e tecnologias correlatas mostrar-se-iam como construções capazes de reunir os benefícios de diversas tecnologias, o que refletiria em um aumento da sua eficiência, ao depositar seu funcionamento sobre um conjunto de técnicas relevantes em si, além de possuir robustas bases voltadas à construção democrática desse meio. Nesse sentido, seriam amálgamas técnicas que se destinam a fazer frente às falhas marcantes na garantia de direitos no ambiente digital, marcando-se por possuir uma natureza coletiva, democrática, consensual e autoexecutável.

As referidas tecnologias, portanto, trariam, em si, mecanismos dotados de poder programacional, capazes de empreender atividade regulatória sobre o ambiente virtual de forma autônoma e não repudiável, ao mesmo tempo que garantiria uma estrutura de funcionamento potencialmente legítima, baseada no consenso da coletividade de nós, ao menos concebendo a grande maioria das *Blockchains*, criptoativos e tecnologias correlatas.

As bases de funcionamento dessas técnicas centram-se na desintermediação das estruturas de registro de dados, na ruptura com dinâmicas centralizadas, na estruturação de redes pautadas em pseudo-anonimato, a imutabilidade dos registros e o poder da coletividade, expresso através de algum algoritmo de regência. Sob essas características, haveria que se

conceber o potencial de tais tecnologias produzirem efeitos concretos sobre a tutela de direitos humanos.

Nesse ponto, a hipótese central do trabalho foi testada e os resultados apontam para a possibilidade dos criptoativos, *Blockchains* e tecnologias correlatas empreenderem a efetivação dos direitos de privacidade e liberdade no ambiente digital, com indicativos dedutivamente testados de que o funcionamento de tais mecanismos projetaria efeitos preventivos com relação a eventuais lesões, promovidas por intermédio do poder programacional, estruturando formas arquitetônicas de tutela e efetivação de direitos humanos no ambiente digital.

Trazendo os resultados para o paradigma filosófico da técnica, que, de fato, embasa o substrato lógico da pesquisa, há que se levantar a concepção das técnicas apontadas como ambivalente, coadunando com o pensamento de Jacques Ellul. Portanto, apesar das *Blockchains*, criptoativos e tecnologias correlatas trazerem benefícios à tutela de direitos humanos sob um paradigma privado de efetivação, esses benefícios viriam acompanhados também de malefícios, que, ainda que não ofusquem o lado positivo, precisam ser considerados. O automatismo que denota a técnica significaria o emprego dos mecanismos mais eficientes para os fins que se destinam (BARRIENTOS-PARRA, 2011, p. 57), quando aplicado à questão abordada, indicaria uma maior eficiência pendendo rumo à capacidade regulatória das redes descentralizadas, sugerindo uma possível imposição sobre a norma estatal, tipicamente menos eficiente.

Enquanto seriam projetados efeitos de tutela sobre a privacidade e liberdade no ambiente digital, haveria formas de afetação decorrentes dessas medidas, especialmente considerando sua natureza arquitetônica e pouco flexível, indicando pontos de recrudescimento das medidas de controle e vigilância, ou mesmo promovendo a garantia de direitos de forma a causar lesões sobre outros direitos humanos. Portanto, é necessário compreender que a técnica não teria uma dinâmica prometeica, capaz de projetar apenas efeitos úteis, mas, também, produzindo situações não antecipadas e que podem aprofundar lesões aos direitos humanos.

As *Blockchains*, criptoativos e tecnologias correlatas possuiriam capacidade de produzir efeitos benéficos aos direitos de privacidade e liberdade, promovendo tutela de forma mais eficiente que mecanismos não adaptados tecnicamente. No entanto, dada sua natureza algorítmica, relacionada à exequibilidade automática das medidas, não repúdio das informações registradas e inalterabilidade, poderia haver uma proteção exacerbada sobre esses direitos, a ponto de inviabilizar uma tutela ponderada de todos os direitos humanos.

A ausência de ponderação e possibilidade de relativização de direitos, situação que ocorre, na prática, durante a atividade jurisdicional, mostra-se como ferramenta necessária para

a construção coletiva de direitos humanos, impondo limitações à individualidade em nome de benefícios comuns ou benefícios individuais com maior necessidade de tutela na realidade concreta.

Apesar do apontamento, indica-se que as referidas tecnologias, em sua grande maioria, possuiriam pontos de “fragilidade estrutural”, capazes de permitir a adoção de práticas de relativização dos direitos, o que estaria diretamente relacionada à capacidade dessas redes e sistemas se integrarem ao ordenamento jurídico de forma harmônica. O pseudo-anonimato mostra-se como a principal característica das *Blockchains* capaz de fornecer espaço para a ponderação dos direitos, de forma que a existência de certos dados públicos permitiria a adoção de práticas de rastreamento, cruzamento de dados e identificação das partes, pontos essenciais para que sejam empreendidas relativizações legítimas sobre a privacidade e liberdade.

Sob esse paradigma, apesar de serem estruturadas como sistemas tipicamente descentralizados e de origem privada, seria cabível a adoção desses mecanismos pelos Estados para promoverem uma tutela mais efetiva sobre os direitos de privacidade e liberdade e garantirem uma melhor integração com os demais direitos humanos. Não somente isso, haveria que se conceber a necessidade de expansão desses mecanismos de tutela de direitos por via de políticas públicas, como forma de facilitar o acesso dos indivíduos a tais mecanismos, especialmente considerando a inerente natureza econômica que denota essas tecnologias.

Portanto, um ponto de fragilidade das *Blockchains* e tecnologias correlatas estaria relacionado aos procedimentos para sua instrumentalização, dependendo, diretamente, da existência de *hardwares* de acesso à rede, formas de acesso estável e veloz à *Internet*, assim como em grande parte dos casos, a necessidade de pagamento de taxas, usualmente chamadas *fees*, para a realização de registros nas redes descentralizadas. Dessa forma, haveria um anteparo de acesso a grande parte dos indivíduos a tais tecnologias, em especial, aquelas populações de países em desenvolvimento e, portanto, sujeitas a maiores exposições da sua dignidade a violações.

O Estado se posicionaria como elo garantidor do acesso dos indivíduos a essas tecnologias, provendo meios materiais para que fosse possível fazer uso desses mecanismos ou mesmo provendo sistemas descentralizados para a utilização de seus cidadãos. Não somente isso, o Judiciário atuaria na ponderação dos direitos envolvidos, empreendendo as devidas intervenções, por intermédio de mecanismos tecnicamente hábeis, para que a integridade do ordenamento e a proteção coletiva dos direitos humanos seja possível.

Portanto, apesar de possuir uma natureza inicialmente disruptiva, é necessário perceber que o emprego dessas tecnologias dependeria de uma efetiva integração com o ordenamento,

permitindo mais vias de proteção e efetivação de direitos humanos, mecanismos legítimos e adequados a uma realidade democrática. Mesmo que oriunda de uma dinâmica estatal, sua base descentralizada e desintermediada traria legitimidade para o poder programacional, ali exercido por meio do consenso democraticamente construído, pontos que se mostram essenciais para superar a crise de legitimidade que afeta o ambiente informacional e o exercício do poder nessa via.

Apesar das necessárias relativizações às tecnologias para a integração ao ordenamento, é necessário manter as características essenciais das referidas tecnologias, enquanto pontos de garantia capazes de impor barreira ao exercício ilegítimo do poder programacional, considerando a utilização massiva desses meios, tanto pelos Estados quanto pelas corporações. A ponderação se faz necessária, como forma de bloquear atuações ilegítimas por meio de padrões arquitetônicos de regulação e, ao mesmo tempo, permitir que os demais direitos humanos sejam tutelados.

Haveria que se projetar uma estrutura de autorregulação regulada, com uma dinâmica pautada na regência digital por meio de dinâmicas tecnicamente adequadas, que é o caso das *blockchains* e tecnologias correlatas, sujeitas a diretivas de controle e adequação, como forma de garantir a fidelização dessas estruturas técnicas às bases do ordenamento jurídico.

Apontando para outros direcionamentos, há que se visualizar a projeção de efeitos das *Blockchains* e tecnologias correlatas sobre outros direitos e questões, como o uso das tecnologias para garantir processos democráticos de eleição, tema tão bem aprofundado na academia. Não bastasse isso, lembremos da utilização, já feita pelo Estado, das tecnologias para validar documentos públicos, aumentando a eficiência dos notários e permitindo maior segurança.

Dessa forma, os objetivos apontados comungaram, em grande parte, com os resultados obtidos, sugerindo, desde já, a possibilidade de utilização das *Blockchains*, criptoativos e mecanismos correlatos para empreender tutela e efetivação dos direitos de privacidade e liberdade no ambiente virtual. Tendo sido a pesquisa metodologicamente guiada e pautada em estruturas hipotéticas previamente definidas e testadas dedutivamente, concebe-se a reprodutibilidade da pesquisa.

REFERÊNCIAS

- ABRAMOWICZ, Michael. Cryptocurrency-based Law. **Arizona Law Review**, Tucson (EUA), v.58, n.2, 2016, p.359-420. Disponível em: <https://arizonalawreview.org/pdf/58-2/58arizlrev359.pdf>. Acesso em: 13 out.2021.
- ACHARYA, Bhairav et al. **Deciphering the European encryption debate: Germany**. Washington (EUA): Open Technology Institute, 2018. Disponível em: https://d1y8sb8igg2f8e.cloudfront.net/documents/Transatlantic_Encryption_Germany.pdf. Acesso em: 13 out. 2021.
- AGAMBEN, Giorgio. **Estado de Exceção: Homo Sacer, II, I**. São Paulo: Boitempo, 2004.
- AGLIETTA, Michel. Whence and wither Money? In: OCDE (ed.) **The future of money**. Paris: OCDE, 2002. p.123-145.
- ALLEN, Darcy W. E. et al. **The new technologies of freedom**. Great Barrington (EUA): American Institute for Economic Research, 2020.
- AL-SAQAF, Walid; SEIDLER, Nicolas. Blockchain technology for social impact: opportunities and challenges ahead. **Journal of Cyber Policy**. Londres (GB), v. 2, n.3, 2017. p. 338-354. Disponível em: <https://www.tandfonline.com/doi/abs/10.1080/23738871.2017.1400084>. Acesso em: 03 abr.2021.
- ALSARSOUR, Israa et al. Free Blockchain: enabling freedom of expression through public Blockchains. In: IEE International Conference on Dependability on Sensor, Cloud and Big Data Systems and Applications, 6, 2020, Fiji (FJ). **Proceedings [...]**. Fiji(FJ): IEEE, 2020. p.33-40. Disponível em: <https://ieeexplore.ieee.org/xpl/conhome/9356390/proceeding>. Acesso em: 15 jan. 2021.
- AMMOUS, Saifedean. Economics Beyond Financial Intermediation: Digital Currencies' Potential for Growth, Poverty Alleviation and International Development. **The Journal of Private Enterprise**, Lubbock (EUA), v.30, n.3, 2015. p.19-50. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2832738. Acesso em: 15 abr. 2020.
- ANDREAZZA, Cristiana de Moraes; BARRIENTOS-PARRA, Jorge David. Unicidade da Técnica na visão de Jacques Ellul. In: Seminário Brasileiro sobre o pensamento de Jacques Ellul: novos atores globais, técnica e direito-um diálogo com Jacques Ellul, 1, 2009, Araraquara. **Anais [...]**. Araraquara: FCL-UNESP, 2009. p.239-244. Disponível em: <https://jacquesellulbrasil.files.wordpress.com/2011/07/cadernos-ellul-completo.pdf>. Acesso em: 20 maio 2020.
- ANEESH, A. Technology coded authority: the last post industrial decline in buireaucratic hierarchies. In: International Summer Academy on Technology Studies, 1, 2002, Graz (AT). **Proceedings [...]**. Graz: IFF/IFZ, 2002. Disponível em: <http://web.stanford.edu/class/sts175/NewFiles/Algocratic%20Governance.pdf>. Acesso em: 20 jun. 2020.

