UNIVERSIDADE DE BRASÍLIA
Faculdade de Direito
Programa de Pós-Graduação em Direito

"*Fazer do Reino Unido o lugar mais seguro do mundo para estar on-line*": uma análise crítica do *Online Safety Act* como ferramenta de moderação de conteúdo no espaço britânico.

Júlia Gomes Mota

Brasília
2024

UNIVERSIDADE DE BRASÍLIA
Faculdade de Direito
Programa de Pós-Graduação em Direito

Júlia Gomes Mota

"*Fazer do Reino Unido o lugar mais seguro do mundo para estar on-line*": uma análise crítica do *Online Safety Act* como ferramenta de moderação de conteúdo no espaço britânico.

Dissertação apresentada como requisito parcial à obtenção do grau de Mestre no Programa de Pós-Graduação da Faculdade de Direito da Universidade de Brasília, linha de pesquisa "Transformações na Ordem Social e Econômica e Regulação", sob a orientação do Professor Alexandre Kehrig Veronese Aguiar.

Brasília

2024

[Referências para catalogação]

Júlia Gomes Mota

"*Fazer do Reino Unido o lugar mais seguro do mundo para estar on-line*": uma análise crítica do *Online Safety Act* como ferramenta de moderação de conteúdo no espaço britânico.

Apresentada à banca examinadora em 7 de março de 2024.

BANCA EXAMINADORA

Professor Dr. Alexandre Kehrig Veronese Aguiar
(Presidente – Orientador – FD/UnB)

Professor Dr. Márcio Iorio Aranha
(Examinador interno – FD/UnB)

Professor Dr. Murilo César Ramos
(Examinador interno – FC/UnB)

Professora Dra. Laura Schertel Ferreira Mendes
(Examinadora interna – FD/UnB)

Professora Dra. Yasmin Curzi de Mendonça
(Examinadora externa – FGV Rio)

Agradecimentos

Atravessado por uma pandemia, por duas mudanças de continente e pela chegada de minha filha, a escrita desse trabalho deve agradecimentos a uma extensa rede de apoio. Desde o âmbito institucional da Universidade de Brasília até o núcleo de minha família, todos os sujeitos que estiveram comigo ao longo dessa caminhada guardam seu quinhão no meu reconhecimento de que, sozinha, a conclusão desse mestrado não teria ocorrido do modo tranquilo – ou quase tranquilo – como ocorreu.

Primeiramente, registro aqui meu agradecimento à Universidade de Brasília, pública, produtiva, pulsante e acolhedora. Ainda hoje lembro o sentimento de satisfação que foi ler meu nome entre os aprovados para a seleção de mestrado. Ter em minha trajetória profissional o selo de uma instituição como a UnB é uma honra que carregarei, com orgulho, até o fim. Agradeço ao Programa de Pós-Graduação em Direito e a sua maravilhosa equipe. Desde o ensino remoto até a licença-maternidade, não houve um e-mail, uma pergunta, uma única dúvida que não tenha sido prontamente atendida por seus funcionários, cujo trabalho merece ser repetidas vezes exaltado. Agradeço, também, à Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e à Fundação de Apoio à Pesquisa (FUNAPE), financiadoras de meu trabalho nessa dissertação e junto ao Grupo de Pesquisa DR.IA UnB. Ainda no âmbito institucional, mas já a adentrar a esfera dos afetos, agradeço a meu orientador, Professor Alexandre Kehrig Veronese Aguiar, pela prontidão ao atender minhas dúvidas e por ter apostado em mim, aluna forasteira e virtual surgida em meio a uma emergência sanitária.

Meus mais especiais agradecimentos vão, como não poderia deixar de ser, a minha família. Sou grata aos meus pais, Paulo e Valquíria, que sempre me apoiaram diante de qualquer projeto a que eu tenha me lançado. Sou grata aos meus sogros, César, Liliana e Marijane, pela acolhida e pela extensão do que chamo de família, especialmente ao longo dos duros anos que foram essa pandemia. Meu obrigada, como não poderia deixar de ser, se estende às minhas irmãs, Lígia e Alice, sem as quais minha alegria nunca seria completa. Um agradecimento especial deve ser feito à minha irmã Lígia, pelo carinho e pela paciência de ler e reler esta dissertação. A dívida por *aquele* trabalho sobre tecido ósseo que fiz para ela durante o Ensino Médio não poderia estar mais quitada do que está.

Agradeço, por fim, a minha filha e ao meu marido, Teresa e Caetano, cerne de tudo. À Teresa, sou grata pela sua vida e por toda força que ela trouxe consigo. Maternidade e academia não são grandezas fáceis de conciliar. Muito embora o PPGD, a CAPES, minha família e meu orientador tenham a todo tempo me dado o suporte necessário para levar a pesquisa e o maternar adiante, ser mãe e acadêmica segue sendo desafiador. A chegada de Teresa e a conclusão deste trabalho despontam, para mim, como a certeza de que a combinação de maternidade e carreira não apenas é necessária, como é possível. Ao Caetano, meu par e meu amor, sou grata por toda a inspiração e por nossa amizade. Sou uma pessoa melhor ao lado de Caetano, e tenho certeza de que esse trabalho é um pouco melhor, também, pela simples razão de ter sido escrito na sua companhia.

Resumo

Este trabalho tem por enfoque a análise da nova regulação britânica para moderação de conteúdo na internet, o *Online Safety Act* 2023 (OSA). Para fins de melhor compreender as opções regulatórias adotadas no OSA, são também analisados o histórico regulatório da internet no Reino Unido, a estratégia de liderança global em segurança *online* britânica (*Global Britain in a Competitive Age*) e o papel do Brexit na elaboração do OSA. O escopo da análise não se volta a julgar o potencial de sucesso do novo aparato regulatório. Objetiva-se, isso sim, o estudo crítico do OSA como ferramenta política do governo britânico para fins de retomada de sua soberania no ciberespaço. Trata-se de pesquisa qualitativa, realizada no âmbito do Programa de Pós-Graduação em Direito da Universidade de Brasília, junto à linha Transformações na Ordem Social e Econômica e Regulação, sublinha Regulação Social e Políticas Públicas de Educação, Ciência, Tecnologia e Inovação. O trabalho realizado tem vinculação ao Centro de Excelência Jean Monnet em Cidadania Digital e Sustentabilidade Tecnológica. Na pesquisa empreendida, parte-se do pressuposto de que o OSA representa reação do Estado racional ante a sua perda de poder sobre espaços de interesse público na internet. Em vista disso, a nova lei surge como mudança de paradigma regulatório estatal, permitindo à Administração britânica uma maior ingerência sobre a agência de atores transnacionais por meio de regulação indireta, sanções pecuniárias de peso e afastamento da jurisdição das Cortes de Justiça. Tratando-se de lei extensa, a qual não poderia ser explorada em sua totalidade no espaço de uma dissertação, são aqui trabalhados os deveres de cuidado, os deveres de transparência, os poderes atribuídos à autoridade reguladora (o OFCOM) e a possibilidade de responsabilização de plataformas em decorrência de conteúdos ilegais ou nocivos veiculados por intermédio de suas redes. É por meio desses aparatos que as características próprias do OSA são exploradas, revelando sua abordagem sistêmica, sua aproximação com o Direito Administrativo e seu teor voltado a encarar o ciberespaço como espaço público por excelência. Os aportes teóricos de Lawrence Lessig, Evelyn Douek, Paul Schiff Berman, Mike Feintuck e Vili Lehdonvirta acompanham, a todo tempo, a análise crítica aqui proposta.

Palavras-chave: *Online Safety Act*; Reino Unido; moderação de conteúdo; Estado racional; regulação da internet; abordagem sistêmica; responsabilização de agentes intermediários.

Abstract

This work aims to analyze the UK's new regulation of internet content moderation, the Online Safety Act 2023 (OSA). To better understand the regulatory choices adopted in the OSA, an analysis of the history of internet regulation in the UK, its strategy of global leadership in online safety (Global Britain in a Competitive Age) and the role of Brexit in the elaboration of the OSA are also undertaken. The scope of the analysis does not seek to assess the new regulation's potential for success. Instead, it proposes a critical study of the OSA as a political tool of the British government in its aim of reclaiming sovereignty in cyberspace. This is a work of qualitative research, conducted within the Graduate Program in Law of the University of Brasília as part of the research line entitled 'Transformations in Social and Economic Order and Regulation', specialism 'Social Regulation and Public Policies in Education, Science, Technology, and Innovation'. It is associated with the Jean Monnet Excellency Center in Digital Citizenship and Technological Sustainability. The research departs from the premise that the OSA represents a reaction by the rational State against its loss of power over public interest space. Within such context, the new law emerges as a change of paradigm in state regulation, allowing British Administration a greater command over the agency of transnational players through indirect regulation, onerous pecuniary sanctions, and a withdrawal from Court jurisdictions. Given that its extensive dimensions prevent its full exploration in the space of this dissertation, I focus on the duties of care, duties of transparency, the powers afforded to the regulatory authority (the OFCOM), and the possibility of platform accountability in the case of illegal or harmful content circulation. The specific characteristics of the OSA are hence explored through such framework, revealing its systemic approach, its proximity with Administrative Law, and its central tenet of facing cyberspace eminently as a public space. The theoretical contributions of Lawrence Lessig, Evelyn Douek, Paul Schiff Berman, Mike Feintuck, and Vili Lehdonvirta support the entirety of the critical analysis hereby advanced.

Keywords: Online Safety Act; United Kingdom; content moderation; the rational State; internet regulation; systemic approach; intermediate agent accountability.

Lista de Abreviaturas

AEDPA - Antiterrorism and Effective Death Penalty Act of 1996.

BBFC – British Board of Film Classification.

CA 2003 – Communications Act 2003.

CAESI - Conteúdo abusivo e de exploração sexual infantil.

CDA - Communications Decency Act.

CMA - Competition and Markets Authority.

DCMS – Department for Digital Culture, Media and Sport.

DEA 2010 – Digital Economy Act 2010.

DEA 2017 – Digital Economy Act 2017.

DOSB – Draft Online Safety Bill.

DRCF – Digital Regulation Cooperation Forum.

EFF – Electronic Frontier Foundation.

FCA - Financial Conduct Authority.

FEM - Fórum Econômico Mundial.

FTC – Federal Trade Commission.

GBCA - Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy.

HSWA - Health and Safety at Work Act 1974.

ICO – Information Communication's Office.

ISS – Internet Safety Strategy.

ISSGP - Internet Safety Strategy Green Paper.

LMD – Lei dos Mercados Digitais.

NetzDG – Netzwerkdurchsetzungsgesetz.

NCA – National Crime Agency.

OCDE - Organização para Cooperação e Desenvolvimento Econômico.

OHWP – Online Harms White Paper.

OSA – Online Safety Act.

OSB – Online Safety Bill.

TAR – Teoria do Ator-Rede.

Sumário

1. Introdução.

É com crescente frequência que presenciamos, mundo afora, embates entre atores transnacionais do mercado de mídias digitais e agentes representantes do Poder Público. O banimento do TikTok do estado de Montana, nos EUA, é exemplo de tal dinâmica (Delouya, 2023). A acusação do governo alemão de que o Twitter não remove desinformações ilegais, desafiando o determinado em lei naquele país (Lomas, 2023), é outro caso a ilustrar o fenômeno. Também o é a suposta divulgação de conteúdo contra o Projeto de Lei 2630/2020 (PL 2630/2020) pelo *Google* e pelo *WhatsApp* no Brasil (Brasil, STF, 2023), juntamente com a reação dos Poderes Judiciário e Legislativo à ofensiva das *bigtechs* ante o PL que regula suas atividades no país (Marques, 2023) (Brasil, MPF, 2023) (Siqueira, 2023). No cenário britânico, recorte espacial do trabalho que aqui se introduz, não é diferente. Suspeitas de interferência externa na votação do *Brexit* 2016, a partir de dados coletados e manipulados por empresas de tecnologia, somadas à moção coletiva de se desvencilhar do espaço europeu e recobrar a "soberania" do Reino Unido (Schelesinger, 2022), acabaram por culminar na promulgação do *Online Safety Act* 2023 (OSA). Em termos muito enxutos, o OSA consiste na resposta legal do governo ao crescente ganho de influência de plataformas de serviços de internet na sociedade britânica. As contendas comentadas, via de regra, se dão entre agentes públicos e privados, representando disputas por espaços de poder. Nesse cenário, os atores envolvidos concorrem por ditar de que modo serão tratadas matérias como controle de dados, o tratamento dispensado a questões de privacidade, moderação de conteúdo, liberdade de expressão, direitos de autoria, propriedade intelectual, ou temas relacionados ao direito da concorrência. Em todos os casos os debates estão relacionados ao fluxo de dados nas redes, com repercussões que têm assumido dimensões cada vez maiores na ordem mundial multipolar.

À medida que empresas prestadoras de serviços *online* ganham espaço nos cotidianos de cidadãos das mais diversas nações, aumenta também o poder dessas para influenciar e tomar decisões sobre as ações dos sujeitos no ciberespaço. Isso, em diversos pontos, entra em rota de colisão com atividades próprias da Administração Pública. Fosse o embate apenas em razão do poderio das *bigtechs* sobre as atividades econômicas por elas exploradas, é possível que a questão se resolvesse no âmbito da regulação de mercados. No entanto, as searas da vida social abarcadas pelo ciberespaço são cada vez mais numerosas e complexas, de modo que a paleta de atividades que compõem o fluxo de informações e capitais

online extrapola a mera concorrência. Adentra-se, cada vez com maior profundidade, questões morais, democráticas, de saúde e de direitos fundamentais. Atividades de socialização, comércio, relacionamentos interpessoais, campanhas políticas, mídia, educação, difusão de conhecimento, entre outras tantas, foram e seguem sendo transportadas para as redes. O fato de tais relações serem travadas por meio de plataformas fornecidas quase em sua totalidade por agentes privados transnacionais, sobre os quais os Estados nacionais pouca ingerência têm, torna a distribuição de poder no ciberespaço especialmente complexa. É em vista de tal cenário que são desvelados os traços iminentemente políticos das disputas em comento.

As relações sociais no ciberespaço e a crescente importância da qual gozam fazem com que as instâncias do mundo virtual assumam, de forma cada vez mais nítida, características próprias de espaço público. Como consequência, muitos dos serviços prestados por *bigtechs* acabam por fazer jus a tratamento de matéria de interesse público. A fim de ilustrar a relevância das facilidades oferecidas por plataformas ao redor do mundo, basta realizar um pequeno exercício de imaginação: como seria sua rotina se, ao acordar pela manhã, sua conta *Google* não estivesse disponível? Se o *WhatsApp* estivesse fora do ar? Se, ao viajar, o *AirBnb* suspendesse seu catálogo de acomodações? Se as ferramentas de busca *online* hoje disponíveis fossem, da noite para o dia, eliminadas? Por certo, o desempenho de atividades cotidianas estaria comprometido, isso pois a popularização de tais instrumentos veio acompanhada de uma crescente dependência dos produtos por eles ofertados, em tal medida que sua ausência súbita impactaria atividades econômicas em larga escala. Esse fato, não há como negar, é assunto de interesse estatal. Como consequência de tal processo é que surgiram as dissenções entre governos tradicionais e atores privados ora mencionadas. Indo mais a fundo, é em decorrência da popularização dos espaços virtuais que as decisões tomadas a nível administrativo por dirigentes de plataformas acabam por afetar discursos públicos e debates democráticos em escala massiva também no mundo *real*, deslocando eixos de poder e inspirando reações regulatórias da parte dos Estados. O PL2630/2020 no Brasil, popularmente conhecido como PL das *Fake News* (Brasil, Câmara dos Deputados, 2023), é exemplo disso. Também o são o Regulamento dos Mercado Digitais (RMD), da União Europeia, e o *Netzwerkdurchsetzungsgesetz* (NetzDG), da Alemanha. Esses para enumerar apenas alguns exemplos de moderação de conteúdo no Ocidente. Para além das respostas formais, é importante observar que, mesmo ante a inexistência de leis estrito senso para regular a atuação desses agentes transnacionais, existe uma expectativa social de que *bigtechs* respeitem preceitos basilares do Estado de Direito (Douek, 2022), o que cimenta a constatação de que os

usos e o controle a serem desenvolvidos no ciberespaço consistem em assunto de interesse da coletividade. A profusão de relações de comércio e de socialização *online* permite afirmar que foram erigidas verdadeiras cidades virtuais no ciberespaço, em tal medida que é fácil traçar paralelos entre a conformação das cidades comerciais no passado, gérmen do processo de centralização e racionalização do Estado moderno, e a ascensão das cidades virtuais do presente - metáfora que será evocada diferentes vezes ao fio deste trabalho.