ANEESH, A. Global labor: algocratic modes of organization. **Sociological Teory**, Madison (EUA), v. 27, n. 4, dez. 2009. p. 347-371. Disponível em: <https://journals.sagepub.com/doi/10.1111/j.1467-9558.2009.01352.x>. Acesso em: 20 maio 2020.

ANÍSTIA INTERNACIONAL. **Scale of secretive cyber surveillance ‘an international human rights crisis’ in which NSO Group is complicit**. 23 jul. 2021. Disponível em: <https://www.amnesty.org/en/latest/news/2021/07/pegasus-project-spyware-digital-surveillance-nso/>. Acesso em: 08 ago. 2021.

ANTUNES, Ana Maria Pereira. **Sociedade da Informação**. Coimbra: Faculdade de Economia da Universidade de Coimbra, 2008. Disponível em: <http://www4.fe.uc.pt/fontes/trabalhos/2008007.pdf>. Acessado em 25 nov. 2021

ARENDDT, Hannah. **Entre o passado e o futuro**. São Paulo: Perspectiva: 2005.

ARENDDT, Hannah. **Sobre a Violência**. Rio de Janeiro: Relume Damará, 2001.

ARMER, Paul. **Computer Technology and Surveillance**. Santa Clara (EUA): Center for Advanced Studies in the Behavioral sciences. 1975. Disponível em: <https://stacks.stanford.edu/file/druid:zf198qx6952/zf198qx6952.pdf>. Acesso em: 25 maio 2019.

ARTICLE 19. **Blockchain and freedom of expression**. Londres (GB): Article 19, 2019. Disponível em: <https://www.article19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf>. Acesso em: 10 jun. 2020.

ASSANGE, Julian. **Cypherpunks: liberdade e o futuro da Internet**. São Paulo: Boitempo, 2013.

ATHEY, Susan. 5 ways digital currencies will change the world. **World Economic Forum**, 22 jan. 2015. Disponível em: <https://www.weforum.org/agenda/2015/01/5-ways-digital-currencies-will-change-the-world/>. Acesso em: 15 abr. 2020.

BALFANZ, Dirk et al. In search of usable security: five lessons from the field. **IEE Security and Privacy**, Nova York (EUA), v. 2, n.5, set. 2004. p.19-24. Disponível em: <https://dl.acm.org/doi/abs/10.1109/MSP.2004.71>. Acesso em: 20 maio 2021.

BALKIN, Jack M. Digital Speech and Democratic Culture: A Theory of a Freedom of Expression for the Information Society. **New York University Law Review**, Nova York (EUA), v.79, n.1, 2004. p.1-55. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=470842. Acesso em: 20 maio 2020.

BARLOW, John Perry. **A Declaration of Independence of Cyberspace**. 8 fev. 1996. Disponível em: <https://www.eff.org/cyberspace-independence>. Acesso em: 09 nov. 2019.

BARRIENTOS-PARRA, Jorge David. A violação dos direitos fundamentais na sociedade técnica. **Revista de Informação Legislativa**, Brasília, a.48, n.189, jan. mar. 2011. p.55-67. Disponível em:

<https://www2.senado.leg.br/bdsf/bitstream/handle/id/242860/000910792.pdf?sequence=1&isAllowed=y>. Acesso em: 15 mar. 2021.

BARRIENTOS-PARRA, Jorge David; MELO, Elaine Cristina Vilela Borges. O direito à intimidade na sociedade técnica: rumo a uma política pública em matéria de tratamento de dados pessoais. **Revista de Informação Legislativa**, Brasília, a.45, n.180, out./dez 2008. p. 197-213. Disponível em: <https://www2.senado.leg.br/bdsf/bitstream/handle/id/176571/000860618.pdf?sequence=3&isAllowed=y>. Acesso em: 15 mar. 2021.

BAUMAN, Zygmunt. **Tempos líquidos**. Rio de Janeiro: Jorge Zahar, 2007

BELL, Daniel. **O Advento da sociedade pós-industrial**. São Paulo: Cultrix, 1974.

BENJAMIN, Walter. A caixa de costura, Infância em Berlim em 1900. In: BENJAMIN, Walter. **Rua de mão única** (Obras escolhidas, II). Trad.: Rubens Rodrigues Torres Filho e José Carlos Martins Barbosa. São Paulo: Brasiliense, 1987.

BENKLER, Yochai. Practical Anarchism: peer mutualism, market power and the fallible State. **Politics and Society**, Thousand Oaks (EUA), v. 41, n.2, 2013. p.213-251. Disponível em: <https://www.ssc.wisc.edu/~wright/929-utopias-2013/Real%20Utopia%20Readings/Politics%20&%20Society-2013-Benkler-213-51.pdf> . Acesso em: 14 jul. 2020.

BENKLER, Yochai; MORELL, Mayo Fuster; HASSAN, Samer. Commons-based peer production. **Real Colégio Complutense**, Cambridge (EUA), 2020. Disponível em: [https://rcc.harvard.edu/commons-based-peer-production#:~:text=Commons%2Dbased%20peer%20production%20\(CBPP\)%20is%20an%20emerging%20innovative,accessible%20and%20reusable%20by%20anyone](https://rcc.harvard.edu/commons-based-peer-production#:~:text=Commons%2Dbased%20peer%20production%20(CBPP)%20is%20an%20emerging%20innovative,accessible%20and%20reusable%20by%20anyone). Acesso em: 20 jul. 2020.

BENNARDO, Christian. The Fourth Amendment, CSLI tracking and the mosaic theory. **Fordham Law Review**, Nova York (EUA), v.85, n.5, 2017. p.2385-2416. Disponível em: <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5368&context=flr>. Acesso em: 20 abr. 2020.

BERLE, Ian. **Face recognition technology: Compulsory visibility and its impact on privacy and the confidentiality of personal identifiable images**. Cham (SWZ): Springer, 2020.

BERLIN, Isaiah. **Two concepts of liberty in Isaiah Berlin 1969: four essays on liberty**. Oxford (RU): Oxford University Press, 1958.

BLANCHETTE, Jean-François. A Material History of bits. **Journal of the American Society for Information Science and Technology**, Nova Iorque, v.62, n.6, jun. 2011. p.1042-1057. Disponível em: <https://onlinelibrary.wiley.com/doi/abs/10.1002/asi.21542>. Acesso em: 16 mar. 2019.

BOLDRINI, Nicoletta. Algocracy and surveillance capitalism: we live in a world governed by algorithms. **Medium**, [s. l.], 30 maio 2017. Disponível em:

<https://medium.com/@NicBoldrini/algorithm-and-surveillance-capitalism-we-live-in-a-world-governed-by-algorithms-abd1f158186a> . Acesso em: 03 nov. 2019.

BOMBARDA, Carla Barbieri; FRANCISCO, Mayra Bruna; BARRIENTOS-PARRA, Jorge David. A Autonomia da Técnica na visão de Ellul. In: Seminário Brasileiro sobre o pensamento de Jacques Ellul: novos atores globais, técnica e direito-um diálogo com Jacques Ellul, 1, 2009, Araraquara. **Anais** [...]. Araraquara: FCL-UNESP, 2009, p.217-223.

BONAVIDES, Paulo. **Ciência Política**. São Paulo: Malheiros, 2000.

BRASIL **Medida Provisória nº 954 de 17 de abril de 2020**. Dispõe sobre o compartilhamento de dados por empresas de telecomunicações prestadoras de Serviço Telefônico Fixo Comutado e de Serviço Móvel Pessoal com a Fundação Instituto Brasileiro de Geografia e Estatística, para fins de suporte à produção estatística oficial durante a situação de emergência de saúde pública de importância internacional decorrente do coronavírus (covid-19), de que trata a Lei nº 13.979, de 6 de fevereiro de 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 18 mar. 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 abr. 2020.

BRASIL. **Lei nº 12.965, de 22 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. (Marco Civil da Internet). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm. Acesso em: 20 abr. 2020.

BRASIL. **Lei nº 13.709, de 17 de agosto 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso: em 30. set. 2020.

BRASIL. MINISTÉRIO DA JUSTIÇA. Conselho Administrativo de Defesa Econômica-CADE. **Nota Técnica nº 39/2018/CGAA2/SGA1/SG/CADE**. Procedimento Preparatório. Recusa de contratar. Discriminação. Instauração de Inquérito Administrativo para Apuração de Infrações à Ordem Econômica, nos termos dos artigos 13, III, e 66 da Lei 12.529/11 c/c artigo 181 do Regimento Interno do CADE. Diário Oficial da União. Brasília, DF, 21.dez.2018. Disponível em: https://sei.cade.gov.br/sei/modulos/pesquisa/md_pesq_documento_consulta_externa.php?DZ2uWeaYicbuRZEFhBt-n3BfPLlu9u7akQAh8mpB9yOq_PAOpP9dDSgD6LArOomnyuCuxWvMxZXH0h_hNIMOXVz24XbbZ7YVbHdLYBX85ikU5J-39JyCQbDhh5GXrOjb. Acesso em: 20 jun. 2021.

BRASIL. SUPREMO TRIBUNAL FEDERAL. **Ação Direta de Inconstitucionalidade nº 6.389/DF**. Relatora Ministra Rosa Weber. Disponível EM: <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=754358482>. Acesso em: 15 mar. 2021.

BRASIL. Tribunal Regional Federal da Terceira Região. **Sentença 5002801-64.2018.4.03.6105**. 2ª Vara Federal de Campinas, SP. Autor: Walltime Serviços Digitais Ltda. Réu: Caixa Econômica Federal. Juiz José Luiz Paludetto. 11.fev.2020. Disponível em:

<https://pje1g.trf3.jus.br/pje/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?ca=a0c35631a6ff08cbce45cc4573b1aa8d7336eaf4ec2140153d06bc8509c db88d4446971f700b03048685619232361f1e361bd0b8f5bf1229&idProcessoDoc=28165553>. Acesso em: 02 jun. 2021.

BRENNEN, J. Scott; KREISS, D. Digitalisation. In: JENSEN, K. B. et al (Eds.). **The International Encyclopedia of Communication Theory and Philosophy**. Nova Jersey (EUA): John Willey and Sons, 2016. Disponível em: <https://onlinelibrary.wiley.com/doi/book/10.1002/9781118766804> . Acesso em: 10 nov. 2019.

BUTERIN, Vitalik. **Ethereum white paper**. 2013. Disponível em: https://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf. Acesso em: 30 ago. 2020.

CAMPBELL-VERDUYN, Malcolm. What are blockchains and how are they relevant to governance in the global political economy? In: CAMPBELL-VERDUYN, Malcolm (ed.). **Bitcoin and beyond: Cryptocurrencies, blockchains and global governance**. Londres (GB): Routledge, 2018, p. 1-25.