É a partir da expectativa coletiva de que critérios elementares de Direito Público, regularidade procedimental e não arbitrariedade sejam observados no trato dispensado ao fluxo de dados *online,* que é proposto, aqui, refletir sobre a moderação de conteúdo como matéria de interesse público, indispensável para o funcionamento salutar do Estado moderno democrático (Feintuck, 2010). Para isso, pensa-se, a todo tempo, as relações entre agentes privados e a reação do Estado tradicional frente a tal fenômeno. De início, é fundamental fazer constar que, ao se tratar apenas de matéria de moderação de conteúdo, opta-se por recorte muito pontual do conjunto de temas pertinentes ao controle de fluxo de dados no ciberespaço - o qual engloba gradação bastante mais matizada de matérias atinentes às trocas realizadas no mundo virtual. Para empreender a dissertação proposta, trataremos de estudo de caso do modelo regulatório britânico para moderação de conteúdo *online*. Sob o lema de "fazer do Reino Unido o local mais seguro do mundo para estar *online*" (Reino Unido, 2019), o Parlamento vem trabalhando ativamente, desde 2021, em extenso projeto de lei que visa a controlar e a suprimir conteúdos danosos circulantes em redes sociais, serviços de mensageria e ferramentas de busca utilizadas naquela jurisdição. Como produto desse processo legislativo, surgiu a *Online Safety Bill* (OSB), debatida em Westminster ao fio dos últimos anos e recentemente convertida em lei, em 26 de outubro de 2023, quando passou a ser denominada *Online Safety Act*.

Tratando-se de lei extensa, não é pretensão deste trabalho cobrir a totalidade dos dispositivos do OSA, mas sim utilizá-lo como exemplo concreto do embate político em comento, avaliando a factibilidade e as estratégias adotadas pelo governo britânico. O que se propõe aqui, desse modo, consiste em pesquisa qualitativa e crítica, realizada no âmbito do Programa de Pós-Graduação em Direito da Universidade de Brasília, junto à linha "Transformações na Ordem Social e Econômica e Regulação", sublinha "Regulação Social e Políticas Públicas de Educação, Ciência, Tecnologia e Inovação". Importante anotar, neste ponto, que o trabalho proposto também tem vinculação com o Centro de Excelência Jean Monnet em Cidadania Digital e Sustentabilidade Tecnológica, e seus capítulos estão estruturados conforme a exposição que segue.

O capítulo 2, onde estão expostos os marcos teóricos que respaldam a reflexão aqui proposta, está alicerçado sobre quatro pilastras principais, todas correlacionadas entre si ao longo do texto. [1] De início, apresenta-se uma revisão bibliográfica da literatura que discute a regulabilidade da internet. Nesse ponto, explora-se que a existência de fatores condicionadores do comportamento é indissociável da estrutura do ciberespaço, buscando com isso demonstrar que a regulação da internet não é uma opção, e sim uma realidade. A julgar pelas características próprias do ciberespaço e as relações entre moderação de conteúdo e liberdade de expressão, serão trabalhados os motivos que fazem preferível tratar o controle dos discursos *online* desde o viés administrativo, deixando de lado a primazia das cortes e do sistema judiciário para lidar com o tema. Nesse ponto, o trabalho se valerá fortemente das obras de Lawrence Lessig (1996, 1997, 1999 e 2006), Andrew Murray (2015) e Cass Sunstein (2017). [2] O segundo ponto de relevância deriva de seu antecessor. Ele se debruça a liberdade de expressão e o uso de ferramentas administrativas para garantir o direito à livre manifestação das ideias também no ciberespaço. Na ocasião, serão repisados argumentos a literatura acadêmica mais recente que defendem a implementação de sistema de controle de conteúdo de arquitetura preventiva, em formato *ex ante*, admitindo eventuais falhas em nome de estrutura mais abrangente e democrática, na qual plataformas estariam legalmente obrigadas a observar critérios básicos fixados pelo Poder Público. Como apoio principal a esse argumento será utilizado, sobretudo, o trabalho de Evelyn Douek (2022). [3] Ante a ambiguidade do ciberespaço como ambiente disponibilizado por atores privados e que, com o passar do tempo, revestiu-se de aspectos de espaço público, será também examinado o oxímoro existente entre Direito Público e Direito Privado, aplicando-o ao mundo virtual. Pretende-se ilustrar, por meio disso, os limites turvos entre elementos pertinentes ao público e ao privado nos espaços disponibilizados em plataformas *online*, especialmente em vista do ganho de importância desses locais para a organização social hodierna. Para levar a cabo essa reflexão, serão utilizados os autores acima mencionados e, em especial, o trabalho de Paul Shiff Berman (2000). [4] No último pilar teórico trabalhado no capítulo 2, retira-se o enfoque da ação regulatória estatal e se volta o olhar exclusivamente para a agência das *bigtechs* na atualidade. Com base na obra de Vili Lehdonvirta (2022), será explorado o comportamento institucional das empresas proprietárias de plataformas *online*, as quais crescentemente emulam mecanismos próprios do Estado moderno nacional para organizar seus espaços internos. Como consequência de tal movimento empresarial, provedores de serviços de redes sociais, mensageria e ferramentas de busca – os mesmos ora regulados pelo OSA – acabaram por destravar movimento que abocanha poder e influência próprios do Estado, porém no ciberespaço. Essa análise é particularmente profícua

para pensar o novo projeto regulatório britânico como reação do poder estatal, que busca recobrar sua influência sobre espaços de relevância para a coletividade.

O capítulo 3 é aquele que, dentre todos os demais, possui mais fino teor de retrospecto histórico e estudo de caso propriamente ditos. Inicia-se por explorar cronologicamente o percorrido legal britânico para regulação de mídias digitais. No curso dessa tarefa, serão esmiuçadas particularidades do *Communications Act* de 2003 do Reino Unido (CA 2003), onde pela primeira vez mídias digitais foram classificadas como redes públicas de comunicação eletrônica, sem, contudo, admitir seu caráter de essencialidade para a segurança da democracia (Feintuck e Varney, 2006). É também analisado projeto de política pública intitulado *Digital Britain Report*, seguido de seu produto legal, o *Digital Economy Act* de 2010 (DMA 2010), no qual foram consolidadas as primeiras regras formais para regular atividades humanas no ciberespaço, voltadas sobretudo à proteção a direitos de autoria e de propriedade intelectual. Na sequência, será abordado o *Digital Economy Act* 2017 (DMA 2017), quando regras de compartilhamento de dados e proteção a usuários crianças foram criadas e, após sucessivos fracassos, postas de lado. O malogro do DMA 2017 coincidiu com nova política regulatória do ciberespaço no Reino Unido, mais ousada e abrangente que a anterior, e a qual, para fins de moderação de conteúdo, resultou no OSA (o projeto de Westminster prevê a criação de outros corpos regulatórios para outras searas do fluxo de dados *online,* como questões de concorrência, privacidade, e direitos de consumo nas redes).

Também no capítulo 3, para esmiuçar o texto do OSA, extenso e denso por sua natureza, escolheu-se trabalhar alguns aspectos pontuais da nova lei com maior profundidade, ressaltando outros pontos apenas a título de menção. Julgou-se que essa abordagem será suficiente para embasar a proposta de análise crítica aqui empreendida, evidenciando as dissenções entre Estados e *bigtechs* como embates políticos e de poder. Serão analisados, desse modo, os deveres de cuidado e alguns outros deveres especiais impostos a provedores de serviços de internet regulados pela lei, detalhando quais deveres e tratamentos serão dispensados às diferentes categorias de plataformas – isso pois o OSA separa provedores em nichos apartados, a depender de seu tamanho e serviço oferecido, conferindo tratamento diferenciado a cada grupo. Serão analisados também os deveres de transparência, de identificação de usuários, o tratamento especial a usuários crianças e os deveres de pagar taxas. Esses últimos pontos representam trechos de grande relevância do OSA para esse trabalho, uma vez que a exigência de maior transparência e prestação de contas de plataformas está diretamente relacionada com a capacidade do governo de controlar o fiel cumprimento dos

deveres de cuidado exigidos dos agentes privados pela nova lei. Por fim, serão esmiuçados os poderes atribuídos ao *Office of Communications* (OFCOM), autoridade reguladora incumbida da formalização, execução, e fiscalização das determinações contidas no OSA. O alargamento dos poderes do órgão regulador é fundamental para compreender a envergadura da ação empreendida pelo governo britânico com o OSA, o abandono parcial do modelo atual de autorregulação, bem como seu caráter administrativo e sistêmico. Apenas a título de menção, a partir da vigência da lei, o OFCOM estará capacitado a realizar ações como: responsabilizar plataformas por conteúdos de terceiros, requerer informações protegidas por criptografia de ponta a ponta, encaminhar casos à apreciação do Judiciário, definir códigos de boas práticas a serem seguidos pelos atores regulados, promover buscas e investigações nas sedes de empresas sitas no Reino Unido, dentre outras atribuições.

No capítulo 4, em desfecho ao apanhado teórico e ao estudo de caso que o antecedem, será empreendida a análise dos atributos do OSA sob a luz da literatura comentada no capítulo 2. Com isso, se buscará dar robustez ao entendimento de que o projeto regulatório britânico consiste, por essência, em reação estatal ante a nova ordem mundial digital. Para alcançar esse fim, julgou-se suficiente focar em três aspectos pontuais, os quais podem ser correlacionados entre si a qualquer tempo. [1] Por primeiro, serão analisados os deveres de cuidado impostos aos atores regulados e o empoderamento do OFCOM como autoridade reguladora, pontos por meio dos quais será explorada a opção do governo britânico de tratar o problema do controle de conteúdo desde o viés administrativo e sistêmico, abandonando o modelo de autorregulação e de controle de conteúdo *ex post*, ora vigente no Reino Unido. [2] Em um segundo subcapítulo, serão trabalhadas as determinações do OSA voltadas a exigir maior transparência das plataformas reguladas, por intermédio da prestação periódica de avaliação de risco e informações requeridas pela autoridade reguladora. A partir das ferramentas legais comentadas, será explicitado como o governo britânico, com a vigência do OSA, deve passar a dispensar tratamento de espaço público ao ciberespaço, resgatando sua ingerência sobre atividades dos cidadãos ora transferidas ao mundo digital por meio do acesso a dados que, até então, estavam concentrados junto a agentes transnacionais privados. É também nesse ponto que será discutido o oxímoro Direito Público *versus* Direito Privado aplicado ao caso concreto da nova lei britânica. [3] Por fim, no último subcapítulo será abordada a possibilidade de responsabilização dos atores regulados pelo OSA, vinculando essa opção do Parlamento à reação estatal que visa recobrar poder sobre o ciberespaço através de ferramentas clássicas do Estado racional coator – no caso, o poder de punição e de violência

legítima. É nesse último ponto que será discutida a adoção, pelas *bigtechs*, de mecanismos de ordenação clássicos do Estado moderno, aqueles mesmos apontados na obra de Vili Lehdonvirta (2022). Ao esmiuçar essa dinâmica enovelada – onde agentes privados emulam o comportamento estatal e Estados se valem de legitimidade e força de lei para manter a soberania -, esse trabalho se esforça por desvelar ao leitor as finalidades políticas do OSA como mecanismo de *hard power,* bem como seu viés realista.

Como encerramento, optou-se por não apenas retomar os pontos explorados ao longo do texto. A escolha foi por aportar ponderações novas, em conclusão às observações produzidas nos capítulos anteriores. Hão de ser comentados, neste ponto, tópicos relativos à regulação indireta proposta pelo OSA; seu teor voltado ao interesse público e a estender garantias cidadãs ao ciberespaço; as vantagens e desvantagens da textura preponderantemente aberta da nova lei britânica; e o tratamento administrativo que se passa a dar à liberdade de expressão *online* naquela jurisdição. A metáfora que vincula a ascensão do poder das *bigtechs,* mediante emulação de comportamentos estatais, ao surgimento do Estado moderno é novamente retomada e comentada. Por fim, as considerações empreendidas nessa seção, não obstante venham sob cabeçalho onde se lê "conclusão", não devem se encerrar em si mesmas. Elas têm o intuito de expandir os estudos sobre o produto regulador que é o OSA e o momento que vivemos a nível mundial, deixando portas abertas para a continuidade das reflexões aqui entabuladas.

2. Regulabilidade da internet, liberdade de expressão e comportamento político-administrativo de provedores transnacionais de serviços de internet: análise teórica.

2.1 Moderação de conteúdo e crise da democracia: a analogia entre o ciberespaço e as cidades modernas.

O livro “Morte e Vida das Grandes Cidades Norte-Americanas”, publicado por Jane Jacobs em 1961, foi uma das inspirações de Cass Sunstein ao escrever sobre os riscos à democracia advindos do isolamento comunicacional, ocasionados pela digitalização em massa da vida em sociedade (Sunstein, 2017). Embora não se trate de obra voltada ao ramo jurídico - longe disso, o livro de Jacobs é uma crítica às políticas de planejamento urbano da década de 1950 nos Estados Unidos -, a centelha de Sunstein é analogia de fácil explicação. Ao passo em que Jacobs descreve as grandes cidades, ela permite entrever, a todo tempo, que se tratava de lugares de trocas entre pessoas de diferentes classes e ideologias. Muito embora não fosse possível diluir essas diferenças, os cidadãos, ocupantes desses espaços em comum, logo chegavam a termos e se familiarizavam com a estranheza alheia. Essa relação, pautada pela ciência da coletividade da cidade, poderia perdurar ao longo de muito tempo e era extremamente enriquecedora para quem dela partilhava (Sunstein, 2017, p. 12).

A analogia escolhida por Sunstein não poderia ser mais acertada. "O ar da cidade liberta", máxima comumente inscrita sobre os portões das cidades helvéticas medievais, consolidou-se como lema do potencial dos centros urbanos para criar, comercializar, pluralizar e permitir que os sujeitos quebrassem com o estamento social típico do período feudal (Barros, 2011, p. 102). De tal forma que é confortável afirmar, como fez Sunstein (2017), que, não fossem essas trocas, as democracias modernas não teriam podido se desenvolver da forma como o fizeram. As trocas individuais e coletivas possibilitadas pela ascensão das cidades comerciais, de forma sucinta, estão na gênese do Estado Moderno racional. Elas representam peça chave no desenvolvimento e consolidação do pensamento liberal que, ainda hoje, pauta os ideais ocidentais, e estão vigentes a todo tempo quando se imagina o ciberespaço como ambiente público de convivialidade. A importância da distribuição do espaço e das trocas citadinas, desse modo, é fundamental tanto na cidade real quanto no mundo virtual, e isso em boa medida ajuda a ilustrar o poder regulador no ciberespaço atribuído à arquitetura/código por Lawrence Lessig (Lessig, 1997) (como há de ser explorado adiante, os espaços possíveis e disponibilizados no mundo virtual são conformadores dos comportamentos e condutas

possíveis naquele ambiente). Além disso, e não à toa, o atual momento de aumento do poder e influência das *bigtechs* pode também ser comparado ao movimento de ascensão do Estado Moderno, já que muitas analogias entre as cidades do ciberespaço e as cidades modernas são facilmente traçáveis, e revelam a reprodução de mecanismos de controle estatal pelos provedores de serviços de internet em geral (o que igualmente há de ser explorado adiante, com base na obra de Vili Lehdonvirta (Lehdonvirta, 2022)).