CARDON, Dominique. L Révolution du web social :demain, tous des peuples? In : COMMISSION NATIONALE DE L'INFORMATIQUE ET DE LIBERTÉS. **Vie Privée à l'horizon 2020 : Parole d'experts**. Paris: CNIL, 2020, p. 15-18. Disponível em: https://www.cnil.fr/sites/default/files/typo/document/CNIL-CAHIERS_IPn1.pdf. Acesso em: 03 maio 2021.

CARLSTEN, Miles et al. On the instability of Bitcoin without the block reward. In: ACM SIGSAC – Conference on Computer and communications Security, 16, 2016, Viena (AU). **Proceedings [...]**. Viena: ACM, 2016. p.154-167. Disponível em: https://www.cs.princeton.edu/~arvindn/publications/mining_CCS.pdf. Acesso em: 13 mar. 2020.

CASTELLS, Manuel. **A Galáxia da Internet: Reflexões sobre a Internet, os negócios e a sociedade**. Rio de Janeiro: Zahar, 2003.

CASTELLS, Manuel. **A Sociedade em Rede**. São Paulo: Paz e Terra, 2013.

CAVOUKIAN, Ann. **Privacy by design: The 7 foundational principles**. Jan. 2011. Disponível em: <https://www.ipc.on.ca/wp-content/uploads/resources/7foundationalprinciples.pdf>. Acesso em: 10 jun. 2020.

CAWREY, Daniel. Bitcoin and M-Pesa: Why Money in Kenya has gone digital. **Coindesk**, 10 jul. 2013. Disponível em: <https://www.coindesk.com/bitcoin-and-m-pesa-why-money-in-kenya-has-gone-digital>. Acesso em: 18 abr. 2020.

CAZABET, Remy et al. Tracking Bitcoin users activity using community detection on a network of weak signals. In: International Conference on Complex Networks and Their Applications, 6, Nov. 2017, Lyon (FR). **Proceedings [...]**. Lyon (FR): Springer, 2017. p. 166-177. Disponível em: <https://link.springer.com/book/10.1007/978-3-319-72150-7>. Acesso em: 20 maio 2020.

- CEPI. **Cryptomap**: Alemanha. São Paulo: FGV, 2021. Disponível em: <http://www.fgv.br/direitosp/cryptomap/paginas/Germany.html>. Acesso em: 13 out.2021.
- CHAUM, David. Achieving Electronic Privacy. **Scientific American**, Nova York (EUA), v. 267, n. 2, Ago. 1992. p. 96-101. Disponível em: <https://www.chaum.com/publications/ScientificAmerican-AEP.pdf>. Acesso em: 10 jun. 2020.
- CHAUM, David. Blind signatures for untraceable payments. In: CHAUM, David et al (eds). **Advances in Cryptology**. Boston (EUA): Springer, 1983. Disponível em: https://link.springer.com/chapter/10.1007/978-1-4757-0602-4_18. Acesso em: 14 maio 2019.
- CHEN, Min et al. Big Data: a survey. **Mobile Network and Applications**, Cham (CH), v.19, 2014. p.171-209. Disponível em: <https://link.springer.com/article/10.1007%2Fs11036-013-0489-0>. Acesso em: 17 maio 2020.
- CHESTERMAN, Simon. **One nation under surveillance**: a new social contract to defend freedom without sacrificing liberty. Oxford (GB): Oxford University Press, 2011.
- CHOI, Bryan H. The grokster dead-end. **Harvard Law and Technology**, Cambridge (EUA), v.19, 2005. p.393-411. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=918644. Acesso em: 13 maio 2020.
- CLARK, Charles. **The answer to the machine is in the machine and other collected writings**. Oslo (NO): Institutt for Rettsinformatikk, 1996.
- CLARKE, Roger; WIGAN, Marcus. **You Are Where You've Been The Privacy Implications of Location and Tracking Technologies**. Disponível em: <http://www.rogerclarke.com/DV/YAWYB-CWP.html>. Acesso em: 23 abr. 2020.
- CLAYTON, Richard et al. Ignoring the Great Chinese Firewall of China. In: International Conference on Privacy Enhancing Technologies, 6, 2006, Cambridge (GB). **Proceedings** [...]. Cambridge: Springer-Verlag, 2006. p.20-35. Disponível em: <https://www.cl.cam.ac.uk/~rnc1/ignoring.pdf>. Acesso em: 11 maio 2020.
- CLEMONS, Erick K; MADHANI, Nehal. Regulation of digital business with natural monopolies or third-party payment business models: antitrust lessons from the analysis of Google. **Journal of Management Information Systems**, Londres (GB), v. 27, n.3, 2010, p.43-80. Disponível em: https://repository.upenn.edu/cgi/viewcontent.cgi?article=1368&context=fnce_papers. Acesso em: 13 out.2021.
- COHEN, Julie E. Cyberspace as/and space. **Columbia Law Review**, Nova Iorque, v. 107, 2007. p. 210-256. Disponível em: <https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=1822&context=facpub>. Acesso em: 18 maio 2020.
- COLEMAN, Gabriella. Code is Speech: Legal tinkering, expertise, and protest among free and open source software developers. **Cultural Anthropology**, Arlington (USA), v. 24, n.3, 2009. p.420-454. Disponível em:

<https://anthrosource.onlinelibrary.wiley.com/doi/epdf/10.1111/j.1548-1360.2009.01036.x>. Acesso em: 13 mar. 2020.

COMPARATO, Fábio Konder. **A afirmação histórica dos Direitos Humanos**. 7.ed. São Paulo: Saraiva, 2010.

CONSELHO DA EUROPA. **Convenção Europeia de Direitos Humanos**, de 04 nov. 1950. Roma (IT): Conselho da Europa, 1950. Disponível em: https://www.echr.coe.int/documents/convention_por.pdf. Acesso em: 19 jul. 2020.

DAHL, Robert. **Análise política moderna**. Brasília: UNB, 1988.

DAI, Wei. **B-Money**. 1998. Disponível em: <http://www.weidai.com/bmoney.txt>. Acesso em: 20.fev.2021.

DANAHER, John. The Threat of Algocracy: Reality, Resistance and Accomodation. **Philosophy & Technology**, Nova Iorque, v. 29, 2016. p.245-268. Disponível em: <https://link.springer.com/article/10.1007/s13347-015-0211-1>. Acesso em: 07 abr. 2021.

DASKAL, Jennifer. The un-territoriality of Data. **The Yale Law Journal**, New Haven (EUA), v. 125, n.2, 2015. p.326-397. Disponível em: https://www.yalelawjournal.org/pdf/a.326.Daskal.398_qrhgeoar.pdf . Acesso em: 20 maio 2021.

DE BRUIJN, Hans; HUEVELHOF, Ernst Tem. **Management in Networks**. 2. ed. Londres: Routledge, 2018.

DE FILIPPI, Primavera. **100 women in P2P**: Interview with Primavera De Filippi. 12.maio.2015. Disponível em: <https://p2pvalue.eu/100-women-in-p2p-interview-with-primavera-de-filippi/>. Acesso em: 4 jul. 2020.

DE FILIPPI, Primavera; LOVELUCK, Benjamin. The invisible politics of Bitcoin: governance crisis of a decentralized infrastructure. **Internet Policy Review**, Berlin (DE), v. 5, n. 3, 2016. p. 1-28. Disponível em: <https://policyreview.info/pdf/policyreview-20163-427.pdf>. Acesso em: 18 jan. 2021.

DE FILIPPI, Primavera; WRIGHT, Aaron. **Blockchain and the Law**: The rule of code. Cambridge (EUA): Harvard Press, 2018.

DE FILIPPI, Primavera; HASSAN, Samer. Blockchain technology as a regulatory technology: from code is law to law is code. **First Monday**, Chicago (EUA), v.21, n.12, 2016. Disponível em: <https://firstmonday.org/ojs/index.php/fm/article/view/7113>. Acesso em: 13 out. 2021.

DEEKS, Ashley. An international legal framework for surveillance. **Virginia Journal of International Law**, Charlottesville (EUA), v. 55, n.2, 2015. p. 291-370. Disponível: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2490700. Acesso em: 19 maio 2021.

DENG, Lei et al. Building big data analytics service framework for mobile advertising and marketing. In: IEE International Conference on Big Data Computing Service and

Applications, 1, 2015, Redwood (EUA). **Proceedings** [...]. Redwood: IEE, 2015. p.256-266. Disponível em: <https://ieeexplore.ieee.org/abstract/document/7184889>. Acesso em: 3 mar. 2021.

DIFFIE, Whitfield ; HELLMAN, Martin E. New directions in cryptography. **IEEE Transactions on Information Theory**, Nova York (EUA), v. IT-22, n.6, Nov.1976. p.644-655. Disponível em: <https://ee.stanford.edu/~hellman/publications/24.pdf>. Acesso em: 15 abr. 2020.

DOTTI, René Ariel. A liberdade e o direito à intimidade. **Revista de Informação Legislativa**, Brasília, v. 17, n.66, 1980, p.125-152. Disponível em: <https://www2.senado.leg.br/bdsf/handle/id/181214>. Acesso em: 13 out. 2021.

DUVERGER, Maurice. **Droit Constitutionnel et Institutions Politiques**.2.ed. Paris: Presses Universitaires de France, 1956.

DWORKIN, Ronald. **The Theory and the practice of autonomy**. Cambridge (GB): Cambridge University Press, 1988.

EASTERBROOK, Frank. H. Cyberspace and the law of the horse. **University of Chicago Legal Forum**, Chicago, v. 1996, n.1, 1996. p.207-216. Disponível em: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1204&context=uclf> . Acesso em: 21 jun. 2020.

ELLUL, Jacques. **A técnica e o desafio do século**. Rio de Janeiro: Paz e Terra, 1968

ELLUL, Jacques. A Ambivalência da Técnica. In: Seminário Brasileiro sobre o pensamento de Jacques Ellul: novos atores globais, técnica e direito-um diálogo com Jacques Ellul, 1, 2009, Araraquara. **Anais** [...]. Araraquara: FCL-UNESP, 2009. p.259-294.

ENTREVISTA de Vilém Flusser: On writing, complexity and the technical revolutions. 1 vídeo (10:25 minutos). Osnabrück: Miklós Peternák, set. 1988. Publicado pelo canal Arquivo Vilém Flusser São Paulo. Disponível em: <https://www.youtube.com/watch?v=8rtZXpMUIS8&t=2s>. Acesso em: 02 maio 2020.

ESTADOS UNIDOS DA AMÉRICA. Corte Distrital do Norte do Estado da Califórnia. **Ebay v. Bidder'sEdge**. 24 maio. 2000. Disponível em: <https://casetext.com/case/ebay-v-bidders-edge>. Acesso em: 25 de maio de 2020.

ESTADOS UNIDOS DA AMÉRICA. Estado da Califórnia. Corte de Apelação do 3º Distrito. **Thrifty Tel Inc. v. Bezenek**. 28 jun. 2020. Disponível em: <https://caselaw.findlaw.com/ca-court-of-appeal/1770092.html>. Acesso em: 25 maio 2020.

ESTADOS UNIDOS DA AMÉRICA. Estado da Califórnia. Suprema Corte do Estado da Califórnia. **Intel Corp. v Hamidi**. 10 dez. 2003. Disponível em: <https://law.justia.com/cases/california/court-of-appeal/4th/94/325.html>. Acesso em: 25 maio 2020.

ESTADOS UNIDOS DA AMÉRICA. **Public Law No. 107-56, of 2001(USA Patriot Act)**. Washington (EUA): Congress, [2001]. Disponível em: <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>. Acesso em 20 jun. 2021.

ESTADOS UNIDOS DA AMERICA. Suprema Corte dos Estados Unidos. **Kyllo v. United States**. 11 jun. 2001. Disponível em: <https://supreme.justia.com/cases/federal/us/533/27/case.pdf>. Acesso em: 12 maio 2020.

EYERS, James. Why the Blockchain will propel a services revolution. **Australian Financial Review**, Sidney (AU), 14. dez. 2015. Disponível em: <https://www.afr.com/technology/why-the-blockchain-will-propel-a-services-revolution-20151212-glm6xf>. Acesso em: 12.ago.2020.

FALQUE-PIORRETIN, Isabelle. **Vie Privée à l’horizon 2020 : Parole d’experts**. Paris: CNIL, 2020, p. 15-18. Disponível em: https://www.cnil.fr/sites/default/files/typo/document/CNIL-CAHIERS_IPn1.pdf. Acesso em: 03 maio 2021.

FEIR, Scott. E. Regulations restricting *Internet* access: attempted repair of rupture in China’s great wall restraining the free exchange of ideas. **Pacific Rim Law and Policy Journal**, Seattle (EUA), v.6, n.2, mar. 1997. p.361-389. Disponível em: <https://digitalcommons.law.uw.edu/wilj/vol6/iss2/5/>. Acesso em: 20 jul. 2019.

FERKISS, Victor. Technology and culture: gnosticism, naturalism and incarnational integration. **Cross Currents**, [s. l.], v.30, n. 1, 1980. p.13-26. Disponível em: <https://www.jstor.org/stable/24458026?seq=1>. Acesso em: 01 abr. 2020.

FERRAZ JUNIOR, Tércio Sampaio. **Introdução ao estudo do direito: técnica, decisão e dominação**. São Paulo: Atlas, 2001.

FERRAZ, Maria Cristina Franco. Sociedade Tecnológica: de Prometeu a Fausto. **Contracampo**, Rio de Janeiro, v. 12, n.4, 2000. p.117-124. Disponível em: <https://periodicos.uff.br/contracampo/article/view/17304/10942>. Acesso em: 10 abr. 2020

FINCK, Michèle. **Blockchain regulation and governance in Europe**. Cambridge (GB): Cambridge University Press, 2019.

FINN, Rachel et al. Seven types of privacy. In: GUTWIRTH, et al. **European Data Protection: coming of age?** Dordrecht (NL): Springer, 2013.

FIRMINO, Rodrigo et al. The spatial bonds of Wikileaks. **Government Information Quarterly**, Londres, v.35, 2018. p.389-397. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0740624X17301922>. Acesso em: fev. 2020.

FLORIDI, Luciano et al. **The Onlife Manifesto:being human in a hyperconnected era**. Nova York (EUA): Springer Open, 2015.

FLUSSER, Vilém. **A Escrita. Há futuro para a escrita?** São Paulo: Anablume, 2010.

FLUSSER, Vilém. Do objeto. **Arte, Tecnologia e Novas Mídias**, São Paulo, v.4, n.8, 2006. p.30-35. Disponível em: revistas.usp.br/ars/article/view/2970/3660. Acesso em: 10 mar. 2020.

FLUSSER, Vilém. **Elogio da Superficialidade: o universo das imagens técnicas**. São Paulo: É realizações, 2019.

FLUSSER, Vilém. **Filosofia da caixa preta**. São Paulo: Relume Dumará, 2002.

FLUSSER, Vilém. **Língua e Realidade**. São Paulo: Annablume, 2007.

FLUSSER, Vilém. **O Mundo codificado: por uma filosofia do design e da comunicação**. São Paulo: Cosac & Naif, 2013.

FLUSSER, Vilém. **Vampyrotheuthis infernalis**. São Paulo: Annablume, 2002a.

FOBE, Nicole Julie. **O Bitcoin como moeda paralela: uma visão econômica e a multiplicidade de desdobramentos jurídicos**. Tese (Mestrado em Direito) - Escola de Direito da Fundação Getúlio Vargas. São Paulo. 2016.

FOUCAULT, Michelle. **Segurança, Território e População**. São Paulo: Martins Fontes, 2008.

FOUCAULT, Michelle. **Vigiar e Punir: nascimento da prisão**. Petrópolis: Vozes, 1987.

FRANÇA. **Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure**. Paris (FR): L'Assemblée Nationale, 2011. Disponível em <https://www.legifrance.gouv.fr/loda/id/JORFTEXT000023707312/>. Acesso em: 20.jun.2021.

FRENI, Pierluigi et al. Fixing Social media with the Blockchain. In: EAI International Conference on Smart Objects and Technologies for Social Good, 6, 2020, [S. l.]. **Proceedings** [...]. [s. l.]: EAI, 2020. p. 175-180. Disponível em: <https://dl.acm.org/doi/abs/10.1145/3411170.3411246>. Acesso em: 20.jan.2021.

FRIEDMAN, Milton. **Capitalismo e Liberdade**. São Paulo: LTC, 2014.

FRISCHMANN, Brett M. The Prospect of Reconciling *Internet* and Cyberspace. **Loyola University Chicago Law Journal**, Chicago (EUA), v.35, n.1, 2003. p.205-234. Disponível em: <https://www.ssrn.com/abstract=515970>. Acesso em: 13 jun. 2020.

FROSINI, Vittorio. Los Derechos Humanos em la era tecnológica. In: PÉREZ LUÑO, Antonio Henrique (Coord.). **Derechos Humanos y Constitucionalismo ante el Tercer Milenio**. Madrid: Marcial Pons, 1996. p.79-87. Disponível em: <https://www.corteidh.or.cr/tablas/a19202.pdf>. Acessado em 04 maio 2021.

G1. **Nem FBI consegue decifrar arquivos de Daniel Dantas, diz jornal**. 2010. Disponível em: <http://g1.globo.com/politica/noticia/2010/06/nem-fbi-consegue-decifrar-arquivos-de-daniel-dantas-diz-jornal.html>. Acesso em: 02 mai. 2021.

GALIMPERTI, Umberto. O ser humano na era da técnica. **IHU Ideias**, São Leopoldo, v. 13, n.218, 2015. p.3-18. Disponível em: <http://www.ihu.unisinos.br/images/stories/cadernos/ideias/218cadernosihuideias.pdf>. Acesso em: 10 maio. 2020.

GARCÍA-PELAYO, Manuel. **Derecho Constitucional Comparado**. 4.ed. Madrid: Revista de Occidente, 1967.

GASSER, Urs. Recording privacy law: reflections on the future relationship among law, technology and privacy. **Harvard Law Review Forum**, Cambridge (EUA), v. 130, n.2, Dez.2016 p.61-70. Disponível em: <https://harvardlawreview.org/2016/12/recoding-privacy-law-reflections-on-the-future-relationship-among-law-technology-and-privacy/> . Acesso em: 17 maio 2020.

GILLEPSIE, Tarleton. A relevância dos algoritmos. **Parágrafo**, São Paulo, v.6, n.1, jan./ abr. 2018. p.95-121. Disponível em: <http://revistaseletronicas.fiamfaam.br/index.php/recicofi/article/view/722>. Acesso em: 02 dez. 2019.

GNU. **Filosofia do Projeto GNU**. 2021. Disponível em: <https://www.gnu.org/philosophy/philosophy.html>. Acesso em: 10 maio 2021.

GÓIS JÚNIOR, José Calda. **O Direito da era das redes**. São Paulo: Edipro, 2002.

GOLDSMITH, Jack. Against Ciberanarchy. **University of Chicago Law Review**, Chicago (EUA), v.65, n.4, 1999, p.1199-1250. Disponível em: <https://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=5000&context=ucprev>. Acesso em: 13 out. 2021.

GOLDSMITH, Jack Landman; WU, Tim. **Who Controls the Internet? Illusions of a borderless world**. Nova Iorque: Oxford University Press, 2006.

GOULART, Guilherme Damasio Duarte. Impacto das novas tecnologias nos direitos humanos e fundamentais: acesso à internet e a liberdade de expressão. **Revista Direitos Emergentes na Sociedade Global**, Santa Maria, v.1, n.1, 2012, p.145-168. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/5955/pdf_1#.YWegFtrMLIU. Acesso em: 13 out. 2021.

GRÉCIA. **Regulation No 165/2011**. Atenas (GR): Parlamento Helénico, 2011. Disponível em: <https://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Greece.pdf>. Acesso em: 19.mar. 2021.

GREER, Damon. Safe harbor: a framework that works. **International Data Privacy Law Review**, Oxford (GB), v. 1, n.3, 2011. p. 143-148. Disponível em: <https://academic.oup.com/idpl/article/1/3/143/688691>. Acessado em: 26 maio 2021.

GROSS, Leo. The Peace of Westphalia. **The American Journal of International Law**, Washington (EUA), v.42, n.1, p.20-41, jan. 1948. Disponível em: http://www.kentlaw.edu/faculty/bbrown/classes/IntlOrgSp07/CourseDocs/IGross_PeaceofWestphalia1648_1948.pdf. Acesso em: 15 jan. 2020.

GUPTA, Neha. Security and privacy issues of Blockchain technology. In: KIM, Shiho; DEKA, Ganesh Chandra (eds.). **Advanced applications of Blockchain technology**. Cingapura (SIN): Springer, 2020. p. 204-226.

GURSES, Seda et al. Crypto and empire: the contradictions of conter-surveillance advocacy. **Media, Culture and Society**, Nova York (EUA), v.38, n.4, 2016. p.576-590. Disponível em: <https://journals.sagepub.com/doi/abs/10.1177/0163443716643006?journalCode=mcsa>. Acesso em: 20 mar. 2020.

HABERMAS, Jürgen. **Técnica e ciência como ideologia**. Lisboa: Edições 70, 2009.

HACKER, Philipp; TOMALE, Chris. Crypto-securities regulation: ICOs, token sales and cryptocurrencies under EU Financial Law. **European Company and Financial Law Review**, Berlin (DE), v. 15, Nov. 2015, p.645-696. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3075820. Acesso em: 13 abr. 2021.

HAN, Byung-Chul. **No enxame: perspectivas do digital**. Petrópolis: Vozes, 2018.

HARDY, Trotter. The proper legal regime for cyberspace. **Pittsburg Law Review**, Pittsburgh (EUA) v. 55, 1994. p. 993-1053. Disponível em <https://scholarship.law.wm.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1536&context=facpubs>. Acesso em: 12 abr. 2021.

HARRIOU, Maurice. **Princípios de Derecho Público y Constitucional**. Trad. Ruíz del Castillo. Santiago (CL): Ediciones Jurídicas Olejnik, 1926.

HEIDEGGER, Martin. **Marcas do Caminho**. Petrópolis: Vozes, 2008.

HEIDEGGER, Martin. A questão da técnica. Trad. Marco Aurélio Werle. **Scientiae Studia**, São Paulo, v.5, n.3, 2007. p.375-398. Disponível em: http://www.scientiaestudia.org.br/revista/PDF/05_03_05.pdf. Acesso em: 10 abr. 2020.

HEIDEGGER, Martin. **Seminários de Zollikon**. Petrópolis: Vozes, 2001.

HERIAN, Robert. The politics of blockchain. **Law Critique**, Amsterdam (NL), v. 29, 2018, p.129-131. Disponível em: <https://link.springer.com/article/10.1007%2Fs10978-018-9223-1>. Acesso em: 05 mar. 2021.