Hoje em dia, com a transposição dos cotidianos para o ciberespaço e as filtragens promovidas por algoritmos cada vez mais sofisticados, o espírito de convivência citadina do mundo real vai se perdendo no ambiente virtual. A escalada do direcionamento de conteúdo conduz internautas, pouco a pouco, a bolhas de pensamento, onde as trocas se dão quase tão somente entre usuários de ideias afins. Essa sistemática vai contra o que diz Sunstein (2017), para quem um sistema de garantia de liberdades saudável deve contar com duas características imprescindíveis. A primeira é que as pessoas têm de ser expostas a materiais com os quais elas não teriam escolhido, de antemão, ter contato. A segunda é que os cidadãos, em sua maioria, devem partilhar de uma gama de experiências comuns entre si, de modo a promover uma espécie de "amarração social" entre eles (Sunstein, 2017, p. 6-12). No ciberespaço, o crescente ostracismo das ideias e esboroamento de tais características acabam por conduzir-nos, progressivamente, segundo Sunstein, a crises do sistema democrático - não somente as que hoje presenciamos, como outras, vindouras e ainda imprevisíveis. Para o autor, o excesso de autoisolamento e personalização de conteúdo promovem a fragmentação do corpo social e representam sério risco à democracia. Em vista disso, a reabilitação dos indivíduos para conviver com a coletividade requer medidas que, de um jeito ou de outro, alterem a estrutura de funcionamento das redes. Em outros termos, a regeneração das democracias demanda a regulação das atividades da vida em rede. A discussão sobre moderação de conteúdo *online* que norteia esse trabalho tem como pano de fundo a mesma crise da democracia e da liberdade aventada por Sunstein.

Apresentados os contrastes entre as cidades democráticas do mundo real e a concentração dos indivíduos em bolhas no ciberespaço, metáfora que será revisitada ao longo de todo este trabalho, se passa à análise da bibliografia que discute a regulabilidade da internet.

2.2 Afinal, a internet é regulável? O embate entre ciberlibertários e ciberpaternalistas.

Ainda nos anos 90, quando a internet comercial começava a ganhar popularidade, a publicação da "Declaração de Independência do Ciberespaço", por John Perry Barlow (1996), causou alvoroço. Tomando emprestado o termo "ciberespaço", cunhado por William Gibson na obra *cyberpunk* "*Neuromancer*"[1], Barlow inaugurava a chamada corrente ciberlibetária ao defender que a inexistência de territorialidade e a ausência de soberanias nacionais, no controle do ciberespaço, fariam com que jurisdição alguma pudesse ali ser imposta (Murray, 2015, p. 198). Em outros termos, dizia que a internet seria incontrolável por Estados tradicionais. "Nos espalharemos por todo o planeta e ninguém poderá capturar nossos pensamentos" (Barlow, 1996, p. 2), profetizava o autor em momento de exaltação libertária. A moção antirregulatória dos ciberlibertários, vinculados em sua maioria somente à sociedade civil[2], não durou muito, e logo provocou respostas por parte da comunidade acadêmica[3]. Espelhando-se na obra de Joel Reidenberg (1997), um dos primeiros autores a sugerir que desenvolvedores de tecnologias eram tão importantes para a proteção de dados e segurança no ciberespaço quanto formuladores de políticas e legislação convencionais, Lawrence Lessig revolucionou o debate ao discorrer sobre o papel do código na regulação mundo virtual. Para o autor, o estudo das relações do direito com o ciberespaço é tudo menos inócuo, distante da metáfora da "lei do cavalo", da qual outrora ciberlibertários se valeram para se referir a possíveis "leis do ciberespaço"[4]. Para ele, conhecer a fundo a relação da lei com o ciberespaço tem importância para além das fronteiras do mundo virtual (Lessig, 1999).

Para demonstrar os modos como os comportamentos podem ser conduzidos ou direcionados, Lessig (1996) lista quatro modalidades que, combinadas entre si, promovem o controle das condutas dos indivíduos - tanto no mundo real, quanto no ciberespaço. São elas: [1] As normas sociais, que regulam por meio da coação moral e social; [2] os mercados, que regulam por meio dos preços; [3] as leis, que regulam por meio da imposição de regras jurídicas

[1] Nos termos de Gibson: "Ciberespaço. Uma alucinação consensual experimentada diariamente por bilhões de operadores legítimos, em todas as nações, por crianças que aprendem conceitos matemáticos... Uma representação gráfica de dados abstraídos dos bancos de todos os computadores do sistema humano. Complexidade inimaginável. Linhas de luz espalhadas no não-espaço da mente, grupos e constelações de dados. Como as luzes da cidade, afastando-se." [tradução nossa] (apud., Lehdonvirta, 2022, p. 15).

[2] É interessante pontuar que Barlow sustentou ativismo sem vincular-se à academia, e foi um dos fundadores da Electronic Frontier Foundation (EFF).

[3] Considerando que os meandros desse debate são em boa medida conhecidos, hoje em dia, nos círculos que estudam a regulação da internet, e em vista das limitações de espaço do presente trabalho, não cabe aqui pormenorizar, amiúde, os desdobres da discussão. De forma que é suficiente comentar alguns dos autores de maior relevância do período, elementares para a discussão teórica que segue adiante.

[4] O artigo "The Law of the Horse" foi assim intitulado em referência à declaração de Frank Easterbrook, quem em conferência menosprezou a relevância do direito de ciberespaço ao afirmar que "não havia uma lei do ciberespaço, assim como não havia uma lei do cavalo". (Lessig, 1999, p. 2).

e previsão de sanções; e [4] a arquitetura, ou natureza, que regula o comportamento por meio de disposição do espaço. Por arquitetura o autor se refere às estruturas que permitem, facilitam, dificultam, ou até mesmo impedem o acesso dos indivíduos a determinados espaços - como uma "ponte que impede a passagem de ônibus", ou "uma estrada que separa dois bairros" (Lessig, 1999, p. 7). Por consequência, a arquitetura condiciona o comportamento dos ocupantes dos ambientes de modo geral. O ponto central do argumento de Lessig está no fato de que tal arquitetura também existe no ciberespaço, embora lá, diferentemente do que ocorre no mundo real, seja representada pelo código. Nesse ponto calha anotar que, conforme observa Andrew Murray, a proposta regulatória de Lessig se baseia na assunção de que a geografia do ciberespaço é análoga à do mundo real (Murray, 2015, p. 202), e não causa espanto, embora desponte como curiosidade, que as metáforas de pontes e estradas utilizadas em sua obra advenham dos mesmos exemplos escolhidos por Jane Jacobs para as reflexões de "Morte e Vida nas Grandes Cidades Norte-americanas"[5]. É por intermédio da codificação e programação dos ambientes virtuais disponibilizados aos usuários que, aqueles que detém o poder para criar e modificar o código condicionam comportamentos *online,* reproduzindo em boa medida as delimitações da arquitetura do mundo real. Segundo Lessig (1996, 1997, 1999, 2006), essas quatro modalidades regulatórias não operam isoladamente. Elas costumam ser combinadas para que determinados fins regulatórios sejam alcançados, tanto no mundo real quanto no mundo virtual. O poder de influência de cada modalidade no ciberespaço, no entanto, e em comparação ao mundo real, é que tende a ser diferente. Enquanto no mundo de carne e osso a lei costuma ser a modalidade de maior influência, no ciberespaço é o código que goza do mais relevante potencial regulatório.

Diversamente da arquitetura do mundo real, no ciberespaço o código possui maleabilidade e permissividade ímpares, dependendo (quase sempre) tão somente da criatividade de desenvolvedores de *softwares*, *hardwares* e serviços digitais em sentido amplo. Desse modo, o código funciona de forma desvinculada de restrições naturais inamovíveis pelo trabalho humano, enquanto a arquitetura deve respeitar limites fisiológicos, de espaço físico, de orçamento e de forças da natureza que não se aplicam ao ciberespaço. A mera existência dessa particularidade, alerta Lessig (1999), evidencia que o ciberespaço não apenas é regulável,

[5] A autora se refere, em mais de uma ocasião, às políticas de urbanização capitaneadas por Robert Moses na cidade de Nova Iorque, na primeira metade do século XX. Em que pese tenha viabilizado obras de estruturação da cidade que até hoje gozam de enorme relevância, Moses é acusado de racismo por ter projetado pontes baixas que impediam a chegada de ônibus a espaços nobres de convívio, por ter construído estradas que circulavam bairros populares e os punham em parcial isolamento, dentre outros. Ver em https://en.wikipedia.org/wiki/Robert_Moses. Último acesso 16/10/2023.

como já é conduzido em função do *design* das plataformas e dos serviços disponibilizados aos usuários. O que é possível operar em determinado serviço, ou o que é vetado, bem como os modos que cada plataforma se apresenta ou direciona usuários é, por si só, fruto das escolhas de agentes que *decidiram* como tal serviço se estruturaria. Essa constatação, de largada, rechaça a expectativa libertária absoluta outrora veiculada na Declaração de Independência do Ciberespaço de Barlow. Em outros termos, já há regulação. Não apenas isso, tal movimento acaba por tirar, de sobremaneira, o poder regulatório direto das mãos de agentes públicos, transferindo-o ao controle privado. Nos termos de Lessig:

> O código pode ser projetado da maneira que seu criador desejar, e os criadores de código têm pouco incentivo para tornar seu produto imperfeito. Sistemas confiáveis, portanto, são formas de direito privado. São arquiteturas de controle que deslocam as arquiteturas de controle efetivadas pelo direito público. E na medida em que as arquiteturas do direito são equilibradas entre valores privados e públicos, devemos nos preocupar se as arquiteturas do código se tornarem desequilibradas. Devemos nos preocupar, isto é, se eles respeitam valores privados, mas deslocam valores públicos [tradução nossa] (Lessig, 1999, p. 29).

O excerto revela uma das principais inquietações do autor com relação a nova ordem imposta pelo poder do código e pela concentração de poder regulador nas mãos de atores privados: como preservar, no ciberespaço, valores e princípios basilares do Estado de Direito? Em breve parênteses, é importante acrescentar que, para Lessig, direito público e direito privado são oxímoros. Valendo-se de entendimento da escola realista, o autor entende que os contratos derivados das relações de consumo originadas no ciberespaço são, ao fim e ao cabo, matéria de direito público. Tais contratos devem, portanto, servir a valores públicos comuns (Lessig, 1999, p. 30). Para ele, embora o Estado tradicional tenda a perder a ingerência direta sobre o ciberespaço, garantir que valores públicos essenciais sigam sendo aí respeitados deverá ser o principal desafio, para o qual Lessig propõe soluções mediante o emprego de regulação indireta. Segundo o autor, os governos tradicionais não necessariamente terão de ceder espaço ante o agigantamento de agentes privados, e poderão se adaptar ao novo equilíbrio entre as quatro modalidades regulatórias, controlando o código indiretamente por intermédio da lei (Lessig, 1997).

A relação paradoxal entre direito público e privado é objeto de discussão de diversos autores que pensam o ciberespaço, e há de ser abordada novamente neste trabalho. De momento, vale mencionar que, para Lessig, a natureza pública inerente ao ciberespaço derruba o argumento ciberlibertário de que a ausência do Estado garantiria total e irrestrita liberdade de expressão. Por essa razão, consistindo o ciberespaço em ambiente de uso público, estruturado por meio de ferramentas de *design*, a garantia que valores constitucionais originais

sejam preservados deve vir, preferencialmente, de atores em alguma medida vinculados ao Estado ou imbuídos de legitimidade democrática (Lessig, 1997). Segundo ele, a regulação atacada por partidários da declaração de Barlow "é a mesma regulação que deveriam abraçar", a fim de garantir a liberdade de expressão pela qual tanto prezam (Lessig, 1997, p. 182).

As quatro modalidades condicionadoras do comportamento e o papel fulcral do código propostos por Lessig representam verdadeiro divisor de águas e permeiam, até os dias atuais, o debate acadêmico sobre a regulação do ciberespaço. Dentre os autores que estenderam a proposta, é importante mencionar, ainda que brevemente, Andrew Murray e o comunitarismo de rede. Murray complexifica a proposta regulatória de Lessig, adicionando elementos sociais à tecnicidade de seu antecessor, visando melhor entender a divisão de forças entre as modalidades regulatórias e as eventuais falhas do código como condicionador dos comportamentos. Para o britânico, o que explica o fato de a internet ser tão vastamente "não controlada", a despeito do poder regulador do código aventado por Lessig, guarda relação com o fato de o ciberespaço não ser geograficamente análogo ao mundo real. O ciberespaço é um local "não apenas de geografia e estrutura, como também de comunicação e discursos" (Murray, 2015, p. 203). Após definir essa máxima, Murray expande o escopo de sua análise para além da tecnicidade, adotando princípios de teorias de ciências sociais e da Teoria do Ator Rede (TAR), de Bruno Latour. Com isso, o autor se esforça por indicar que os sujeitos ativos nas diversas comunidades existentes no mundo virtual não são apenas *receptores* das determinações impostas pelo código, mas sim participantes ativos das inúmeras teias comunicacionais que compõem o mundo virtual - contrariando termo cunhado por Lessig (2006), que afirmou que tais sujeitos seriam um mero "ponto patético", sem qualquer influência na formulação das redes.

Os diversos indivíduos do ciberespaço, pertencentes a agrupamentos dos mais variados tipos, exercem diferentes níveis de influência sobre os demais membros de suas comunidades, a depender dos dados e canais de comunicação que retêm. Ou seja, Murray não contesta o poder regulador do código, mas atribui enorme relevância às redes de fluxo de informação formadas por usuários e provedores, as quais compõem estruturas que influenciam e são influenciadas pela conformação do próprio código. Em termos muito enxutos, é certo que grandes provedores de plataformas gozam de grande poder, sugerindo serviços e possibilidades de usufruir do ciberespaço aos usuários. Isso, porém, não quer dizer que sujeitos e grupos de menor envergadura não exerçam qualquer tipo de influência nesse processo. Muito embora a divisão desigual de fluxo de dados entre os diversos atores acabe por produzir alguns canais

mais poderosos do que outros, usuários individuais retiram sua força de sua numerosidade (Murray, 2015, p. 219). É dessa forma que os fluxos comunicacionais, de afinidades e aprovação, os quais invariavelmente passam por todos os sujeitos conformadores de comunidades no ciberespaço, acabam por confirmar ou rechaçar as estruturas virtuais colocadas pelo código (ou, em outras palavras, construídas e disponibilizadas pelas plataformas, a exemplo do que veremos mais adiante com a edição do *Digital Economy Act* 2010 do Reino Unido, para combater o compartilhamento ilegal de arquivos). Para Murray, ainda que o comunitarismo de rede não seja uma teoria que sirva para explicar a legitimidade da regulação do ciberespaço, ela representa um meio para medir a possível eficácia de políticas regulatórias propostas para o ciberespaço (Murray, 2015, p. 208). Isso ocorre porque a chancela de sujeitos aleatórios, para serviços de provedores desvinculados de corpos governamentais tradicionais, não consiste em processo democrático propriamente dito.

Ao levar em conta elementos sociológicos e dinâmicos, a teoria de Murray complexifica a proposta regulatória de Lessig. Esse movimento intelectual é fundamental ante o cenário vertiginoso no qual, hoje em dia, são debatidos a necessidade e os limites da regulação do ciberespaço. É certo que a relevância de atores não-estatais nos movimentos regulatórios é uma realidade que antecede o processo de virtualização da vida em sociedade. Entretanto, o agigantamento de *bigtechs* e o poder que elas gozam para influenciar diretamente a estrutura do ciberespaço levaram o Estado pós-regulatório a um nível sem precedentes. Com base em analogia do próprio Murray, tal momento representa um marco histórico, que separa os modos de governança da era Westfaliana dos novos meios de governança pós-Westfália (Leiser e Murray, 2016).

Nas disputas políticas e econômicas que hoje permeiam os processos de tentativa de regulação do ciberespaço, especialmente no tocante ao controle de conteúdo e possibilidade de responsabilização das plataformas, é certo que qualquer movimento de governança terá de se dar em negociação com atores não-estatais. Ainda que a possibilidade de regular o ciberespaço seja debate (praticamente) pacificado nos tempos atuais, equilibrar os interesses de governos e *bigtechs*, levando em consideração valores democráticos e demandas sociais hodiernas, é equação ainda sem solução, a qual vai além da simples regulação indireta outrora proposta por Lessig (1996).

2.3 Queira sim, queira não, há regulação.

Como descrito, os diálogos sobre a possibilidade de regulação do controle de conteúdo na internet são parte de um debate maior, filosófico e ideológico, longe de ser pacificado: o que garante a liberdade, afinal? A ausência de intervenção de autoridades? Ou seria a garantia, por parte das mesmas, de que direitos individuais serão respeitados? Por certo, este trabalho não pretende responder definitivamente a tais perguntas, as quais devem seguir ecoando por tempo indefinido. Ainda assim, entende-se que a liberdade absoluta é inatingível, para não dizer utópica, e partilha-se do entendimento de Lessig de que a regulação, tal qual conhecemos, não implica necessariamente na mitigação das liberdades, muitas vezes podendo significar justamente o contrário. Fazendo uso das palavras de Cass Sunstein,

> [...] liberdade não pode ser sempre identificada como 'escolhas'. Por certo, sociedades livres geralmente respeitam escolhas livres. Mas, por vezes, escolhas refletem e podem, na verdade, dar origem a falhas na liberdade dos indivíduos (Sunstein, 2017, p. 177).

Igualmente se está de acordo com a ideia de que é ingênuo supor que o ciberespaço não é regulável, como outrora proclamaram os ciberlibertários. Consistindo a internet em espaço cuja disposição de arquitetura e *design* condiciona comportamentos – nos termos da proposta de Lessig -, os agentes responsáveis pela criação e manutenção do código estão sempre, de um jeito ou de outro, induzindo as atividades humanas no ambiente virtual. Isso, por si só, já é regulação.

Em vista do exposto, é interessante que se discorra com maior fôlego sobre os dois pontos basais da obra de Lessig acima mencionados. Primeiro, ainda que não se perceba, a regulação dos discursos no ciberespaço já é uma realidade, de forma que não é cabível a pergunta "se teremos regulação", mas "qual tipo de regulação teremos" (Sunstein, 2017, p. 178). Segundo, a regulação não é sinônimo de restrição da liberdade, e pode muitas vezes servir para garanti-la. Para isso, ferramentas administrativas tradicionais serão fundamentais para assegurar direitos.

No que tange ao primeiro ponto, importa observar o quanto *bigtechs* e empresas de telecomunicações em geral são, na atualidade e desde sempre, dependentes de aparatos estatais que garantam direitos de propriedade. Em que pese muitos críticos da regulação busquem distinguir entre direitos de propriedade e regulação coercitiva propriamente dita, ambas são fruto de atuação estatal, a qual busca o bom funcionamento de atividades privadas. O mesmo é verdade no tocante à internet. Atividades comerciais e administrativas de grandes plataformas

atuam segundo regras contratuais que, em sua essência, são asseguradas por mecanismos de direito privado disponibilizados pelo Estado. A recente venda do Twitter para Elon Musk é exemplo disso. A resistência da Meta em garantir a criptografia de ponta a ponta em suas mensagens, independente do teor das comunicações que possam estar a circular, é outro exemplo. O mesmo ocorre com a relação entre os desenvolvedores do Instagram e aqueles que pagam para anunciar seus produtos em *timelines* diversas. Dessa forma, o objetivo-fim destas empresas, que é por óbvio o lucro, somente é garantido a partir de instrumentos criados e proporcionados pelo aparato estatal, os quais, a seu turno, consistem em ferramentas regulatórias de direito público. Na obra *#Republic: Divided Democracies in the Age of Social Media*, Cass Sunstein assim afirma:

> Embora muitas pessoas não pensem desde essa perspectiva, regras de propriedade, quando garantidas por lei, são a quintessência da regulação estatal. Elas criam e limitam poderes. Determinam quem é dono do que, dizem quem pode fazer o quê e para quem. Elas permitem que algumas pessoas excluam outras de seus domínios. E isto é regulação, em poucas palavras [tradução nossa] (Sunstein, 2017, p. 180).

A mesma estrutura se aplica à circulação dos discursos e fluxo de informação *online,* deflagrando o poder do código como ferramenta de condicionamento dos comportamentos. Isso ocorre porque os provedores, ao deterem os códigos que desenham e arquitetam plataformas, desfrutam da capacidade de preservar alguns discursos e de suprimir outros com base nos mesmos direitos de propriedade aqui mencionados. Eles selecionam e direcionam algoritmos de modo a maximizar seu lucro mediante a exploração comercial de suas empresas. Obviamente, não se quer dizer com isso que plataformas têm controle absoluto das informações que por suas redes circulam (se assim fosse não teríamos a miríade de trabalhos discutindo moderação de conteúdo, qual ora temos). Tampouco se nega aqui que há, sim, diferenças entre direitos de propriedade, contratos e regras que visam especificamente a regular a liberdade de expressão no âmbito do direito público. O que buscamos deixar claro é que, apesar das diferenças, são todos meios de regulação, e chamar um de um modo e o outro de outro é "questão de semântica" (Sunstein, 2017, p. 187). O intuito, desse modo, é explicitar que regulação é condição *sine qua non* e já existente para o funcionamento – e mesmo para a existência – dos mercados na internet, seja qual for sua razão de ser, queira sim, queira não. Mais do que isso, busca-se evidenciar que a liberdade de expressão se beneficia de direitos de propriedade bem estruturados, uma vez que garantias sobre a propriedade e os contratos tendem a fazer com que as instituições funcionem de modo mais estável e seguro. Por consequência, esse processo estimula o investimento em garantir a circulação salutar de conteúdo e discursos por parte das plataformas.

Com base nessa última afirmação, adentra-se no segundo ponto aventado no início deste subcapítulo, onde se afirmou que regulação não é sinônimo necessário de restrição de liberdade. Tal qual mencionado por larga gama de autores, a exemplo de Lessig e Jacob Rowbotton, definir regras de controle de discurso mais serve para garantir a liberdade e a possibilidade de manifestação dos diferentes sujeitos do que, de fato, reprimi-los. A ideia, grosso modo, é criar mecanismos básicos que permitam que diferentes vozes possam ser ouvidas independente do seu poder de barganha ou de influência, ao mesmo tempo em que é evitada a difusão de ideias incondizentes com o Estado democrático, como a apologia à violência ou o racismo (Rowbottom, 2010). É certo que a moderação de conteúdo no ciberespaço demanda ferramentas regulatórias para além das matérias de propriedade e de contratos, e boa parte da urgência com que vem se tratando desse tema está relacionada com o debate sobre o modo como administrar os discursos. Também não há dúvida de que, tratando-se de assunto que invade a seara da política e da ideologia, qualquer interferência regulatória (de governos ou de agentes privados) deve ser bem pautada e promotora do debate democrático, jamais o oposto. Isso de modo algum implica dizer que não há, nem deve haver, regulação do ciberespaço. Novamente, a citar Sunstein:

> Aqui, então, está meu apelo: quando estamos a discutir possíveis abordagens para a internet ou outras tecnologias da comunicação - hoje, no horizonte, ou as nunca antes imaginadas - não devemos nunca sugerir que um caminho envolve regulação governamental e o outro não. Declarações desse tipo produzem confusão sobre o que se está a fazer e sobre quais são nossas verdadeiras opções. E esta confusão está longe de ser inócua. Ela coloca aqueles que estão tentando avançar a operacionalidade do discurso em séria desvantagem. Um público pautado pela democracia deve ter a possibilidade de discutir questões aberta e pragmaticamente, e sem a interferência de mitos que apenas sirvam a interesses próprios, invocados por quem se beneficia, todos os dias, do exercício dos poderes de governo em seu favor [tradução nossa] (Sunstein, 2017, p. 190).

Não se trata de debater se a internet é, ou não, regulável. Trata-se, isso sim, de discutir quais os modos, qual a extensão, e quais os atores que estarão envolvidos em tal processo de regulação. Na esteira de Lessig, isso de modo algum deveria servir para coagir os discursos. Pelo contrário, regular garante o exercício da liberdade individual e equânime. Conforme afirma Sunstein, aqueles que mais ferozmente reclamam a liberdade de expressão, vociferando ante qualquer tentativa regulatória por parte das autoridades, são geralmente os que mais se beneficiam da ineficiência regulatória do Estado (ou de outro agente centralizador) nesta seara (Sunstein, 2017, p. 200). Em vista dos correntes debates públicos - no Reino Unido, no Brasil, ou onde seja -, tal afirmação escancara que o que está em jogo vai além da garantia do direito de livre manifestação das ideias, envolvendo disputas sobre como a política econômica do fluxo de informação e mercados na internet será empreendida de aqui em diante. Os usos

sociais a serem permitidos e incentivados na internet são, desse modo, palcos de disputas políticas e econômicas, através dos quais os diferentes movimentos regulatórios, que ocorrem concomitantemente ao redor do globo, tendem a privilegiar alguns comportamentos e discursos em detrimento de outros. Os cenários no quais ocorrem essas disputas envolvem muitos agentes além da simples lógica indivíduo *versus* Estado, e mesmo a participação de atores privados guarda particularidades próprias da era digital, na qual plataformas crescentemente emulam mecanismos estatais a fim de fazer prevalecer seus interesses (Lehdonvirta, 2022). Essa conjuntura será novamente comentada ao longo deste trabalho. Por ora, vale analisar de que maneiras o controle de conteúdo e a liberdade de expressão podem coexistir no ciberespaço de um Estado democrático.

2.4 Do direito constitucional ao administrativo: o controle dos discursos e a liberdade de expressão na era digital.

A esta altura da revisão que aqui se desenrola, não resta dúvida de que um dos debates mais candentes na seara da regulação da internet recai sobre a relação entre controle de conteúdo e liberdade de expressão. Tratando-se de direito inerente a regimes democráticos, a liberdade de expressão goza das mais substanciosas garantias legais em qualquer Estado de Direito. Embora alcance extensões diversas, a depender da jurisdição, a liberdade de expressão ocupa lugar central nas democracias mundo afora, de modo que, para que o direito de livre manifestação seja afastado ou mitigado, via de regra, é necessária a chancela do Poder Judiciário. Na era da sociedade informacional, todavia, os limites e as possibilidades da liberdade de expressão ganham novos contornos. A velocidade e a capilarização com que os discursos circulam pelas redes esgarçam debates doutrinários sobre a liberdade de discurso, bem como quanto ao modo pelo qual a garantia deste direito deve ser tratada pelas autoridades e agentes envolvidos. Ainda que não seja possível indicar ao certo qual a melhor abordagem para lidar com as mudanças aportadas pela digitalização da sociedade, torna-se cada vez mais claro que demandas coletivas, administrativas e de arquitetura tendem a ganhar relevância neste novo cenário, diminuindo a incidência da apreciação judicial sobre os discursos.

Esse fenômeno foi antevisto, em parte, por Jack M. Balkin, quem discorreu sobre as prováveis particularidades da liberdade de expressão na era da sociedade informacional, tendo por cerne a Primeira Emenda da constituição estadunidense. Segundo Balkin, ao passo em que

nossas vidas se tornam cada vez mais dependentes da tecnologia e do fluxo de informação, a Primeira Emenda se mostra menos relevante para solucionar embates sobre direitos individuais de livre manifestação. Não se trata de diminuir a importância dos valores resguardados pela referida Emenda, senão o contrário. A proteção para que os sujeitos se expressem, criem e questionem, bem como a proteção para compartilhar e debater conteúdos, deve seguir em sua condição de protagonismo. O modo como essa proteção deve ser levada a cabo, no entanto, é que tende a ser modificado pelo contexto de tecnologia. Balkin defende que a apreciação de tais valores deverá ser paulatinamente deslocada do âmbito constitucional para outras áreas do conhecimento e do Poder Público, notadamente para regulações administrativas e legislativas, bem como para soluções de *design* das plataformas (Balkin, 2009, p. 427).

Ao supor que provedores de serviços de internet deverão filtrar conteúdos mais por motivos econômicos do que morais – "para favorecer parceiros de negócios e proteger modelos comerciais específicos" (Balkin, 2009, p. 431) -, Balkin argumenta que o resguardo à liberdade de expressão deverá passar pela regulação antitruste e pela promoção da inovação no âmbito das empresas de tecnologia. Ou seja, para que o fluxo de informação respeite a pluralidade de discursos e permita que novas ideias e serviços floresçam e circulem, é importante manter as redes virtuais como ambientes não discriminatórios. Desse modo, garantir que serviços de informação digitais permaneçam abertos à concorrência é fundamental para salvaguardar a liberdade de expressão. Em outros termos, o livre fluxo das ideias depende não apenas da ausência de censura, como também da existência de uma infraestrutura livre, competitiva, viva e pulsante, capaz de garantir a circulação de informação e discursos, bem como do desenvolvimento e inovação de tecnologias comunicacionais. Ao apostar na democratização das possibilidades de comunicação através da internet, Balkin afirma que o crescente protagonismo dos serviços de rede gera dois movimentos concomitantes e contraditórios entre si. Por um lado, há um movimento de aumento da participação dos usuários nos debates públicos, por outro, há uma crescente tendência à apropriação desses espaços de comunicação pelos agentes privados que os disponibilizam. Tal dinâmica dá origem a uma relação moto-contínua, que faz com que a tecnologia incentivadora do envolvimento dos cidadãos seja a mesma tecnologia que cerca e engessa tais serviços. É para controlar esse fenômeno que Balkin afirma que a proteção "aos valores da liberdade de expressão na era digital será cada vez menos um problema de direito constitucional – embora estas proteções seguirão sendo importantes – e mais um problema de tecnologia e regulação administrativa" (Balkin, 2009, p. 441). O modo

como construído o *design* das plataformas, igualmente, é fundamental para salvaguardar os espaços de livres fluxos de conteúdos.

Balkin vai além. Para o autor, a sociedade da informação tende a reformular o modo com o qual nos relacionamos com a liberdade de expressão, e, por consequência, possui o condão de modificar o modo pelo qual esse direito é garantido no Estado democrático. Ele sugere que a era digital fará com que a liberdade de expressão não seja apenas uma ferramenta para promover a democracia, mas sim para alavancar o que chamou de *cultura democrática.* Por cultura democrática, Balkin se refere à "cultura na qual cidadãos ordinários poderão participar, tanto coletiva quanto individualmente, da criação e elaboração dos significados culturais que os constituem como indivíduos" (Balkin, 2009, p. 438). Isto é, partindo do entendimento de que nós, seres humanos, como sujeitos e sociedade, somos culturalmente constituídos, o autor prevê que a informatização tende a catalisar o movimento de debate e circulação de ideias que põem em marcha a produção cultural, democratizando as possibilidades de participação de todo e qualquer cidadão em tal processo. Nos termos de Balkin, "a cultura democrática não é democrática por que as pessoas podem votar em como a cultura deve ser [...], mas sim porque as pessoas participam da produção da cultura através de comunicação e influência mútuas" (Balkin, 2009, p. 438). Além disso, a cultura democrática transborda os limites do Estado Nação, já que tais debates e circulação de ideais não se contêm dentro das fronteiras políticas nacionais.

É interessante mencionar que, para Balkin, manter viva a cultura democrática guarda íntima relação com as garantias prestadas pela Seção 230(c)(1) no ordenamento norte-americano. Em brevíssima explicação, cabe afirmar que esse dispositivo legal isenta prestadores de serviços de internet de responsabilidade sobre conteúdos produzidos por terceiros e veiculados através de suas redes. O autor entende que a responsabilização de empresas de tecnologia serviria como incentivo para que filtros e ferramentas de controle de conteúdos que *devem* ser removidos fossem desenvolvidos. Ainda assim, ele sustenta que tal responsabilização tenderia mais a um resultado daninho à cultura democrática do que o contrário, pois forçaria provedores a simplesmente encerrarem seus serviços. Isso, por consequência, reduziria o acesso de usuários a mecanismos de circulação de informação (Balkin, 2009, p. 436).