HERRERA-FLORES, Joaquin. Direitos Humanos, interculturalidade e racionalidade de resistência. **Sequência**, Florianópolis, v. 23, n.44, 2002, p.9-29. Disponível em: <https://periodicos.ufsc.br/index.php/sequencia/article/view/15330/13921>. Acesso em: 13 out. 2021.

HESMONDHALGH, David. Bordieu, media and cultural production. **Media, Culture and Society**, [s.l.], v. 28, n. 2., 2006. p. 211-231. Disponível em: <http://oro.open.ac.uk/3156/>. Acesso em: 15 jan. 2020.

HOLANDA. Ministério da Segurança e Justiça. **Cabinet's view on encryption**. 04.jan.2016. Amsterdam: Ministry of Security and Justice, 2016. Disponível em:

<https://www.enisa.europa.eu/about-enisa/structure-organization/national-liaison-office/news-from-the-member-states/nl-cabinet-position-on-encryption>. Acesso em: 06 maio 2020.

HOOD, Christopher; MARGETTS, Helen. **The Tools of Government in the age of the Digital Age**. 2.ed. Londres: Red Globe Press, 2007.

HUGHES, Eddie et al. Unlocking Blockchain: embracing new technologies to drive efficiency and empower the citizen. **The Journal of the British Blockchain Association**, Londres (GB), v. 1, n.2, Dez.2018. p.63-73. Disponível em: <https://jbba.scholasticahq.com/article/3741.pdf>. Acesso em: 25 jun. 2020.

HUGHES, Eric. **A Cypherpunk's Manifesto**. 9.mar.1993. Disponível em: <https://nakamotoinstitute.org/static/docs/cypherpunk-manifesto.txt>. Acesso em: 28 maio 2020.

INFOMONEY. **China anuncia que todas as transações com criptomoedas são ilegais**. 24 Set. 2021. Disponível em: <https://www.infomoney.com.br/mercados/china-anuncia-que-todas-transacoes-com-criptomoedas-sao-ilegais/>. Acesso em: 24 set. 2021.

INTERNET GOVERNANCE FORUM. **Carta de Direitos Humanos e Princípios para a Internet**. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2015.

ISHAI, Yuval. Cryptography from anonymity. In: Annual IEEE Symposium on Foundations of Computer Science, 47, 2006, Berkeley (EUA). **Proceedings [...]**. Los Alamitos (EUA): IEEE, 2006. p.239-248. Disponível em: <https://ieeexplore.ieee.org/document/4031360/>. Acesso em: 20 abr. 2020.

JOHNSON, David R.; POST, David G. Law and Borders: the rise of Law in Cyberspace. **Stanford Law Review**, Stanford (EUA), v. 48, 1996. p. 1367-1404. Disponível em: <https://www.ssrn.com/abstract=535>. Acesso em: 02 dez. 2019.

JOHNSON, Deborah G. **Computer ethics: the philosophy of computing and information**. Englewood Cliffs (EUA): Prentice-Hall, 1985.

LIMA, Roberto Kant. **Aspectos jurídicos da internet**. São Paulo: Saraiva, 2008.

KANT, Immanuel. **Duas introduções à Crítica do Juízo**. Ricardo Ribeiro Terra (Org.). São Paulo: Iluminuras, 1995.

KAYSER, Pierre. **La protection de l'avie privée : protection du secret de la vie privée**. Marseille (FR) : Presses Universitaires d'Aux-Marseille, 1984.

KELSEN, Hans. Sovereignty. In: PAULSON, Bonnie Litschewski e PAULSON, Stanley (Orgs.). **Normativity and Norms: Critical Perspectives on Kelsenian Themes**. New York: Oxford University Press Inc.: 2007, p. 525-536.

KELSEN, Hans. **Teoria Pura do Direito**. Coimbra: Armênio Amado, 1984.

KELSEN, Hans. **Teoria Pura do Direito: introdução à problemática científica do Direito**. Trad. J. Cretella Jr; Agnes Cretella. São Paulo: Editora dos Tribunais, 2003.

KELTY, Christopher M. **Two bits: The cultural significance of Free Software**. Durham (EUA): Duke University Press, 2008.

KERR, Orin S. The problem of perspective in the *Internet Law*. **Georgetown Law Journal**, Washington (EUA), v. 91, p.357-405, 2003. Disponível em:

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=310020. Acesso em: 11 maio 2020.

KIRDEMIR, Baris et al. Assessing bias in Youtube's video recommendation algorithm in a cross-lingual and cross-typical context. In: International Conference on Social Computing, Behavioural Cultural Modeling and Prediction and Behavior Representation in Modeling and Simulation, 14, 2021, Washington (EUA). **Proceedings [...]**. Washington (EUA): SBP-BRIMS, 2021, p.71-80. Disponível em: <http://sbp-brims.org/2021/proceedings/>. Acesso em: 15 ago.2021.

KIZZA, Joseph Migga. **Ethical and social issues in the information age**. Londres (GB): Springer, 2017.

KLONICK, Kate. The new governors: the people, rules, and processes governing online speech. **Harvard Law Review**, Cambridge (EUA), v. 131, n.6, 2018. p.1598- 1670.

Disponível em: <https://harvardlawreview.org/2018/04/the-new-governors-the-people-rules-and-processes-governing-online-speech/>. Acesso em: 04.mar.2021.

KRAUSE, Max J.; TOLAYMAT, Thabet. Quantification of energy and carbon costs for mining cryptocurrencies. **Nature Sustainability**, Londres (GB), v.1, 2018. p.711-718.

Disponível em: <https://www.nature.com/articles/s41893-018-0152-7>. Acesso em: 20 jun. 2020.

KUBIATOWICZ, John. Extracting guarantees from chaos. **Communications from ACM**, Nova York (EUA), v.46, n.2, Fev.2003. p.33-38. Disponível em:

<https://dl.acm.org/doi/10.1145/606272.606297>. Acesso em: 20 abr. 2021.

LAFFER, Celso. **A reconstrução dos direitos humanos: um diálogo com o pensamento de Hannah Arendt**. São Paulo: Companhia das Letras, 1988.

LAFFERIÈRE, Julien. **Manuel de Droit Constitutionnel**. Paris (FR): D. Montcrestien, 1947.

LAMPORT, Leslie. The Byzantine Generals problem. **ACM Transactions on Programming Languages and Systems**, Nova York (EUA), v. 4, n.3, Jul.1982. p.383-401. Disponível em:

<https://www.microsoft.com/en-us/research/uploads/prod/2016/12/The-Byzantine-Generals-Problem.pdf>. Acesso em: 14 abr. 2020.

LAND, Molly Beutz. Protecting rights online. **The Yale Journal of International Law**, New Haven (EUA), v.34, n.1, 2009. p. 1-44. Disponível em:

<https://digitalcommons.law.yale.edu/yjil/vol34/iss1/2/>. Acesso em: 23 jun. 2021.

LAPRISSE, John. **US National Security Agency Surveillance: A Problem of Alegality**. 10. Jun. 2013. Disponível em: <http://ohrh.law.ox.ac.uk/us-national-security-agency-surveillance-a-problem-of-allegality/>. Acesso em: 10 nov. 2019.

- LEDGER. **The Blockchain Generations**. 11 maio 2021. Disponível em: <https://www.ledger.com/academy/blockchain/web-3-the-three-blockchain-generations>. Acesso em: 15 jul. 2021.
- LEMKE, Thomas. **Foucault, governamentalidade e crítica**. São Paulo: Politeia, 2017.
- LEMONS, Ronaldo. **Direito e Tecnologia**. Rio de Janeiro: FGV, 2005.
- LESSIG, Lawrence. **The Code is the Law**. 09 abr. 1999. Disponível em: <https://www.tech-insider.org/berkman-center/research/1999/0409.html>. Acesso em: 13 out. 2021.
- LESSIG, Lawrence. **Code**. Nova York (EUA): Basic Books, 2006.
- LESSIG, Lawrence. The New Chicago School. **The Journal of Legal Studies**, Chicago (EUA), v.27, n. S2, jun. 1998. p.661-691. Disponível em: <https://www.jstor.org/stable/10.1086/468039?seq=1>. Acesso em: maio 2020.
- LIMA, Roberto Kant. **Aspectos jurídicos da Internet**. São Paulo: Saraiva, 2000.
- LIPPERT, Randy K.; NEWELL, Bryce Clayton. Debate introduction: the privacy and surveillance implications of police body cameras. **Surveillance and Society**, Windsor (Canada), v. 14, n.1, 2016. p. 113-116. Disponível em: https://www.researchgate.net/publication/301340317_Debate_Introduction_The_Privacy_and_Surveillance_Implications_of_Police_Body_Cameras. Acesso em: 09 ago. 2020.
- LYON, David. **The rise of surveillance society: computers and social control in context**. Cambridge (GB): Polity Press, 2001.
- MARTÍNEZ-BEJAR, R.; BRÄNDLE, G. Contemporary technology management practices for facilitating social regulation and surveillance. **Technology and Society**, Amsterdam (NL), v. 54, 2018, p. 139-148. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0160791X17301161>. Acesso em: 13 out. 2021.
- MACKENZIE, Adam et al. **Improving obfuscation in the CryptoNote Protocol**. 26 jan. 2015. Disponível em: <https://web.getmonero.org/es/resources/research-lab/pubs/MRL-0004.pdf>. Acesso em: 06 fev. 2021.
- MACLUHAN, Marshall. **Os meios de comunicação como extensões do homem**. São Paulo: Cultrix, 1969.
- MANCINI, Anna. **Ancient Egyptian Wisdom for the Internet**. Washington (EUA): University Press of America, 2002.
- MANKIW, Nicholas Gregory. **Macroeconomics**. Nova Iorque: Worth Publishers, 2010.
- MARCHETTO, Patrícia Borba; BARRIENTOS-PARRA, Jorge David; RODRIGUES, Gustavo Alarcon. A técnica informacional como ferramenta de redução da privacidade na rede: análise do caso Wikileaks. **Relações Internacionais no Mundo Atual**, Curitiba, v. 3, nº 24, 2019. p.494-520. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RIMA/article/view/4061>. Acesso em: 12 jul. 2020.

MARÍAS, Julian. **Introducción a la filosofía**. Madrid: Revista de Occidente, 1947.

MARINHO, Gustavo. Mais de R\$ 1 bilhão em Bitcoin negociados na Venezuela. **Cointimes**, 19 fev. 2020. Disponível em: <https://cointimes.com.br/mais-de-r-1-bilhao-em-bitcoin-negociados-na-venezuela/>. Acesso em: 18 abr. 2020.

MARION YOUNG, Iris. **Justice and the Politics of Difference**. Princeton (EUA): Princeton University Press, 1990.

MARTÍNEZ-BEJAR, R.; BRÄNDLE, G. Contemporary technology management practices for facilitating social regulation and surveillance. **Technology and Society**, Amsterdam, v. 54. p. 139-148, 2018. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0160791X17301161>. Acesso em: 16. jan. 2020.

MARTINS, Hermínio. **Experimentum Humanum: Civilização Tecnológica e Condição Humana**. Belo Horizonte: Fino Traço, 2012.

MARTINS, Hermínio. **Hegel, Texas e outros ensaios da Teoria Social**. Coimbra: Século XXI, 1996.

MARX, Garry T. What's new about the "new surveillance? classifying for change and continuity. **Surveillance and Society**, Chappel Hill (EUA), v. 1, n. 1, 2002. p. 9-29. Disponível em: https://www.researchgate.net/publication/250812871_What's_New_About_the_New_Surveillance_Classifying_for_Change_and_Continuity. Acesso em: 21.set.2020.