No que tange a esse último ponto, a literatura mais moderna em boa medida diverge de Balkin, bem como a nova legislação britânica optou justamente pelo oposto. A ter por

escopo o atual estado da arte sobre controle de conteúdo, é interessante comentar alguns pontos que, no entendimento desse trabalho, foram equivocadamente antecipados pelo autor. Ao publicar o artigo "O futuro da liberdade de expressão na era digital" (no original, *"The future of free expression in a digital age*") (Balkin, 2009), ele defendeu que a internet libertaria os usuários do intermédio de *broadcasters* da comunicação. Ao mencionar o processo de desenvolvimento tecnológico de mídias de massa do começo do século XX – notadamente rádio, televisão, cinemas e transmissão via satélite -, Balkin afirmou que esse se deu concomitantemente à concentração de jornais nas mãos de alguns poucos, o que resultou no fato de que poucas pessoas podiam, individualmente, tomar parte em debates públicos. Para o autor, esse fenômeno tenderia a ser mitigado na era digital. Na opinião desse trabalho, essa afirmação está parcialmente correta. De fato, multiplicaram-se os canais através dos quais a comunicação entre os sujeitos se dá. E é verdade que *é possível* que um pequeno comunicador alcance um público maior do que alcançaria antes da popularização da comunicação digital. Todavia, possível não é sinônimo de provável. A mesma arquitetura de rede que Balkin considerou ser chave para o controle dos canais de comunicação digital, há mais de uma década, hoje manipula dados e direciona os usuários a conteúdos afins, impulsionada por algoritmos, anunciantes comerciais, engajamento, e outros incontáveis fatores (Sunstein, 2017). Diante disso, a inexigência de responsabilidade de plataformas em razão dos conteúdos que circulam em suas redes, além de não ter propriamente contribuído para o incremento saudável do debate público, vem crescentemente abrindo espaço para que discursos daninhos à cultura democrática ganhem espaço[6].

[6] Recentemente, a inafastabilidade da mesma Seção 230 (1) c do *Communications Decency Act* (CDA), aclamada por Balkin como fundamental à livre circulação de ideias no ambiente virtual, foi submetida a júdice pela Suprema Corte norte-americana, que anunciou que no ano de 2023 apreciaria os casos *Gonzalez vs Google* e T*witter vs Taamneh.* Em explicação muito enxuta, o caso *Gonzalez vs Google LLC* tem por escopo decidir se a Seção 230(c)(1) do CDA garante a imunidade de plataformas quando estas fazem recomendações direcionadas de informações fornecidas por outro provedor; ou apenas limita a responsabilidade dos serviços de plataformas no tocante a funções editoriais tradicionais, novamente em relação a tais informações. Disponível em https://www.supremecourt.gov/docket/docketfiles/html/qp/21-01333qp.pdf Último acesso 10/05/2023. No que concerne ao caso *Twitter vs Taamneh*, as questões sob apreciação foram: se um servidor que fornece serviços genéricos e amplamente disponíveis a todos os seus numerosos usuários e "regularmente" trabalha para detectar e impedir que terroristas usem esses serviços "conscientemente" forneceu assistência substancial sob a Seção 2333 apenas porque supostamente poderia ter tomado medidas mais "significativas" ou ação "agressiva" para impedir tal uso; e se um servidor cujos serviços genéricos e amplamente disponíveis não foram usados em conexão com o "ato de terrorismo internacional" específico que prejudicou o autor pode ser responsabilizado por auxílio e cumplicidade nos termos da Seção 2333 do Antiterrorism and Effective Death Penalty Act (AEDPA). Disponível em https://www.supremecourt.gov/qp/21-01496qp.pdf Último acesso 10/05/2023.
Em maio de 2023, a Corte pronunciou-se no sentido de que, no caso *Twitter*, as acusações à empresa não poderiam ser feitas sob o *Antiterrorism Act*, aplicando o mesmo entendimento ao caso Gonzalez. Este último foi devolvido à Corte originária, e em nenhum dos dois foi apreciada a polêmica questão da Seção 230 (1).

O processo de digitalização da sociedade consiste em movimento social e político de enorme complexidade. Há que se ter em conta que se trata de fenômeno ainda em andamento (uma história do tempo presente, afinal). Assim, é natural que os rumos do fluxo da informação digital e suas consequências não pudessem ser totalmente antevistos por Balkin, quem publicou seu artigo há mais de 15 anos. O ensaio, ainda assim, contribuiu de forma substanciosa às reflexões sobre as relações entre o Direito e o ciberespaço, em especial no que se relaciona com a necessidade transpor o cuidado com direitos de expressão para as searas administrativa e de *design,* abandonando o controle casuístico até hoje feito pelas cortes.

Em artigo recentemente publicado pela Harvard Law Review, Evelyn Douek critica a ineficácia do modelo que mimetiza, no mundo virtual, o controle judicial *offline* sobre a liberdade de expressão e toma a linha proposta por Balkin para defender a construção de uma abordagem sistêmica para moderação de conteúdo *online*. Professora em Stanford, Douek, tal qual Balkin, fala desde a perspectiva estadunidense e afirma que o controle judicial e casuístico dos direitos de expressão no ciberespaço consiste em reprodução grosseira dos mecanismos de garantia de direitos de expressão utilizados no mundo real. Esses últimos, para ela, são insuficientes e impróprios para as demandas da era digital. Segundo a autora, a mera transposição das ferramentas de garantia de liberdade de expressão do espaço físico para o virtual replica o controle pautado pelo Direito Constitucional, e faz com que se suponha que o modo mais eficaz de tornar plataformas responsáveis por suas decisões (no tocante a quais conteúdos devem ser mantidos e/ou suprimidos) é fazer com que estas ofereçam a seus usuários ferramentas por meio das quais seja possível recorrer das decisões tomadas pelos moderadores de conteúdo. Em outros termos, fazer com que seja oferecida a possibilidade de usuários recorrerem, individual e casuisticamente, quando sentirem que seus direitos de expressão foram injustamente feridos pelo controle de conteúdo de cada servidor - em uma espécie de devido processo legal privado, criado e disponibilizado por *bigtechs* (Douek, 2022).

Douek firma pé, no entanto, que tal modo de operação é ineficaz e parcial. Primeiramente, porque a escala e a velocidade da comunicação no mundo virtual não permitem que o controle de conteúdo seja entendido meramente como o somatório de muitas – muitas – adjudicações pessoais *ex post.* Dessa forma, o incremento de mecanismos que buscam garantir o devido processo legal para fins de liberdade de expressão não é suficiente. Além disso, uma vez que o sistema padrão de controle de conteúdo foca nos méritos e particularidades de cada discurso, ele acaba por conduzir a intermináveis discussões, pesos e medidas, sobre o cabimento das normas para cada caso concreto (mais uma vez, determinados pelas próprias

plataformas). Para a autora, tal quadro não satisfaz as demandas sociais ora impostas pelo enorme fluxo de conteúdo *online*, tampouco impõe responsabilidade substantiva a provedores. A essa dinâmica, Douek se refere como "nada além de teatro de *accountability"* (Douek, 2022). Em que pese a autora fale tendo por escopo o modelo norte-americano, a sistemática por ela atacada é realidade em diversas jurisdições, na brasileira e britânica inclusive, focos principais deste trabalho.

Ao passo que o modelo atual de controle de conteúdo, via de regra, reproduz a estrutura padrão do resguardo judicial da liberdade de expressão, as plataformas têm pendido a cada vez mais se comportar como espécies de novos governos, criando regras e as aplicando aos usuários. Esse funcionamento muito se assemelha às funções legislativas e judiciais estatais. Nessa toada, o sistema de filtragem e controle de conteúdo das plataformas espelha modelos burocráticos hierárquicos, girando ao redor de casos paradigmáticos eleitos pelos mesmos agentes privados que desenham o sistema e impõem suas regras, inevitavelmente invocando valores de Direito Constitucional para isso (Douek, 2022, p. 538). Segundo Douek, dita arquitetura não ocorre apenas em razão do vácuo de poder deixado aos provedores, e em boa medida dialoga com a resistência das autoridades e sociedade civil para reconhecer que a dinâmica das garantias democráticas de liberdade de discurso são, na era digital, estruturalmente diferentes do modo como constituídas no passado. Para a autora, falta aos reguladores conhecimento sobre o funcionamento e particularidades do fluxo de conteúdo na era digital. Esse fato, somado ao reconhecimento de que aos governos não mais é possível trabalhar sem a agência das *bigtechs,* resulta na transferência do cuidado com os direitos constitucionais de livre manifestação das ideias aos agentes privados.

Polêmicas sobre o tratamento dado pelas plataformas aos diferentes discursos que circulam nas redes evidenciam a mentalidade *ex post* e subjetiva com que o controle de conteúdo *online* é socialmente encarado - a exemplo dos debates sobre o dever do *Facebook* de proibir o negacionismo de temas como vacina ou Holocausto, ou o quão correta foi a decisão do *Twitter* de banir a conta de Donald Trump após a invasão do Capitólio. Ao mesmo tempo, essas polêmicas explicitam a negligência com que se trata a velocidade e capilaridade do fluxo de informação. Afinal de contas, discursos afins ao negacionismo ou apoiadores do golpe ensaiado quando da invasão do Capitólio seguem circulantes e, em sua maioria, livres de qualquer exame por parte dos controladores de plataformas. Em vista desse cenário, a autora salienta que a simples reprodução de parâmetros judiciais para apreciação da liberdade de expressão ignora a capacidade técnica de vigilância efetiva dos dados que circulam nas redes.

Essa realidade, a seu turno, também corrobora a imparcialidade do controle de conteúdo praticado. É a ter em conta esse quadro que Douek propõe que a abordagem da liberdade de expressão na era digital deve ser sistêmica, *ex ante,* desligada do indivíduo, e se valer, para isso, de ferramentas institucionais de *design* e de princípios e práticas de Direito Administrativo (Douek, 2022). Nesse ponto, a proposta da autora é bastante semelhante ao proposto anos antes por Balkin (2009).

É interessante que se discorra um pouco mais sobre a proposição de Douek. A autora afirma que a abordagem individualizada e *ex post* para correção de erros de filtragem de conteúdo é equivocada por quatro razões. Primeiro, porque os casos individuais são parâmetros pobres para identificação de erros sistêmicos e tendências de problemas ocasionados pelo *design* de cada plataforma. Segundo, porque ainda que tais erros sejam identificados, solucioná-los casuisticamente é ineficaz para efetivamente consertar um sistema falido. Terceiro, pois qualquer política de transparência orientada por casos individuais tenderá a refletir uma visão limitada da dinâmica dos sistemas de moderação de conteúdo. Quarto, a aplicação simplista da lógica do devido processo legal não é suficiente para prestigiar todas as trocas e compensações envolvidas no processo de suprimir conteúdos, desincentivar comportamentos, controlar o fluxo de dados, entre outras questões (Douek, 2022, p. 569). Desse modo, ao focar em controlar os discursos de forma individual, o modelo padrão de filtragem ignora que sistemas de moderação de conteúdo devam se voltar a múltiplos objetivos e interesses, para além da simples lógica de tomar a decisão *correta* sobre seguir as regras da plataforma e suprimir apenas os conteúdos que *devem* ser suprimidos. Como qualquer empresa que visa a se manter em funcionamento, provedores são diariamente confrontados com a necessidade de sopesar interesses comerciais, demandas de usuários, moções sociais, regras e valores (sejam morais, sejam legais) que não são totalmente conciliáveis entre si. Admitir que tal modelo é ineficaz ante as demandas próprias da sociedade em rede, portanto, é elementar para a construção de um sistema de filtragem condizente com as possibilidades técnicas e quantitativas hodiernas. Nas palavras de Douek:

> [...] o modelo padrão é repleto de retratos nos quais os formuladores de políticas das plataformas lutam para equilibrar os valores da liberdade de expressão com outros interesses, a fim de chegar a uma *regra ótima*, novamente espelhando a adjudicação constitucional do mundo *offline*. Mas essa figura idealizada é incompleta. Por conta dos desafios práticos da moderação de conteúdo, na escala e velocidade com que ocorrem *online*, saber se uma regra é realística e tecnologicamente capaz de ser posta em vigor é central para o processo de formulação regulatória [tradução nossa] (Douek, 2022*,* p.551).

Além disso, a dificuldade de impor qualquer responsabilização ou transparência a servidores, por parte das autoridades, cria vácuos e insatisfações que, a sua vez, geram questionamentos quanto a legitimidade das plataformas para atuarem do modo qual atuam. É certo que as *bigtechs* são empresas privadas que naturalmente objetivam o lucro. Ainda assim, suas decisões têm impacto na esfera pública, em especial no que tange à liberdade de expressão. Em vista disso, é seguro afirmar que há uma expectativa coletiva quanto aos modos que dados e conteúdos serão tratados pelos servidores, bem como um entendimento tácito de que suas políticas de uso observem valores fundamentais de direito público. Segundo Douek, tais expectativas são constantemente frustradas em razão do sistema padrão de moderação de conteúdo, o qual, ao emular cortes, garantias de devido processo legal, e ao apreciar individualmente usuários que discordam das decisões dos filtros de conteúdo, acaba por reduzir a acurácia da moderação de modo geral. Esse mecanismo acaba por resultar em tratamentos diferenciados entre os usuários (Douek, 2022, p. 554).

Ante o quadro descrito, Douek acrescenta que o chamado "teatro de *accountability"* deriva tanto da reprodução *online* de ferramentas judiciais de garantias de direitos constitucionais quanto da falta de transparência, por parte das plataformas, dos números e motivos para remoção de conteúdos e/ou usuários. Em quase a totalidade das jurisdições onde atuam as *bigtechs*, as autoridades locais não impõem qualquer exigência para que suas políticas e resultados de moderação de conteúdo sejam efetivamente publicizadas. E, em que pese algumas empresas se proponham a entregar tais relatórios como parte de sua política institucional, via de regra são elas próprias que definem o que será e o que não será dito em seus informativos. Além disso, mesmo onde as autoridades reguladoras impõem aos servidores o compromisso de periodicamente prestar informações, tal qual ocorre na Alemanha desde o início da vigência da NetzDG, a fixação de critérios estanques e genéricos a serem esmiuçados deixa espaço para que os servidores não forneçam dados suficientes para "efetivamente avaliar o impacto de tal regulação" (Douek, 2022, p. 574). A situação se agrava ante a afirmação da autora de que relatórios de parâmetros frouxos e mal fixados tendem não apenas a desvirtuar seus propósitos de transparência e democracia, como podem ser facilmente mal compreendidos e conduzir provedores a ajustarem seus serviços de modo equivocado, parcial, e alijado do quadro geral. Segundo ela, a inexigência de transparência, a dificuldade para fixar elementos que *precisem* constar nos números divulgados pelos provedores, bem como os ajustes de *design* equivocados empreendidos pelas plataformas são igualmente desdobres da transposição do

controle de conteúdo *offline* para o ciberespaço. Essas realidades trazem consigo possíveis consequências negativas para os debates democráticos de qualquer espécie.

Já foi aqui pincelado que, para Douek, a solução passa por transpor as querelas sobre o controle de conteúdo *online* do âmbito constitucional para o âmbito administrativo, de *design*, e regulatório. Em que pese a autora não chegue a propor modelo regulatório bem acabado (longe disso, na verdade), para ela a moderação de conteúdo nas plataformas deveria ser estruturada de modo semelhante ao que ocorre em agências reguladoras. Nessas, há uma separação entre as funções políticas e aquelas que determinam como o controle de dados vai ser levado a cabo, o que permitiria exigir das plataformas que suas funções regulatórias e administrativas estejam totalmente alijadas de funções comerciais (nos termos de Douek, exigir que "seja colocada uma parede entre eles" (Douek, 2022, p. 587)). Ao defender uma solução envolvendo pensamento sistêmico[7], a autora admite que a falibilidade é aceitável, "um preço a ser pago", em troca de mecanismos de controle *ex ante,* mais abrangentes e gerais. Por meio da manipulação da arquitetura de cada serviço, esses mecanismos de controle devem servir para efetivamente filtrar e informar autoridades sobre tendências de teor das comunicações para cada caso concreto - promovendo a *administrabilidade* da filtragem de conteúdo e, principalmente, a justiça em massa ao invés da individual. A possibilidade de responsabilização e identificação de agentes envolvidos no processo de moderação é igualmente essencial na proposta de Douek, para quem focar em procedimentos de responsabilidade é politicamente mais viável e constitucionalmente menos suscetível do que a busca incansável por criar um "ambiente ideal para a liberdade de expressão" (Douek, 2022, p. 585). A autora firma pé, ainda, que critérios de transparência rigorosos e meticulosos devem ser exigidos não apenas para publicização de conteúdos removidos, como também quanto aos critérios utilizados, profissionais envolvidos, arquitetura de rede, dentre outros elementos. A obrigação de prestar relatórios de *compliance* regulares, ademais da possibilidade de imposição de multas para quem descumprir com o determinado, também devem estar presentes para a autora. No que tange às possibilidades técnicas de implementação da solução de pensamento sistêmico, ela reconhece que reguladores seguidamente esbarram na dúvida de saber se algo é tecnicamente cabível ou

[7] A proposta de Douek bebe na fonte das chamadas Teorias de *Systems Thinking*, cuja origem remete à primeira metade do século XX. Desenvolvidas a partir de experimentos das áreas de biologia e matemática, a teoria de pensamento sistêmico ganhou destaque na década de 1960, quando Jay W. Forrester desenvolveu modelo de computador que calculava como sistemas dinâmicos se comportavam, a fim de prever ciclos de negócios industriais. A lógica logo se difundiu para as mais diversas áreas do conhecimento - política, sociologia, cibernética, etc. -, e hoje pode ser definida, em termos muito enxutos, como "a investigação de qual conjunto de fatores e interações está contribuindo ou poderia contribuir para um possível resultado pretendido" (Morganelli, 2020) (Vihkornova, 2018).

não, mas que, de fato, não é pertinente exigir o impraticável. Defende, todavia, que plataformas não deveriam alegar limitações tecnológicas para evitar a responsabilidade de aprimorar seus sistemas, o que evidencia ainda mais a importância da transparência. Por fim, a autora esclarece que nem todo controle *ex post* deve ser banido. Para ela, a combinação *ex post* e *ex ante* é o ponto ideal para que a moderação de conteúdo seja equânime e, ao mesmo tempo, não estanque (Douek, 2022).

2.4.1 A primazia da liberdade de expressão na nova regulação da internet e o oxímoro direito público *versus* direito privado.

O cerne dos problemas elencados por Douek faz com que mergulhemos, novamente, no debate sobre como a liberdade de expressão deve ser encarada nas democracias ocidentais modernas. Ao longo do artigo mencionado, a autora não esconde seu incômodo com o altar na qual a liberdade de expressão é posta, estimada, e, via de regra, intocada. É a resistência em admitir que direitos de discurso devam ser tratados de modo diverso, apropriado às demandas da era da informação em massa, que em boa medida acaba por engessar a criatividade regulatória nesta seara. E, diante da necessidade de propor soluções para disputas entre discursos que buscam firmar seu espaço nas redes, combinada com a relutância para reformular a interpretação de dispositivos como a Primeira Emenda, soa quase inevitável que se transponha o sistema padrão *offline* para o ambiente virtual. Essa aparente insolubilidade é tema de reflexão de diferentes pensadores do Direito – Lessig (1997, 1999) já antecipara, em parte, tal contenda -, e guarda proximidade com questões culturais que têm na livre manifestação das ideias um bastião estanque do que é *ser livre* no Estado moderno.

Paul Schiff Berman tangencia o impasse ao comentar elementos que julga turvarem a distinção entre o público e o privado. Em termos muito enxutos, Shiff Berman refuta a possibilidade de distinguir, com clareza, entre as esferas pública e privada. O autor julga que ambas as esferas advêm de construções culturais que refletem a ordem social dominante, o que, por sua vez, faz com que a definição de o que é público e o que é privado seja inevitavelmente fruto de opinião pública (Shiff Berman, 2000). Em posicionamento com o qual esse trabalho se põe de acordo - e outrora aventado por Lessig e outros autores aqui não mencionados -, Shiff Berman admite que a separação entre público e privado é, em sua essência, uma quimera, ao mesmo tempo em que reconhece uma série de objeções que insistem em construir um muro

entre os dois terrenos. Dentre esses óbices, estaria a resistência dos cidadãos (no caso de Berman, cidadãos norte-americanos) ante tentativas acadêmicas de diluírem a separação entre público e privado (Shiff Berman, 2000, p. 1268). Para o autor, existe uma espécie de "intuição social" que faz com que sujeitos em geral suponham que suas escolhas privadas são diferentes, por natureza, das escolhas feitas pelo Estado (Shiff Berman, 2000, p. 1288). Para ele, esses argumentos são ilógicos, porquanto público e privado advêm do mesmo Estado legislador. Ainda assim, é interessante observar que a mesma "intuição social", a qual ele se refere, é aquela sustentada pelo ideal ciberlibertário de que, no ciberespaço, o Estado e o direito público jamais conseguiriam fincar raízes. Para o autor, o poder simbólico que emana da Constituição (e do Direito como corpo uno) serve como uma espécie de veículo de memória social, um sustentáculo da coletividade. E, não obstante defenda o Direito Constitucional como respaldo teórico e técnico para pensar o ciberespaço, diversamente da abordagem sistêmica e administrativista de Douek, ele está em consonância com os demais autores utilizados neste trabalho ao defender que, no ciberespaço, o direito de livre manifestação das ideias é inegociável muito mais por questões culturais do que legais (Shiff Berman, 2000). Em retorno a Douek:

> Porque moderação de conteúdo envolve liberdade de expressão, e porque muito do debate acadêmico e prático sobre moderação de conteúdo tem sido dominado por profissionais do direito, tal discussão é permeada por analogias àPrimeira Emenda. Tais analogias têm sido persistentes, mesmo depois de a burocracia envolvendo a moderação de conteúdo tê-las ultrapassado em importância. Essas analogias, e o modelo padrão que as envolve, se respaldam em pressuposições equivocadas sobre a natureza necessária da governança da liberdade de expressão. Tal entendimento assume que: (1) matérias que envolvem liberdade de expressão são especiais e particularmente resistentes à governança sistêmica; (2) intervenções *ex post* no estilo judicial devem ser individualizadas; (3) perfeição é necessária e desejável na regulação da liberdade de expressão [tradução nossa] (Douek, 2022, p. 556).

Ao sugerir que a liberdade de expressão seja desmistificada e garantida de modo apropriado à sociedade informacional, Douek não está sozinha. Outros autores e pensadores do Direito na era digital igualmente se aventuram a defender ideias de teor semelhante. Cass Sunstein, por exemplo, é categórico ao afirmar que a "liberdade de expressão, propriamente dita, não é absoluta" (Sunstein, 2017, p. 192). O autor inicia por exemplificar que o governo *já* regula inúmeras searas da vida pública na internet, as quais em boa medida sequer são percebidas pelos mais ferrenhos ciberlibertários. Direito de propriedade, crimes cibernéticos, difusão e circulação de vírus e *malwares* são apenas alguns exemplos de atividades *online* atualmente controladas pelas autoridades. Isso, para o autor, evidencia o quanto regulações estruturais, via de regra, não são questionadas pelos paladinos da liberdade de expressão - desde que não envolvam o controle direto sobre os discursos e apenas garantam o bom funcionamento

dos mercados. No entanto, quando a interferência do governo se volta para eventos como "reservar tempo no ar para propaganda eleitoral, ou garantir que a programação para crianças mantenha padrões mínimos de qualidade" *(*Sunstein, 2017, p. 195)*,* pululam arguições de que a Primeira Emenda estaria a ser violada. Para Sunstein, a fim de esclarecer o porquê de tal diferenciação, é fundamental que se separe o joio do trigo, por meio do estabelecimento das diferenças entre o princípio da livre manifestação das ideias proclamado nas cortes e o princípio da livre manifestação das ideias vigente no debate público. O exercício proposto por Sunstein faz com que se aproxime, mais uma vez, da ideia de Paul Shiff Berman de que há uma "intuição social" que faz com que se creia que público e privado consistem em esferas apartadas, enquanto, na verdade, elas se confundem a todo tempo (Shiff Berman, 2000).

A era da sociedade informatizada tem demandado muito de interpretações constitucionais envolvendo a liberdade de expressão. Tanto é assim que, compreendendo a complexidade e crueza do fenômeno que ora vivemos, as cortes de modo geral têm sido prudentes para fixar regras que digam com a livre manifestação das ideias, voltando-se muitas vezes à apreciação casuística comentada por Douek (2022) - como é o caso da Suprema Corte dos Estados Unidos. Tal conjuntura, no entanto, em nada refreia os debates sobre a liberdade de expressão que ocorrem nos espaços públicos, e alcança a sociedade civil de modo geral. Nessa última, a liberdade de expressão tem vida livre e é constantemente invocada, quase sempre de modo a desencorajar iniciativas do governo voltadas a regular o mercado de comunicação digital. Como ressalta o próprio Sunstein, "fora das cortes, dentro dos escritórios de lobistas, jornais, estações de rádio, e estúdios de gravação, bem como em residências familiares, a Primeira Emenda tem uma grande presença cultural" (Sunstein, 2017, p. 196).

A inadequação das cortes para resolver algumas demandas e a insuficiência de interpretações constitucionais são explicitadas em exemplo histórico aportado pelo autor. Nesse, Sunstein relembra o uso da Décima Quarta Emenda no século XX, para impedir que o governo norte-americano regulasse o mercado de trabalho (por meio de regras como a fixação de pisos salariais ou tetos de carga horária, por exemplo). Na ocasião, a Suprema Corte entendeu que as intervenções da administração pública eram ilegítimas e que a constituição norte-americana permitia que empregados e empregadores contratassem entre si *do modo qual melhor entendessem.* O caso, descrito por Sunstein como "grotesco abuso de poder" (Sunstein, 2017, p. 200), traz à tona a inadequação de soluções judiciais para temas que são de relevância democrática, bem como a confusão que se erige entre direitos fundamentais e direitos de consumo e contrato, em que as fronteiras entre público e privado não poderiam ser mais

borradas. No que se relaciona com os debates hodiernos sobre o princípio da liberdade de expressão, opera-se movimento semelhante. O debate público que entende que tudo é dizível em nome da livre manifestação das ideias, assim como a isenção com que se trata plataformas por meio das quais circulam os discursos, confunde mais e mais a liberdade de expressão com a ideia de soberania do consumidor (em uma simbiose na qual, novamente, é difícil saber onde começa o público e onde termina o privado). Tal combinação não apenas distorce a concepção constitucional do que é a liberdade de discurso, impedindo que alcance as demandas próprias da era digital, como também acaba por contaminar bases democráticas.

Em que pese seja taxativo ao afirmar que a liberdade de expressão não é absoluta, Sunstein faz algumas ressalvas. Para o autor, é fundamental que se estabeleça uma distinção entre os diferentes tipos de discursos, separando os discursos daninhos dos relativamente inofensivos. Na apreciação proposta pelo autor, fatores conjunturais devem ser, a todo tempo, levados em conta. O cerne do movimento de compreender os limites do controle e da liberdade dos discursos na internet, desse modo, deve ser o comprometimento com a ordem democrática, premissa que serve a proteger a liberdade de expressão tanto de agentes privados quanto públicos (Sunstein, 2017, p. 200-205). De modo semelhante, Lessig já alertara para isso, nos anos 90, ao propor que encontrar o espírito da constituição norte-americana deveria ser o objetivo no processo de aproximação entre o direito e o ciberespaço (Lessig, 1996).

As questões aqui tratadas sobre regulação do ciberespaço, o uso do direito administrativo, e os modos pelos quais a liberdade de expressão tende a se relacionar com o controle de conteúdo no ambiente virtual integram um quadro maior, no qual estão retratadas as disputas políticas e econômicas em jogo no processo de regulação de plataformas mundo afora. Resta, então, explorar outro elemento de relevância desse quadro. Não há dúvidas, as ora denominadas *bigtechs* possuem papel ímpar em tal conjuntura, longe de desprezível. Elas influenciam, cada vez mais, os caminhos regulatórios elegidos por governos tradicionais, de forma que refletir sobre seu *modus operandi* é elementar para a crítica que aqui se constrói. É sobre esses agentes que ora se passa a discorrer.

2.5 Bigtechs: novos impérios na era da sociedade informacional.

Concomitantemente à discussão envolvendo a liberdade de expressão e os limites para interferência dos governos nos discursos, outro movimento, em paralelo, imiscuiu-se no

debate sobre o controle de conteúdo nas redes: o modo como plataformas reproduzem mecanismos ancestrais de organização estatal e a forma como governos tradicionais têm se relacionado com esse crescente poder. O fato de plataformas se comportarem cada vez mais como novos governos é percebida por diversos autores e atores, Douek inclusive, e são muitas as menções a esse fenômeno. "Seria a Microsoft uma nação digital e teria ela um secretário de Estado?", indagou a *The Economist* (The Economist, 2019). "Quem precisa de governo quando se tem a *Amazon* para manter as coisas em ordem?" (Naughton, 2020), provocava um editorial do *The Guardian.* Mesmo Mark Zucherberg, em entrevista à VOX, declarou que "sob muitos aspectos, o Facebook é mais um governo do que uma empresa tradicional" (Farrel; Levi e O'Reilly, 2018). A incorporação de atributos estatais pelas *bigtechs* é alvo de recente obra de Vili Lehdonvirta, professor no *Oxford Internet Institute,* o qual, em setembro de 2022, lançou o livro *Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control.* Na obra, Lehdonvirta reconstitui, com enorme fôlego, a trajetória histórica de grandes plataformas da internet, desde seu passado de inspiração em Barlow até a adoção de mecanismos de organização estatal por parte das *bigtechs*. Uma vez que a estruturação institucional das plataformas é elemento chave para compreender as dificuldades e possibilidades envolvidas na regulação de conteúdo, é interessante comentar, ainda que brevemente, sobre a obra de Lehdonvirta e os percursos históricos por ele narrados.

O autor inicia sua reflexão resgatando propostas originais e liberais de plataformas como eBay, Silk Road[8], e Upwork, todas elas frutos de empresários simpatizantes das bandeiras ciberlibertárias e da EFF[9]. Ao reconstruir suas trajetórias, Lehdonvirta se esforça por demonstrar com minúcia que, embora os projetos originais de seus criadores fossem inspirados em ideais libertários, partidários da ideia de que governos tradicionais não alcançariam ou teriam serventia no ciberespaço, a popularização e o crescimento de suas plataformas os conduziram a adotar mecanismos que reproduziam instituições estatais. No caso do eBay, criado originalmente por Pierre Omidyar com a proposta de "unir compradores e vendedores em um *marketplace* honesto e aberto"[10], o crescimento inesperado da comunidade de usuários

[8] Originalmente, a *SilkRoad* foi disponibilizada na *darkweb* para comercialização não rastreável de produtos, sobretudo entorpecentes e outras mercadorias ilícitas. Embora se tratasse de rede em boa medida diferente de plataformas comerciais padrão, ela representa excelente exemplo de rede criada sob aspirações liberais que, com seu crescimento, teve de passar a se valer de mecanismos institucionais estatais para manutenção da ordem.
[9] A Electronic Frontier Foundation (EFF) é um grupo internacional de direitos digitais sem fins lucrativos, com sede em San Francisco, Califórnia. Fundada em 1990 por John Gilmore, John Perry Barlow e Mitch Kapor, tem por escopo a promoção das liberdades civis na Internet. Disponível em https://www.eff.org/about. Último acesso 18/06/2023.
[10] Nos termos utilizados pelo próprio eBay. Disponível em https://www.ebayinc.com/company/our-history/ Último acesso 03/05/2023.

da plataforma fez com que Omidyar se deparasse com a ameaça à credibilidade de seu *site*. Isso pois a falta de retidão de compradores e vendedores, fraudes e comércio de produtos ilegais espalharam-se qual rastilho de pólvora pelos anúncios da plataforma. Ante a iminente desordem, os responsáveis pelo eBay (à época ainda chamado *AuctionWeb*) viram-se obrigados a introduzir regras de comércio - a exemplo de ferramentas de controle de qualidade, procedência de produtos e até mesmo punições a usuários que não cumprissem com as políticas estabelecidas pela empresa. Em resumo, passou a responder de maneira semelhante a qual Estados modernos fazem diante de falhas de mercado (Lehdonvirta, 2022). Nas palavras de Lehdonvirta:

> Alguns colecionáveis só poderiam ser listados se sua autenticidade fosse antes certificada por uma empresa de classificação pré-aprovada. Alguns itens eram restritos a vendedores pré-aprovados; o eBay contratou a *Butterfield & Butterfield* - uma tradicional casa de leilões de San Francisco - para produzir inventários. (...) introduziu uma linha direta para marcas como Louis Vuitton, Disney e Microsoft para denunciar itens falsificados. Alguns produtos de alto risco, como medicamentos prescritos, não podiam mais ser anunciados. Com o tempo, o eBay introduziu dezenas de documentos de política estabelecendo as regras pertencentes a diferentes categorias de produtos, como “Política de álcool”, “Política de alimentos”, “Política de armas de fogo” e “Política de ações e outros valores mobiliários”. A "política de segurança do produto" explicava as consequências aos infratores da seguinte forma: A atividade que não segue a política do eBay pode resultar em uma série de ações, incluindo, por exemplo: encerrar ou cancelar listagens administrativamente, ocultar ou rebaixar todas as listagens dos resultados de pesquisa, rebaixar o vendedor classificação, restrições de compra ou venda e suspensão de conta [tradução nossa] (Lehdonvirta, 2022, p. 50).