MARX, Karl. **Contribuição à crítica da economia política**. 2.ed. São Paulo: Expressão Popular, 2008.

MAY, Timothy. **Crypto Anarchy and Virtual Communities**. Dez. 1994. Disponível em: <https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-virtual-comm.html>. Acesso em: 10 maio 2020.

MAYER, Jeremy D. 9-11 and the secret FISA Court: from watchdog to lapdog. **Case Western Reserve Journal of International Law**, Cleveland (EUA), v. 34, n.2, 2002. p. 249-252. Disponível em: <https://core.ac.uk/download/pdf/214078882.pdf>. Acesso em: 20 maio 2021.

MAYER-SCHÖNBERGER, Viktor. Beyond privacy, beyond rights – toward a "Systems" Theory of Information Governance. **California Law Review**, Berkeley (EUA), v. 98, 2011. p. 1853-1886. Disponível em: <https://29qish1lqx5q2k5d7b491joo-wpengine.netdna-ssl.com/wp-content/uploads/2014/10/Mayer-Schonberger.FINAL-FIXED.pdf>. Acesso em: 17.ago.2020.

MCGOWAN, David. Website Acess: The case for consent. **Loyola University of Chicago Law Journal**, Chicago (EUA), v.35, 2003. p.341-382. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=420620. Acesso em: 22 jun.2020.

MCLUHAN, Marshall. **Os meios de comunicação como extensões do homem**. São Paulo: Cultrix, 1969.

MICHAELIS. **Moderno dicionário da língua portuguesa**. São Paulo: Melhoramentos, 2021. Disponível em: <http://michaelis.uol.com.br/moderno/portugues/index.php>. Acesso em: 07.abr.2021.

MILIBAND, Ralph. **O Estado na Sociedade Capitalista**. Rio de Janeiro: Zahar, 1982.

MILLARD, Christopher. Blockchain and law? Incompatible codes ? **Computer Law and Security Review**, Amsterdam (NL), v.34, 2018. p.843-846. Disponível em: <https://www.sciencedirect.com/science/article/pii/S0267364918302437>. Acesso em: 10 jan. 2021.

MONTERO, Etienne; ENIS, Quentin Van. Enabling freedom of expression in light of filtering measures imposed on *Internet* intermediaries: squaring the circle? **Computer Law and Security Review**, Londres (GB), v.27, 2011. p.21-35. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364910001792>. Acesso em: 15 mar. 2020.

MOZOROV, Evgeny. The real privacy problem. **MIT- Technology Review**, Bostom (EUA), v, 116, n. 6, Nov.2013, p.32-43. Disponível em: <https://www.technologyreview.com/magazines/a-tale-of-two-drugs/>. Acesso em: 13 abr. 2021.

NAKAMOTO, Satoshi. **Bitcoin: a peer-to-peer electronic cash system**. 2008. Disponível em: <https://bitcoin.org/bitcoin.pdf>. Acessado em 20 jan. 2020.

NARAYANAN, Arvind et al. **Bitcoin and Cryptocurrency Technologies: Comprehensive introduction**. Nova Jersey (EUA): University of Princeton Press, 2016.

NARAYANAN, Arvind. What happened to the crypto dream? part 2. **IEE Security and Privacy Magazine**, Nova York (EUA), v.1., n.2, Mar. 2013, p.75-76. Disponível em: <https://www.cs.princeton.edu/~arvindn/publications/crypto-dream-part2.pdf>. Acesso em: 18 maio 2021.

NARAYANAN, Arvind; SHIMITOV, Vitaly. De-anonymizing social networks. In: Symposium on Security and Privacy, 30, 2009, Cleveland (EUA), **Papéis da Conferência [...]**, Cleveland: IEEE, 2001, p. 173-187. Disponível em: <https://ieeexplore.ieee.org/abstract/document/5207644>. Acesso em: 10 maio 2020.

NARAYANAN, Arvind; SHIMITOV, Vitaly. Robust de-anonymization of large sparse datasets. In: Symposium on Security and Privacy, 29, 2008, Cleveland (EUA), **Papéis da Conferência [...]**, Cleveland: IEEE, 2001, p. 111-125. Disponível em: <https://ieeexplore.ieee.org/document/4531148>. Acesso em: 15 maio 2020.

NEGROPONTE, Nicholas. **Being Digital**. Londres: Hodder & Stoughton, 1995.

NISSEBAUM, Helen. **Privacy in context: technology, policy and the integrity of social life**. Stanford (EUA): Stanford University Press, 2010.

NISSIM, Kobbi et al. Bridging the gap between computer science and legal approaches to privacy. **Harvard Journal of Law and Technology**, Cambridge (EUA), v. 31, n. 2, 2018, p. 688-779. Disponível em: <https://privacytools.seas.harvard.edu/files/privacytools/files/02.-article-wood-7.21.pdf>. Acesso em: 8 abr. 2021.

NIWA, Henrique. **Um sistema de voto eletrônico utilizando a Blockchain**. Tese (Mestrado em Computação Aplicada) – Instituto Nacional de Pesquisas Espaciais. São José dos Campos, 2019.

O'TOOLE JR, Lawrence J; MEIER, Kenneth, J. Modelling the impact of public management: Implications of Structural Context. **Journal of Public Administration Research and Theory**, Oxford (Reino Unido), v. 9, n.4, 1999, p.505-526. Disponível em: <https://academic.oup.com/jpart/article-abstract/9/4/505/921326?redirectedFrom=fulltext>. Acesso em: 16 jul.2020.

OCDE. **OECD Guidelines for Multinational Enterprises**. Paris (FR): OECD Publishing, 2011. Disponível em: <https://www.oecd.org/daf/inv/mne/48004323.pdf>. Acesso em: 10 jun. 2021.

OEA. **Convenção Americana sobre Direitos Humanos**, de 22 nov. 1969. San José (CR): OEA, 1969. Disponível em https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 15 abr. 2020.

OLIVEIRA, Rafael Santos et al. **Direito à privacidade na internet: desafios para a proteção da vida privada e o direito ao esquecimento**. **Revista da Faculdade de Direito da UFMG**, Belo Horizonte, n. 70, 2017, p.561-594. Disponível em: <https://revista.direito.ufmg.br/index.php/revista/article/view/1863/1765>. Acesso em: 13 out. 2021.

OLIVEIRA JÚNIOR, José Alcebíades de. **Teoria Jurídica e Novos Direitos**. Rio de Janeiro: Lumen Juris, 2000.

OLSON, Kathleen K. Cyberspace as place and the limits of metaphor. **Convergence**, Thousand Oaks (EUA), v. 11, n. 1, mar.2005, p.10-18. Disponível em: <https://journals.sagepub.com/doi/10.1177/135485650501100102>. Acesso em: 11 maio 2020.

OMRI, Marian. Are cryptocurrencies super tax heavens? **Michigan Law Review**, Ann Arbor (EUA), v.112, 2013, p.38-48. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2305863. Acesso em: 16.jul.2020.

ONU. Alto Comissariado das Nações Unidas para os Direitos Humanos. **Translation 2015/0279-WH – Legal status encryption technology in Germany**. 2015. Disponível em: <https://www.ohchr.org/Documents/Issues/Opinion/Communications/States/Germany.pdf>. Acesso em: 05 mar. 2021.

ONU. Alto Comissariado para Direitos Humanos. **The right to Privacy in the Digital Age**. 9.abr.2018. Disponível em:

<https://www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/PiratePartiesInternational.pdf>. Acesso em: 20 maio 2021.

ONU. Comitê de Direitos Humanos. **Concluding observations on the fourth periodic report to the United States of America**. 23 abr. 2014. Disponível em: <http://docstore.ohchr.org/SelfServices/FilesHandler.ashx?enc=6QkG1d%2FPPrICAqhKb7yhSijKy20sgGcLSyqccX0g1nnMFNOUOQBx7X%2BI55yhIwlkDk6CF00Adiqu2L8SNxDB4%2BVRPkf5gZfbTQO3y9dLrUeUaTbS0RrNO7VHzbyxGDJ%2F>. Acesso em: 20 maio 2020.

ONU. Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD). **How Blockchain can power sustainable development**. 22 jul. 2021. Disponível em: <https://unctad.org/news/how-blockchain-can-power-sustainable-development>. Acesso em: 15 ago. 2021.

ONU. Conselho de Direitos Humanos. **Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression - A/HRC/17/27**. 16 maio 2011. Disponível em: <https://undocs.org/en/A/HRC/17/27>. Acesso em: 20 maio 2020.

ONU. Conselho de Direitos Humanos. **The Promotion, protection and enjoyment of the human rights on the Internet- A/HRC/20/L.13**. 29 jun. 2012. Disponível em: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/20/L.13. Acesso em: 20 maio 2021.

ONU. Conselho de Direitos Humanos. **General Comment No 31: the nature of the general legal obligation imposed on States Parties covenant**. 29. mar.2004. Disponível em: [https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/c\)GeneralCommentNo31TheNatureoftheGeneralLegalObligationImposedonStatesPartiestotheCovenant\(2004\).aspx](https://www.ohchr.org/EN/Issues/Education/Training/Compilation/Pages/c)GeneralCommentNo31TheNatureoftheGeneralLegalObligationImposedonStatesPartiestotheCovenant(2004).aspx). Acesso em: 20 maio 2021.

ONU. Conselho de Direitos Humanos. **Human Rights Council, Rep. of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression - A/HRC/23/40**. 17.abr.2013 (2013a). Disponível em: <https://undocs.org/A/HRC/23/40>. Acesso em: 20 maio 2020.

ONU. Conselho de Direitos Humanos. **Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin – A/HRC/ 13/37**. 28.dez.2009. Disponível em: <https://undocs.org/A/HRC/13/37>. Acesso em: 20 maio 2021.

ONU. Conselho de Direitos Humanos. **Resolution adopted by the General Assembly on 18 December 2013 – A/RES/68/167**. 18.Dez.2013 (2013b). Disponível em: <https://undocs.org/A/RES/68/167>. Acesso em: 25 maio 2020.

ONU. **Declaração Universal dos Direitos Humanos**, de 10 dez. 1948. Genebra (CH): ONU, 1948. Disponível em: <https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>. Acesso em: 10.abr.2020.

ONU. Unidade Conjunta de Inspeção. **Blockchain applications in the United Nations system: towards a state of readiness – JIU/REP/2020/7**. 2020. Disponível em: <https://undocs.org/JIU/REP/2020/7>. Acesso em: 5.jan.2021.

ORTEGA Y GASSET, José. **A Meditação da Técnica**: Vicissitudes da ciência, cacofonia da física. Rio de Janeiro: Livro Ibero-Americano, 1963.

OUA. **Carta Africana dos Direitos Humanos e dos Povos**, de 27 jul. 1981. Nairóbi (KE): OUA, 1981. Disponível em: <http://www.dhnet.org.br/direitos/sip/africa/banjul.htm>. Acesso em: 25 jul. 2020.

PANNIKAR, Raimundo. Seria a noção de direitos humanos um conceito ocidental?. In: BALDI, César Augusto (Org.). **Direitos Humanos na Sociedade Cosmopolita**. Rio de Janeiro: Renovar, 2004, p.205-238.

PARRY, R. Episteme and Techne. In: **Stanford Encyclopedia of Philosophy**. 2003. Disponível em: <http://plato.stanford.edu/entries/episteme-techne/>. Acesso em: 19 abr. 2020.