De modo semelhante, a *Silk Road*, mercado aberto criado por Ross Ulbricht para comercialização anônima e não rastreável de qualquer tipo de produto, sobretudo entorpecentes e outros ilícitos, viu-se em falta de mecanismos que espelhassem instituições estatais modernas ante o crescimento da plataforma, especialmente para fins de identificação de seus membros. A *Silk Road* foi originalmente pensada para permitir que usuários anônimos comercializassem na *dark web* de modo não rastreável pelas autoridades norte-americanas (endereços e dados de compradores e vendedores eram automaticamente destruídos após a confirmação de cada transação, não sendo detidos nem pelo próprio Ulbricht; além disso, a plataforma rodava em navegador *Tor,* e as transações eram feitas em *Bitcoins*). No entanto, o crescente número de fraudes, inadimplência, e outras incorreções dos usuários fez com que Ulbricht passasse a impor uma série de entraves de *design* voltados a garantir a lisura das transações - a exemplo de depósitos de caução e avaliações de reputação. Ainda assim, a política de privacidade absoluta seguiu a todo tempo em vigor. Isso porque Ulbricht via na *Silk Road* verdadeiro "potencial para uma mudança monumental na estrutura de poder do mundo", e uma ferramenta por meio da qual "as pessoas poderiam controlar o fluxo e a distribuição de informação e de

dinheiro de forma a fazer com que, setor por setor, o Estado seja cortado da equação e o poder seja devolvido aos indivíduos" (Lehdonvirta, 2022, p. 59).

A situação, no entanto, se agravou com a chegada de chantagens de um determinado usuário, autodenominado *FriendlyChemist.* Esse sujeito, tendo participado de diversas transações de vendas de narcóticos, coletou e registrou nomes e endereços de centenas de compradores (banco de dados que, como política do *site*, não era mantido em lugar nenhum). Sob ameaças de divulgar tais informações, *FriendlyChemist* passou a exigir pagamentos de Ulbricht em troca de seu silêncio. Em reação à extorsão, o fundador da *Silk Road* se esforçou por desvelar a identidade *no mundo real* do vendedor que o intimidava, a tal ponto que, segundo investigações do FBI, chegou a encomendar que a pessoa que lhe extorquia fosse assassinada[11]. Ao final de dois anos, Ulbricht foi identificado pelo FBI, julgado, e cumpre prisão perpétua nos Estados Unidos. Explorar os pormenores dessa história não cabe ao presente trabalho.

Narrados os fatos, e posto de lado seu teor infausto, a história da *Silk Road* é utilizada por Lehdonvirta para deflagrar a importância da identificação padronizada e os desafios que uma política de privacidade absoluta no ciberespaço pode acarretar. O caso permite que se observe como a ideia de um mercado aberto, totalmente desprendido da autoridade estatal, espontaneamente manifestou a necessidade de identificação dos indivíduos para manutenção da ordem, ainda que por intermédio de pseudônimos. Desmantelada a *Silk Road* original, dezenas de outros *sites* de finalidade semelhante pulularam na *dark web.* Desde então, eles vêm estimulando usuários a vincularem suas identidades virtuais a diferentes sites de comercialização de ilícitos, em clara reprodução de bancos de registro civil estatais. Do mesmo modo, plataformas populares da *world wide web* operam através da atribuição, a cada usuário, de identificação individualizada, via de regra vinculada entre várias plataformas ou à conta de e-mail de cada indivíduo (Lehdonvirta, 2022). Nas palavras do autor:

> À medida que mais e mais aspectos da vida cotidiana e dos negócios fluem pelas plataformas que eles operam, as identidades que eles nos atribuem se tornam muito mais importantes e dolorosas de perder. Embora eles não reivindiquem domínio sobre nossos corpos físicos como os estados territoriais, nossas identidades virtuais – as identidades que cada vez mais importam – estão inteiramente em suas mãos [tradução nossa] (Lehdonvirta, 2022, p. 69).

[11] Não há indícios que tal assassinato tenha de fato ocorrido, uma vez que nenhum homicídio foi registrado ao tempo e nas imediações onde a execução consentida por Ulbricht deveria ter ocorrido. Ainda assim, as mensagens, nas quais foram combinados os assassinados, foram efetivamente trocadas entre Ulbritcht e sujeitos que se vendiam como sicários. O que se supõe que tenha ocorrido é que tenham consistido em conspiração e farsa promovida por usuários, meramente para fins de extorsão (Lehdonvirta, 2022).

Por fim, resta comentar o caso da plataforma *ODesk,* a qual deu origem a atual *Upwork*. Criada com o objetivo de aproximar profissionais e contratantes a nível global para prestação remota de serviços, a *ODesk* tinha por lema atuar de forma independente de regras trabalhistas, imigratórias ou tributárias das diferentes jurisdições. Trocando em miúdos, a *ODesk* trazia em seu seio a ideia de fazer desaparecer os efeitos das fronteiras políticas para fins de prestação de serviços. A proposta de globalização virtual, que de largada ganhou enorme popularidade, logo teve de enfrentar disparidades e revezes derivados de sua própria estrutura de funcionamento, como ocorre em qualquer mercado de trabalho no mundo físico. Inicialmente, fatores culturais e de mercado fizeram com que profissionais que ostentavam em seus currículos experiências em instituições renomadas recebessem mais e melhores ofertas, especialmente em comparação às ofertas recebidas por profissionais tão qualificados quanto, porém advindos de regiões mais pobres do globo. A discrepância logo foi amenizada com a possibilidade de todos os profissionais e contratantes listados receberem testemunhos e avaliações públicas sobre os serviços por eles prestados no âmbito da plataforma. Ainda assim, a organicidade do mercado de trabalho seguiu criando novas disparidades. Tratando-se de listagem internacional de prestadores de serviço, logo se observou um deslocamento das contratações para onde o valor por empreitada era menor. Uma vez que o custo de vida varia enormemente a depender do país, e estando a *ODesk*, por sua feição, desobrigada a observar salários-mínimos e regulações nacionais, a dessemelhança entre os preços para a contratação de um mesmo serviço em diferentes locais acabou por privilegiar *freelancers* de um lugar e desprivilegiar profissionais de outro, a exemplo do aumento dos contratos com profissionais da Índia e esvaziamento dos serviços contratados na Nigéria (Lehdonvirta, 2022). Além disso, o recolhimento pela *ODesk* de percentil por cada serviço contratado acabou afastando os trabalhadores mais qualificados e uma parcela dos clientes, não à toa os mais endinheirados, os quais buscavam justamente esses últimos *experts*.

Para manter a harmonia do mercado proposto pela plataforma, e a fim de garantir a oferta de profissionais bem qualificados e bem pagos, mostrou-se necessária a adoção de regras de funcionamento. Em agosto de 2014 a *Elance-ODesk*[12] anunciou a criação de um piso por hora contratada. Esse piso, ainda que baixo (apenas US$3,00 a hora), era bastante significativo para uma empresa que se propunha a fugir das imposições de regulações trabalhistas nacionais. Mesmo o discurso dos dirigentes da plataforma se revelou mudado a esse tempo. Declararam

[12] Em 2013 a *ODesk* foi fundida à concorrente *Elance*, dando origem à *Elance-ODesk*. Em 2015 a empresa foi rebatizada sob o nome *Upwork*, pelo qual é conhecida até os dias atuais. Disponível em https://en.wikipedia.org/wiki/Upwork Último acesso 05/06/2023.

eles: "nosso desejo é nos tornarmos o maior e mais confiável mercado de trabalho online do mundo, conhecido por nossos talentos e serviços de ponta, (...), e o mínimo por hora irá beneficiar nossa comunidade como um todo" (Lehdonvirta, 2022, p. 86). Com o tempo, outras ferramentas de controle passaram a ser oferecidas pela plataforma. Como exemplos, houve a criação de centro de resolução de disputas, nos moldes de um tribunal de arbitragem; a possibilidade de penhora de valores negociados por intermédio da plataforma para quitação de débitos; e mesmo a implementação de controle de entrada de novos usuários, o que muito se assemelhava a políticas migratórias de Estados Nação tradicionais (Lehdonvirta, 2022, p. 90).

Naturalmente, as medidas postas pela *ODesk* a seus usuários diminuíram alguns problemas e deram origem a outros - como ocorre com qualquer regulação, em qualquer mercado de trabalho -, e sobre esse ponto não há nada de especial. O caso, contudo, é emblemático desde o ponto de vista da emulação de instituições estatais pela plataforma, especialmente em decorrência da reelaboração da territorialidade, dessa vez transportada ao ciberespaço. Vale lembrar, aqui, que uma das propostas iniciais da *ODesk* consistia justamente na transposição de entraves decorrentes das delimitações político-territoriais nacionais em seus respectivos mercados de trabalho. Nesse propósito, de fato, a empresa obteve sucesso. Todavia, para concretizar seu intuito, foi necessário que recriassem instituições modernas para ordenação coletiva – como é o caso dos centros de resolução de disputas, ou das regras para acesso de novos usuários. "No final, eles conseguiram chegar aonde queriam não através da eliminação da importância da territorialidade como tal, mas sim através da substituição do território físico por uma espécie de localização virtual" (Lehdonvirta, 2022, p. 89). Ainda que não trate abertamente sobre a delimitação espacial do mercado de trabalho criado pela *ODesk/Upwork*, "instituições formais como tribunais, regulamentos e normas implicam distinções nítidas entre aqueles que estão dentro e aqueles que estão fora". Em suma, "ao criarem versões digitalizadas de instituições modernas, as plataformas acabaram por recriar também fronteiras" (Lehdonvirta., 2022, p. 90).

Os casos do *Ebay*, *Silk Road* e *ODesk* servem para ilustrar como, ao fim e ao cabo, todas as plataformas que tiveram sucesso na construção de "megalópoles virtuais" assim o fizeram por meio da criação de regras e instituições formais internas. Elas assumiram, para si próprias, "o papel da autoridade coercitiva que tanto se empenharam em abolir" (Lehdonvirta, 2022, p. 205). Segundo o autor

> [...] quatro forças em particular moldaram a evolução da estrutura institucional do mercado eletrônico desde os anos 1980 até os dias de hoje. Primeiro, o

> desafio de manter a ordem social. Segundo, o problema da escala. Terceiro, a economia de escopo. E, por quarto, o poder sedutor do planejamento central [tradução nossa] (Lehdonvirta, 2022, p. 206).

Essas forças, segundo Lehdonvirta, impeliram a organização das plataformas de modo bastante semelhante ao ocorrido quando da ascensão dos Estados-Nação, nos séculos XVIII e XIX, quando a centralização da administração pública e o uso da violência legítima pelo Estado consolidou instituições estatais modernas até hoje vigentes. A proposta central da obra de Lehdonvirta – incutida no título do livro, de que plataformas digitais estão tomando o lugar do Estado -, assim deriva da reimplementação, por parte de grandes portais *online*, da mesma ordem estatal centralizadora que Barlow e os ciberlibertários acreditavam que seria revolucionada pela internet.

O desafio de manter a ordem dentro do ambiente virtual disponibilizado por cada plataforma é possivelmente o aspecto mais evidente no argumento de Lehdonvirta. Em seu gérmen, plataformas em geral – desde o *eBay* ao *Facebook* - eram menores e, naturalmente, mais fáceis de administrar. Com o crescimento dessas comunidades, no entanto, e novamente de modo análogo à conformação das cidades modernas, o gerenciamento da ordem social se tornou necessariamente mais complexo e passou a demandar intervenções de quem detivesse autoridade ou poder para isso. É nesse último ponto que reside o que o autor chamou de "o problema da escala". No tocante à economia de escopo, os exemplos são os mais variados, e seu auge está retratado na crescente concentração de mercado pelas *bigtechs*. Em que pese se trate de fenômeno mais facilmente perceptível hoje em dia – com a compra de concorrentes pela *Meta* ou a expansão de nichos de mercado pela *Amazon*, por exemplo –, o engendramento de uma economia de escopo no ciberespaço acontece, paulatinamente, desde os primórdios de grandes plataformas. O aumento dos lucros por meio dessa engrenagem guarda próxima relação com o controle interno praticado por seus dirigentes. Por fim, o referido "poder sedutor do planejamento central", torna-se autoexplicativo em vista da conjuntura de expansão de plataformas. Nos termos de Lehdonvirta, ao se referir à nova ordem engendrada pelos gigantes da internet: "ao invés de revolucionarem a ordem social, eles acabaram por reimplementá-la com código de computação e agentes de atendimento ao consumidor" (Lehdonvirta, 2022, p. 210).

O autor elenca dois motivos principais para que plataformas tenham tido o sucesso que hoje se percebe. Por primeiro, o fato de governos em geral, na virada do século XXI, terem repassado o processamento de dados públicos a agentes privados. "Reino Unido, Austrália, e muitos outros países terceirizaram quase todas as funções de tecnologia da informação do

governo para fornecedores privados de tecnologia" (Lehdonvirta, 2022, p. 211). Concomitantemente, plataformas aproveitaram essa janela de oportunidade para fazer o movimento oposto e trazer para dentro de seu círculo administrativo direto desenvolvedores e administradores de sistemas. Desse modo, com a massificação do número de usuários da internet nos anos seguintes, plataformas privadas estavam preparadas para angariar esses mercados e fornecer melhores serviços, especialmente em comparação com o poder público em geral. O segundo motivo apontado reside no fato de que as *bigtechs*, não obstante emulem mecanismos estatais, não estão vinculadas ao comportamento exigido de agentes de direito público e são livres para administrar usuários de modo menos democrático do que governos tradicionais.

> O *Uber* pode desativar motoristas com muito menos provas e devido processo do que um Estado precisaria para revogar uma licença de táxi. Os administradores da *Apple* podem aplicar as regras da *App Store* seletivamente quando for conveniente para a empresa. O *Amazon Mechanical Turk* pode permitir que clientes escapem impunes do abuso de trabalhadores digitais, se isso ajudar a economia deles a crescer. (...) As instituições econômicas das plataformas podem ser bastante modernas, mas em termos de instituições políticas – incluindo direitos individuais – elas permanecem na idade das trevas. Isso permite que plataformas concorram com instituições estatais com estruturas institucionais de baixo custo, que priorizam a conveniência sobre a justiça e a dignidade [tradução nossa] (Lehdonvirta, 2022, p. 212).