PELL, Stephanie K; SOGHOIAN, Christopher. Your secret sting-ray's no secret anymore: the vanishing government monopoly over cellphone surveillance and It's impacts on National security and consumer privacy. **Harvard Journal of Law and Technology**, Cambridge (EUA), v.28, n.1, mar/jun., 2014, p.1-76. Disponível em: <https://www.ssrn.com/abstract=2437678>. Acesso em: 04 dez. 2019.

PENG, Kun. **Anonymous communication networks**: Protecting privacy on the web. Londres (GB): CRC Press, 2014.

PÉREZ LUÑO, Antonio Enrique. **La tercera generación de derechos humanos**. Madrid (ES): Aranzadi, 2006.

PERRY, Susan; RODA, Claudia. **Human rights and digital technology**: digital tightrope. Londres (GB): Palgrave-MacMillan, 2017.

PIETERSE, Jan Nederveen. Leaking superpower: Wikileaks and the contradictions of democracy. **Third World Quarterly**, Oxford (GB), v.33, n.1, 2012, p.1909-1924. Disponível em: https://www.researchgate.net/publication/262085793_Leaking_Superpower_WikiLeaks_and_the_Contradictions_of_Democracy. Acesso em: 24.abr.2020.

PIMENTA BUENO, José Antônio. **Direito Público Brasileiro e a Análise da Constituição do Império**. Rio de Janeiro: Ministério da Justiça/Serviço de Documentação, 1958.

PINHEIRO, Marília P. Futre. Utopia and Utopias: a study on a literacy genre in antiquity. In: **Authors, Authority and Interpreters in the Ancient Novel**. Groningen (NL): Barkhuis, 2006, p. 147-171.

PINTO, Álvaro Vieira. **A sociologia dos países subdesenvolvidos**. Rio de Janeiro: Contraponto, 2008.

PIOVESAN, Flávia. Ações humanas e direitos humanos. **Revista USP**, São Paulo, n. 69, 2006, p.36-43. Disponível em:
<https://www.revistas.usp.br/revusp/article/viewFile/13511/15329>. Acesso em: 13 out.2021.

POMPÉO, Wagner Augusto; SEEFELDT, João Pedro. Nem tudo está no Google: deepweb e o perigo da invisibilidade. In: Congresso Internacional de Direito e Contemporaneidade. **Anais [...]**, Santa Maria: UFSM, 2013. Disponível em:
<http://coral.ufsm.br/congressodireito/anais/2013/3-11.pdf>. Acesso em: 20 jul.2019.

POSNER, Richard Allen. Social norms and the law: an economic approach. **American Economic Review**, Pittsburgh (EUA), v. 87, n.2, p. 365-369, 1997. Disponível em:
<https://econpapers.repec.org/scripts/redir.pf?u=http%3A%2F%2Flinks.jstor.org%2Fsci%3Fsi%3D0002-8282%2528199705%252987%253A2%253C365%253ASNATLA%253E2.0.CO%253B2-1%26origin%3Drepec;h=repec:aea:aecrev:v:87:y:1997:i:2:p:365-69> . Acessado em 20 jul. 2020.

POSTER, Mark. **The Second Media Age**. Nova Jersey (EUA): Wiley, 2013.

PUZIS, Rami et al. Controllable Privacy Preserving Blockchain Fiat Chain: Distributed Privacy Preserving Cryptocurrency with Law Enforcement Capabilities. In: International Symposium on Cyber Security, Cryptography and Machine Learning, 3, 2019. **Proceedings [...]**, Beer-Sheva (IL): Springer, 2019, p. 178-197. Disponível em:
<https://link.springer.com/book/10.1007/978-3-030-20951-3>. Acesso em: 20 abr. 2021.

RAEESI, Reza. The silk road, Bitcoins, and the global prohibition regime on the international trade in illicit drugs: can this storm be weathered ? . **Glendon Journal of International Studies**, York (GB), v. 8, n.1, 2015, p.1-20. Disponível em:
<https://gjis.journals.yorku.ca/index.php/gjis/article/view/38935/36402>. Acesso em: 29 mar. 2020.

RAMAMURTHY, Bina. **Blockchain in action**. Shelter Island (EUA): Manning Publications, 2020.

RAMOS, André de Carvalho. **Curso de Direitos Humanos**. São Paulo: Saraiva, 2014.

REIDENBERG, Joel R. Lex Informatica: The formulation of information policy rules through technology. **Texas Law Review**, Austin (EUA), v.76, n.3, Fev. 1998, p.553-593. Disponível em:
https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship. Acesso em: 4 abr. 2020.

REINO UNIDO. Office for Science. **Distributed Ledger Technology: beyond block chain**. Londres: U.K Office for Science, 2016. Disponível em:
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf. Acesso em: 10.maio.2021.

RICKERT, Heinrich. Die Grenzen der naturwissenschaftlichen Begriffsbildung. Freiburg: J.C.B Mohr, 1896 apud LARENZ, Karl. **Metodologia da Ciência Jurídica**. 3.ed. Lisboa: Calouste Gulbenkian, 1997, p.125-132.

RILEY, Jenn. **Understanding metadata**: what is metadata, and what is it for? Baltimore (EUA): NISO Press, 2017.

RIVEST, Ronald Linn. et al. A method for obtaining digital signatures and public-key cyptosystems. **Communications on the ACM**, Nova York (EUA), v. 26, n.1, Jan.1983. p.120-126. Disponível em <https://dl.acm.org/doi/abs/10.1145/357980.358017>. Acesso em: 13 mar.2020.

ROBERT, Jacques. **Liberté religieuse et le régime des cultes**. Paris : Presses Universitaires de France, 1977.

RODRIGUES, Gustavo Alarcon. **Criptomoedas**: análise e adequação dos criptoativos em face do direito. Trabalho de Conclusão de Curso (Bacharel em Direito) - Faculdade de Ciências Humanas e Sociais, UNESP. Franca, 86 p. 2018.

RODRIGUES, Gustavo Alarcon; MARCHETTO, Patrícia Borba. Vigilância Localizacional em tempos de pandemia: uso de tecnologias de rastreamento e seu impacto nos direitos fundamentais. In: AMORIM, José Campos; VEIGA, Fabio da Silva; AZEVEDO, Patrícia Anjos. **Desafios do Legaltech**. Porto: Iberojur e Instituto Superior de Contabilidade de Administração do Porto, 2020, p. 278-286.

RODRIGUES, Gustavo Alarcon; MARCHETTO, Patrícia Borba; SILVA, Otávio Augusto Mantovani. Questionamentos acerca do Libra: criptomoeda, moeda e soberania. **Economic Analysis of Law**, Brasília, v.12, n.1, jan.-abr. 2021, p. 59-78. Disponível em: <https://portalrevistas.ucb.br/index.php/EALR/article/view/11812>. Acesso em: 15 maio 2021.

RODRIGUES, Gustavo Alarcon; MARCHETTO, Patrícia Borba. Controle e vigilância na internet: técnica computacional como mecanismo de engendramento de poder. **Revista Eletrônica e Sociedade**, Canos, v.9, n.1, 2021, p.117-129. Disponível em: <https://revistas.unilasalle.edu.br/index.php/redes/article/view/6534>. Acesso em: 13 out. 2021.

ROHRMANN, Carlos Alberto. **Curso de Direito Virtual**. Belo Horizonte: Del Rey, 2005.

RONA, Gabor; AARONS, Lauren. State responsibility to respect, protect and fulfill human rights obligations in Cyberspace. **Journal of National Security Law and Policy**, Washington (EUA), v.8, 2016, p.1-35. Disponível em : https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2859615. Acesso em: 19 maio 2021.

ROSEN, Jeffrey. The deciders: the future of privacy and free speech in the age of Facebook and Google. **Fordham Law Review**, Nova York (EUA), v.80, n.4, 2012, p.1525-1538. Disponível em: <https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=4774&context=flr>. Acesso em: 09 abr. 2020.

ROTHBARD, Murray N. **O que é o livre mercado?**. Instituto Mises Brasil, 14.mar.2008. Disponível em: <https://www.mises.org.br/Article.aspx?id=52>. Acesso em: 20.fev.2021.

ROUSSEAU, Francis; SAUREL, Pierre. How should digital humanities pioneers manage their data privacy challenges ? In: IFIP WG 12.6 International Workshop, 2, 2014, Varsóvia.

Artificial Intelligence for knowledge management – Revised selected paper. Varsóvia (PO): Springer, 2014, p.75-91. Disponível em: <https://link.springer.com/book/10.1007/978-3-319-28868-0>. Acesso em: 15 jul.2021.

RUBINSTEINN, Gabriel. Cartórios já autenticaram 156 mil documentos com blockchain no Brasil. **Exame**. 30.Mar.2021. Disponível em: <https://exame.com/future-of-money/blockchain-e-dlts/cartorios-ja-autenticaram-156-mil-documentos-com-blockchain-no-brasil/>. Acesso em: 20 maio 2021.

SALEH, Fahad. Blockchain without waste: proof-of-stake. **The Review of Financial Studies**, Oxford (GB), v. 34, n.3, Mar.2021, p.1156-1190. Disponível em: <https://academic.oup.com/rfs/article/34/3/1156/5868423?login=true>. Acesso em: 15.jul.2021.

SÁNCHEZ-RÚBIO, David. Crítica a uma cultura estática e anestesiada de direitos humanos. **Culturas Jurídicas**, Rio de Janeiro, v. 4, n. 7, 2017, p.26-60. Disponível em: <https://periodicos.uff.br/culturasjuridicas/article/view/44855/28770>. Acesso em: 13 out. 2021.

SANTOS, Antonio Jeová dos. **Dano Moral na Internet**. São Paulo: Método, 2001.

SANTOS, Boaventura de Souza. Os Direitos Humanos na pós-modernidade. **Oficina do Centro de Estudos Sociais**, Coimbra, n.10, 1989, p.1-16. Disponível em: <https://www.ces.uc.pt/publicacoes/oficina/010/10.pdf>. Acesso em: 20 abr. 2020.

SANTOS, Milton. **A Natureza do Espaço: técnica e tempo, razão e emoção**. 4.ed. São Paulo: Edusp, 2004.

SAROIU, Stefan et al. A measurement study of peer-to-peer file sharing systems. In: SPIE-The International Society for Optical Engineering, 2002, [s.l.], **Proceedings** [...], [s.l.]: SPIE, 2002, p.82. Disponível em: <https://people.mpi-sws.org/~gummadi/papers/mmcn.pdf>. Acesso em: 13 maio 2020.

SASSON, Eli Bem et al. Zero Cash: decentralized anonymous payments from Bitcoin. In: IEE Symposium on Security and Privacy, 1, 2014, Piscataway (EUA). **Proceedings** [...], Piscataway: IEE, 2014, p.469-474. Disponível em: <https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6956581>. Acesso em: 20.jul.2020.

SCHMITT, Carl. **I tre tipi di pensiero giuridico**. Bologna (IT): Società Editrice Il Mulino, 1972.

SCHMITT, Carl. **Legality and Legitimacy**. Durham (EUA): Duke University Press, 2004.

SCHOLLMEIER, Rüdiger. A definition of Peer-to-Peer networking for the classification of Peer-to-Peer architectures and applications. In: INTERNATIONAL CONFERENCE ON PEER-TO-PEER COMPUTING, 1, 2001, Nova Jersey (EUA). **Papéis da Conferência** [...], Nova Jersey: IEEE, 2001, p. 101-102. Disponível em: https://www.it.lut.fi/wiki/lib/exe/fetch.php/courses/ct30a6900/p2p_definitions.pdf. Acesso em: 26 mar. 2021.

SCHWAB, Klaus. **A Quarta Revolução Industrial**. São Paulo: Edipro, 2016.

SCOTT, Brett. How can cryptocurrency and Blockchain technology play a role in building social and solidarity finance ? In: UNRISD Workshop Social and Solidarity Finance: Tensions, Opportunities and Transformative Potential, 1, 2016, Genebra (CH). **Working Papers**. Genebra: UNRISD, 2016, p.1-18. Disponível em [https://www.unrisd.org/unrisd/website/document.nsf/\(httpPublications\)/196aef663b617144c1257f550057887c?OpenDocument&Click=](https://www.unrisd.org/unrisd/website/document.nsf/(httpPublications)/196aef663b617144c1257f550057887c?OpenDocument&Click=). Acesso em: 13 maio 2020.

SEN, Amartya. **Desenvolvimento como liberdade**. São Paulo: Cia das Letras, 2000.

SHELTON, Dinah. Protecting human rights in a globalized world. **Boston College International and Comparative Law Review**, Boston (EUA), v. 25, n.2, 2002, p.273-322. Disponível em: <https://lawdigitalcommons.bc.edu/cgi/viewcontent.cgi?article=1172&context=iclr>. Acesso em: 13 out. 2021.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. São Paulo: Malheiros, 2005.

SILVEIRA, Renato de Mello Jorge. **Bitcoin e suas fronteiras penais**: em busca do marco penal das criptomoedas. Belo Horizonte: D'Plácido, 2018.

SIMSER, Jeffrey. Bitcoin and modern alchemy: in code we trust. **Journal of Financial Crime**, Bingley (GB), v. 22, n.2, 2015, p.156-169. Disponível em: <https://www.emerald.com/insight/content/doi/10.1108/JFC-11-2013-0067/full/html?skipTracking=true>. Acesso em: 30.abr.2021.

SKINNER, Burrhus Frederic. **Walden Two**. Indianapolis (EUA): Hacket Publishing, 2005.

SNOWDEN, Edward. **Eterna Vigilância**: como montei e desvendei o maior sistema de espionagem do mundo. São Paulo: Planeta do Brasil, 2019.

SOLOVE, Daniel J. **Nothing to hide**. New Haven (EUA): Yale University Press, 2011.

SOMMER, Joseph H. Against cyberlaw. **Berkeley Tech Law Journal**, Berkeley (EUA), v.15, 2000.

STALLINGS, Willian. **Criptografia e segurança de redes**: princípios e práticas. São Paulo: Pearson, 2008.

STIEGLER, Bernard. La Dictature des algorithmes: demais tous calculés? In: COMMISSION NATIONALE DE L'INFORMATIQUE ET DE LIBERTÉS. **Vie Privée à l'horizon 2020**: Parole d'experts. Paris: CNIL, 2020, p. 18-21. Disponível em: https://www.cnil.fr/sites/default/files/typo/document/CNIL-CAHIERS_IPn1.pdf. Acesso em: 03 maio 2021.

STIEGLER, Bernard. **La technique et le temps**. Paris: Galilée, 1996.

STRECK, Lenio Luiz. **Hermenêutica jurídica e(m) crise**: uma exploração hermenêutica da construção do direito. Porto Alegre: Livraria do Advogado, 2011.

SWAN, Melanie. **Blockchain: blueprint for a new economy**. Newton (EUA): O'Reilly Midia, 2015.

SZABO, Nick. **Bitgold**. Dez. 2005. Disponível em: <https://unenumerated.blogspot.com/2005/12/bit-gold.html>. Acesso em: 20.jun.2020.

TABORDA, Alini Bueno dos Santos. Direitos Humanos na sociedade tecnológica: informação, liberdade de expressão e segurança humana. In: Congresso Internacional de Direito e Contemporaneidade: Mídias e Direitos da Sociedade em Rede, 4, 2017, Santa Maria. **Anais [...]**. Santa Maria: UFSM, 2017, p.-1-11. Disponível em: <http://coral.ufsm.br/congressodireito/anais/2017/6-3.pdf>. Acesso em: 4 maio 2021.

TAPSCOTT, Don; TAPSCOTT, Alex. **Blockchain Revolution**. Nova York (EUA): Penguin Press, 2016.

THE LINUX FOUNDATION. **An introduction to Hyperledger**. 2018. Disponível em: https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductiontoHyperledger.pdf. Acesso em: 20 abr. 2020.

TIANJIAO, Yu; CHUNJIE, Cao. Privacy protection in Blockchain Systems: a review. In: CHUANCHAHO, Huang; YU-WEI, Chan (eds.). **Data processing techniques and applications for cyber-physical systems**. Cingapura (SIN): Springer, 2019, p. 2045-2052.

TRAMONTINA, Robison; CRUZ, Marco Aurélio Rodrigues da Cunha e. Sociedade da Informação, Cyberlaw e o conceito kantiano de autonomia na dogmática constitucional brasileira. **Revista Brasileira de Direito**, Passo Fundo, vo.15, n.3, p.158-179, Set./Dez. 2019. Disponível em: <https://doi.org/10.18256/2238-0604.2019.v15i3.3721>. Acesso em: 09 maio 2021.

TSÉ-TUNG, Mao. **On Guerrilla Warfare**. Washington (EUA): Department of the Navy, 1989.

UE. **Carta dos Direitos Fundamentais da União Europeia**, de 18 dez. 2000. Strassbourg (FR): Parlamento Europeu, 2000. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 20 jul. 2020.

UE. **General Data Protection Regulation (GDPR)**, de 25 maio 2016. Strasbourg (FR): Parlamento Europeu, 2016. Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>. Acesso em: 5 jul. 2021.

UHDRE, Dayana de Carvalho. **Blockchain, tokens e criptomoedas: Análise jurídica**. São Paulo: Almedina, 2021.

VANDERBURG, Willen H. Técnica, dessimbolização e o papel do direito. In: BARRIENTOS-PARRA, Jorge David; MATOS, Marcus Vinicius A. B. de. **Direito, Técnica, Imagem: os limites e os fundamentos do humano**. São Paulo: Cultura Acadêmica, 2013.

VARGAS, Milton. **Para uma filosofia da tecnologia**. São Paulo: Alfa - Ômega, 1994.

VECHAIN FOUNDATION. **Vechain Whitepaper 2.0**. 2015. Disponível em: https://www.vechain.org/whitepaper/#bit_zxhvz. Acesso em: 08 abr. 2020.

VEIT, Meredith. **Blockchain and Journalism**: intersection between blockchain-based technology and freedom of the press. Tese (European Master's Degree in Human Rights and Democratization) - Universidade de Coimbra, p.78, Coimbra (PT). 2019. Disponível em: <https://repository.gchumanrights.org/bitstream/handle/20.500.11825/1147/Veit.pdf?sequence=1&isAllowed=y>. Acesso em: 20 maio 2020.

VIANNA, Túlio Lima. **Transparência pública, opacidade privada**: o direito como instrumento de limitação do poder na sociedade de controle. Tese (Doutorado em Direito)- Universidade Federal do Paraná, p. 206, Curitiba. 2006. Disponível em: <https://acervodigital.ufpr.br/bitstream/handle/1884/5281/VIANNA,%20T%FAlio%20Lima%20-%20Tese%20doutorado%20em%20Direito%20UFPR.pdf;jsessionid=A81114F2F7A506B04C4DE9FD9631B549?sequence=1>. Acesso em: 15 maio 2021.

VOEGELIN, Eric. **Science, Politics and Gnosticism**. Southlake: Gateway Editions, 2012.

WACKS, Raymond. **Personal information**: privacy and the law. Oxford (GB): CLarendon Press, 1989.

WARREN, Samuel D; BRANDEIS, Louis D. The Right to Privacy. **Harvard Law Review**, Cambridge (EUA), v.4, n.5, 15. dez. 1890, p.193-22. Disponível em: <https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf>. Acesso em: 08 abr. 2019.

WEBER, Max. **Economia e Sociedade**: fundamentos da sociologia compreensiva. 4.ed. Brasília: UNB, 2009.

WEITZENBOECK, Emily. [...] and still we are left wanting: Malta's white paper on digital human rights. **Computer Law and Security Review**, Londres (GB), v.29, n.3, 2013, p.293-295. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0267364913000642>. Acesso em: 13 out. 2021.

WHITHMAN, James Q. The two western cultures of privacy: dignity versus liberty. **The Yale Law Journal**, New Haven (EUA), v.113, 2004, p.1153-1221. Disponível em: https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1647&context=fss_papers. Acesso em: 20 maio 2021.

WINNER, Langdon. **The whale and the reactor: a search for limits in na age of high technology**. Chicago (EUA): Chicago University Press, 1986.

YAGODA, Ben. **A short history of Hack**. The New Yorker, 6.mar.2014. Disponível em: <https://www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack>. Acesso em: 14 maio 2021.

YEN, Alfred Chueh-Chin. Western Frontier or Feudal Society? Metaphors and Perceptions in Cyberspace. **Berkeley Technology Law Journal**, Berkeley (EUA), v. 17, 2002, p.1207-1263.

YERMACK, David. Is Bitcoin a real currency? In: LEE, David Kuo Chuen. (ed.). **The handbook of digital currency**. Cambridge (EUA): Academic Press, 2015

YEUNG, Karen. Algorithmic regulation: A critical interrogation. **Regulation and Governance**, Brisbane(AU), v. 12, n.4, dez. 2018, p.505-523. Disponível em: <https://onlinelibrary.wiley.com/doi/full/10.1111/rego.12158>. Acesso em: 07 abr. 2021.

YEUNG, Karen. **Blockchain, transactional security and the promise of automated law enforcement**: the withering of freedom under the law ?. Londres (GB): King's College of London, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929266. Acesso em: 16 abr. 2020.

YEUNG, Karen; DIXON-WOODS, Mary. Design-based regulation and patient safety: a regulatory studies perspective. **Social Science and Medicine**, Oxford (UK), v. 71, n. 3, ago. 2010, p.502-509. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0277953610003473?via%3Dihub>. Acesso em: 07 abr. 2021.

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. **Revista de Doutrina da 4ª Região**, Porto Alegre, n.64, fev. 2015. Disponível em: https://revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html. Acesso em: 04 ago. 2020.

ZIEGELDORF, Jan Henrik et al. Secure and anonymous decentralized Bitcoin mixing. **Future Generation Computer Systems**, Amsterdã (NL), v. 80, Mar. 2018, p.448-466. Disponível em: <https://www.sciencedirect.com/science/article/abs/pii/S0167739X16301297?via%3Dihub>. Acesso em: 15 maio 2020.

ZIMMERMAN, E. **Confronte de Heidegger com a modernidade: tecnologia, política e arte**. Lisboa: Instituto Piaget, 1990.

ZUBOFF, Shoshana. **The age of surveillance capitalism**: the fight for a human future at the new frontier of power. Nova York (EUA): Public Affairs, 2019.

ZYSKIND, Guy. Decentralizing privacy: using blockchain to protect personal data. In: IEEE CS Security and Privacy Workshops,36, 2015, San Jose (EUA). **Proceedings** [...] San Jose (EUA): IEEE, 2015, p.180-184. Disponível em: <https://ieeexplore.ieee.org/document/7163223>. Acesso em: 20.abr. 2020.