A despeito do poder colossal que hoje se concentra nas mãos das plataformas, Lehdonvirta indica possíveis saídas para que o ciberespaço sirva melhor ao bem comum, e para que o movimento de tomada de espaço do Estado por parte das plataformas seja refreado. De início, ele reconhece que a mera incidência de regulação de concorrência, nos moldes da *Guilded Age*, não seria totalmente eficaz. Uma vez que os serviços oferecidos pelas plataformas são muitíssimo diversificados, eles não se tratam de *commodities* estrito senso. Ainda que fossem implementadas políticas antitruste horizontais, trocar de plataforma não é tão simples, para um usuário comum, quanto trocar de posto de combustível – mais uma vez, economia de escopo. Isso pois a escolha da plataforma a ser utilizada não é uma escolha individual, e sim coletiva. O autor reconhece, no entanto, que a quebra vertical da cadeia empresarial das b*igtechs* pode ser eficaz, baseado na proposta de Lisa Khan, *chairwoman* na *Federal Trade Commission* (FTC) recentemente indicada por Joe Biden[13]. Não obstante as forças econômicas e sociais que conduziram a constituição das plataformas tenham, no presente, atingido enorme

[13] Lisa Khan é autora do polêmico artigo "*Amazon's Antitrust Paradox*". Nesse, ela afirma que a atual estrutura da lei antitruste americana, que se concentra em manter preços ao consumidor baixos, não pode explicar os efeitos anticompetitivos de modelos de negócios baseados em plataforma, como o da *Amazon* ou da *Meta,* em crítica ao livro *The Antitrust Paradox*, de Robert Bork, 1978. A indicação de Khan para a FTC foi contestada pela *Amazon* e pelo *Facebook*, sob pleito de que seu passado crítico às companhias a impediam de manter conduta imparcial. Tais pleitos, no entanto, foram afastados pela própria FTC.

solidez, as facetas políticas que moldaram e moldam as *bigtechs* "são muito mais maleáveis" (Lehdonvirta, 2022, p. 219). Assim sendo, a imposição de separação de funções administrativas e nichos de mercado, dentro das gigantes do ciberespaço, tende a tornar suas atividades mais transparentes. Evelyn Douek (2022) propõe algo parecido ao dizer que as funções regulatórias e administrativas das plataformas deveriam ser separadas "por uma parede".

A regulação antitruste vertical, todavia, não resolve outros possíveis abusos por parte das plataformas, a exemplo de taxas extorsivas, tratamento preferencial para parceiros e regras injustas ou negligentes que resultam em más condições de trabalho. Para Lehdonvirta, a "raiz do problema permanece: o mercado é governado por tecnólogos bilionários e capitalistas de risco cujos interesses divergem dos interesses das pessoas e empresas que povoam as plataformas" (Lehdonvirta, 2022, p. 223). O autor defende que fontes abertas ou uma maior possibilidade de participação dos usuários nas decisões sobre os rumos a serem tomados pelas diferentes plataformas são interessantes para enfrentar o problema, porém limitados. A experiência passada é prova de que alguma ordem imposta de cima é necessária, diversamente do que defendia Barlow (1996). Lehdonvirta assume que a regulação ferrenha, a ponto de nacionalizar "*de facto*" plataformas, surtiria efeitos positivos sobre o processo de agigantamento de *bigtechs* sobre os Estados. Em contrapartida, a julgar pelo fato de que a esmagadora maioria das plataformas está sediada nos Estados Unidos ou na China, ele entende que a nacionalização também tenderia a concentrar enormemente os poderes desses dois países sobre o ciberespaço. Isso tampouco seria uma solução razoável ou interessante para outros atores internacionais que não China ou Estados Unidos. Além disso, o autor alerta para o fato de que, caso regiões "pobres em plataformas", como é o caso do bloco europeu, passassem a buscar alcançar a "soberania digital" por meio de regulação rigorosa, uma "corrida geopolítica em direção ao nacionalismo de plataforma" poderia ser desencadeada, o que igualmente não seria vantajoso para a maior parte dos países (Lehdonvirta, 2022, p. 222 – 227)[14].

Diante do impasse, o autor se volta a defender que plataformas sejam reconhecidas como espaço de uso público (embora admita que seu caráter transnacional não permita - ou, ao menos em boa medida, intimide - que um poder externo as governe ou dirija). Novamente, aqui o debate se depara com a importância de relativizar o oxímoro existente entre direito público e

[14] "De acordo com um estudo, as cinco principais cidades-plataforma por valor estimado da empresa são: São Francisco, Seattle, Pequim, Hangzhou e Shenzhen. Apenas 15% das empresas-plataforma estão sediadas na Europa, representando apenas 4% do total valor de mercado. A única cidade europeia a figurar entre as dez primeiras é Walldorf, na Alemanha, sede da gigante do software empresarial SAP. Ele ocupa o sétimo lugar, logo após Tóquio" (Lehdonvirta, 2022, p. 227).

privado. Ao mesmo tempo, se firma a necessidade de encarar o ciberespaço como espaço público, a despeito de seus traços de direito privado, em moldes muito semelhantes ao que defenderam Lessig (1997) e Shiff Berman (2000). Com isso, Lehdonvirta afirma que a implementação de governança democrática e cooperativa, conferindo poder de voto aos usuários, é desejável e factível. Não se trata de retirar o poder vinculativo de aplicação das regras do agente privado, já que esse seguiria concentrado junto a dirigentes das plataformas, mas sim de descentralizar o sistema de produção das normas que regem o ciberespaço e ceder espaço de fala aos usuários. Em clara extensão do movimento de apropriação de mecanismos e instituições próprias do Estado moderno, agora visando à democratização e a separação entre os Poderes no ciberespaço, o autor afirma que

> Não há nenhuma lei da história que diga que essas forças vencerão e que as plataformas digitais inevitavelmente emergirão como democracias – longe disso. Mas as forças políticas são maleáveis, dependendo de quão organizados ou difusos são os vários grupos de interesse. Isso significa que os formuladores de políticas territoriais hoje têm outra opção política diante deles enquanto ponderam como lidar com os crescentes abusos das empresas de tecnologia: além de quebrar, regulamentar e nacionalizar plataformas digitais, os formuladores de políticas podem apoiar sua democratização [tradução nossa] (Lehdonvirta, 2022, p. 232).

Indo a fundo na analogia com a qual conduz sua obra, o autor indica o surgimento de quatro diferentes classes de sujeitos presentes nas plataformas - admitidamente com alguma licença criativa. Seriam esses: [1] os aristocratas, no topo; [2] os usuários ordinários, como base; [3] os trabalhadores ordinários, a exemplo de moderadores, rotuladores de dados ou assistentes virtuais, sem grande poder de influência; [4] e o surgimento de espécie de burguesia da internet, representada por desenvolvedores de *softwares* de sucesso, mercadores, influenciadores e outros atores que galgam capital social suficiente para se fazer ouvidos no ciberespaço. Esses últimos, sim, com maior potencial de influência (Lehdonvirta, 2022, p. 230-237). Tal organização social das comunidades do ciberespaço reproduz, mais uma vez, a fluidez comunicacional e de trocas que está na gênese da cidade moderna, aquela mencionada por Cass Sunstein (2017). Ao mesmo tempo, essa organização social reforça a plausibilidade de que outros atores sociais tenham voz na constituição das normas que regem as relações no ciberespaço - em movimento similar ao descrito abstratamente por Murray, no comunitarismo de rede -, possibilitando a atribuição de compromissos sérios com direitos fundamentais por parte das *bigtechs*. Para Lehdonvirta, o fato de que plataformas assumem funções estatais, de maneira mais barata e prática que os próprios Estados, ocorre justamente porque *bigtechs* não estão compromissadas com direitos básicos, claros e previamente instituídos. Nos termos do autor:

> conforme discutido anteriormente, uma das razões pelas quais plataformas são capazes de realizar tarefas administrativas semelhantes às do Estado de forma mais rápida e barata do que o próprio Estado é a falta de compromisso com os direitos básicos. À medida que a regulamentação da UE empurra os termos de serviço das plataformas para um status semelhante à constituição, completo com revisão judicial, elas começam a funcionar como uma fonte de direitos básicos que limitam o exercício do poder dos governantes da plataforma contra seus usuários, assim como as constituições limitam os estados ' poder. O jurista Nicolas Suzor chama essa ideia de "constitucionalismo digital". Por enquanto, os direitos constitucionais dos usuários permanecem muito limitados. Mas o mecanismo para ampliá-los nesse quadro é claro: alterar os termos de serviço. Assim, voltamos à questão de quem escreve as regras da plataforma em primeiro lugar. Transparência, estado de direito, revisão judicial e direitos básicos oferecem, na melhor das hipóteses, consolo temporário ao abusado, desde que o abusador possa mudar as regras à vontade" [tradução nossa] (Lehdonvirta, 2022, p. 234)

A proposta teórica joga, a todo tempo, com a maleabilidade política das plataformas, em contrapartida ao rigor com que conduzem seus interesses econômicos. O autor defende que, muito embora seja quase impossível refrear as engrenagens pró-lucro das *bigtechs* – vivemos em modo de produção capitalista, afinal –, é possível que os governos tradicionais intervenham nas políticas que regem as plataformas, em tentativa de refrear a tomada de espaço do Estado por parte destas. Apesar de a "revolução burguesa" do ciberespaço se tratar de exercício de abstração, qual reconhece o próprio autor, a ideia de democratização política da governança de plataformas, pouco a pouco, ganha corpo em regulações mundo afora (Lehdonvirta, 2022). Como exemplo maior, até antes da promulgação do O*nlnie Safety Act*, tem-se a Lei dos Mercados Digitais (LMD) do bloco europeu. Na LMD, plataformas específicas foram designadas como *gatekeepers*, e deveres de cuidado especiais foram atribuídos a estas justamente em razão de sua relevância como ferramenta de uso público. A regulação europeia vai além, e obriga *bigtechs* a disponibilizarem termos de serviços em linguagem e formato acessíveis a usuários; veta que plataformas promovam seus produtos em detrimento de outros, a não ser que isto esteja expressamente previsto em seus termos de serviço; determina que critérios de busca sejam divulgados ao público; exige que punições sejam justificadas; e exige que sistemas de reclamação sejam disponibilizados a pessoas físicas e jurídicas, de modo transparente e previamente estabelecido. Em suma, garante direitos básicos aos usuários, de modo análogo ao que o Estado faz com relação a seus cidadãos. O *Online Safety Act* do Reino Unido, objeto deste trabalho, ataca a regulação das redes de forma semelhante. Tais normatizações, ainda que insipientes se comparadas à complexa proposta de democratização dos estados digitais erigidos pelas *bigtechs* feita por Lehdonvirta, representam o Estado de Direito se transportando para dentro das plataformas. A imposição de regras básicas para o funcionamento desses serviços representa exemplo prático da regulação indireta que, Lessig

previra, seria o modo mais eficaz de governos tradicionais manterem sua influência no ciberespaço (Lessig, 1997).

Vale recordar, nesse ponto, que Sunstein (2017) afirma que censura por parte das autoridades é uma das maiores ameaças às bases democráticas de qualquer Estado. O autor faz ressalva, no entanto, de que nem toda intervenção do governo deve ser vista como tal, senão o contrário. O resguardo de liberdades individuais depende de regras que, *sine qua non,* devem advir de quem detenha autoridade e legitimidade para isso. Garantir tais direitos básicos no ciberespaço é questão de constitucionalismo digital (Suzor, 2018), e aqueles que mais ferozmente reclamam as tentativas de regular os discursos, sob argumento de que se estaria a ferir a liberdade de expressão, são geralmente os que mais se beneficiam da ausência de regras nesta seara (Sunstein, 2017, p. 200). Jacob Rowbottom partilha deste mesmo posicionamento (Rowbottom, 2010). Partindo das propostas dos autores mencionados, é possível afirmar que as disputas que hoje observamos – entre reguladores vinculados aos governos tradicionais, atores privados ligados às plataformas, organismos internacionais e outros agentes dispersos – representam disputas por espaços de poder. Elas são, ao fim e ao cabo, fruto do esvaziamento do Estado e do ganho de relevância de outros atores no ciberespaço, o mesmo fenômeno aventado por Lehdonvirta. O cenário, a nível mundial, é complexo, e não há perspectivas de que a situação seja estabilizada em um horizonte próximo. Apesar disso, as análises do estado da arte da regulação e dos rumos que o processo vem tomando são não apenas possíveis, como são também frutíferas para o debate.

Em vista das reflexões e do aparato teórico aqui expostos, será iniciada, a partir deste ponto, a análise do cenário britânico para regulação da internet e moderação de conteúdo em plataformas.

3. Histórico da regulação de mídias digitais e do ciberespaço no Reino Unido: do *Communications Act* de 2003 ao *Online Safety Act.*

A *Internet Safety Strategy*[15] (ISS) (Estratégia de Segurança na Internet), lançada pelo governo britânico juntamente com a publicação do I*nternet Safety Strategy Green Paper* (ISSGP) (*Green Paper* da Estratégia de Segurança na Internet)[16], em outubro de 2017, foi a fagulha inicial do projeto administrativo que, hoje, se consolida no *Online Safety Act* (OSA). Entre um evento e outro, no entanto, muito se passou, e as mais diversas estratégias para regulação das atividades e das mídias circulantes o ciberespaço foram debatidas. Por se tratar de projeto amplo, multissetorial e multidisciplinar, o qual se esforça por pensar a relação do Direito e da Administração Pública com o ciberespaço nas mais variadas searas da sociedade britânica, a ISS dialoga com diferentes órgãos e marcos reguladores que a antecedem no tempo. Obviamente, as propostas lançadas pelo ISSGP e pela ISS não se produziram concomitantemente ao *green paper* e à estratégia de segurança. Essas propostas vieram, isso sim, na esteira de tentativas regulatórias anteriores, elaboradas e formalizadas conforme o uso das redes expandia sua importância no cotidiano da população do Reino Unido.

Como em tantos outros cenários, no espaço britânico as demandas geradas pela digitalização da vida em sociedade continuamente se sobrepõem, em velocidade, às ferramentas legais existentes, as quais não se mostram suficientes para enfrentar tais mudanças. Referido traço facilmente se nota em vista da atrapalhada trajetória regulatória percorrida naquele país desde o começo dos anos 2000. Por questões de recorte e espaço, não é pretensão deste trabalho esquadrinhar com o maior fôlego possível todo o histórico que tenta pôr em compasso lei e ciberespaço no Reino Unido. Ainda assim, especialmente em vista da atual proposta de regulação multisetorial, a qual trabalha por regular concomitantemente questões de concorrência, saúde, liberdade de expressão, alfabetização digital, entre outros, é relevante conhecer a conjuntura regulatória que antecedeu o OSA. De modo semelhante ao que ocorre no Brasil, no Reino Unido o controle de conteúdo se deu, até antes do OSA, por meio da combinação de autorregulação e controle judicial. Lá, diferentemente do que ocorre com veículos de comunicação tradicionais, provedores de internet não são automaticamente responsáveis pelo teor das informações que circulam ou são disponibilizadas por intermédio

[15] Estratégia de segurança na internet - tradução nossa.
[16] Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf. Último acesso 03/06/2023.

de suas plataformas, a não ser mediante descumprimento de ordem judicial expressa para remoção desses (Catley, 2023, p. 3).

O controle de conteúdo via autorregulação e análise judicial casuística, estanques ao fio dos anos, são consequência não apenas do descompasso entre lei e tecnologia da informação no Reino Unido. Eles são também resultado de uma sequência de propostas regulatórias malsucedidas para controle do fluxo de dados no ciberespaço. Nessa esteira, o OSA vem como tentativa de inovar no campo regulatório, apostando na imposição de deveres de cuidado, de transparência, e no empoderamento da autoridade reguladora como meios de amainar os efeitos do livre fluxo de dados no espaço virtual, bem como conferir maior durabilidade ao aparato legal britânico. Seu objetivo, assim, é devolver parte da ingerência dos espaços públicos virtuais ao Estado (Neudert, 2023). Os principais pontos da lei, a qual só há pouco ganhou assentimento real (em 26 de outubro de 2023), serão expostos ao final deste capítulo. Antes disso, é importante fazer breve incursão sobre os marcos legais que antecedem o novo projeto. Serão aqui comentados o *Communications Act de 2003* e o *Digital Britain Report*, a primeira geração de regulação com vistas ao controle do fluxo de dados *online* no Reino Unido. Na sequência, serão mapeados o *Digital Economy Act* de 2010 e o *Digital Economy Act* de 2017, principais marcos legais em vigor, até o OSA, para controle do fluxo de informação no ciberespaço britânico. Serão também apresentados o *Internet Strategy Green Paper* e o *Online Harms White Paper*, antessala dos projetos ora concretizados no *Draft Online Safety Bill* e no próprio *Online Safety Act*. Por fim, será esmiuçada a conjuntura de publicação do anteprojeto do OSA, o *Draft Online Safety Bill*, bem como os pontos que ora julgamos mais importantes para conhecer e refletir criticamente sobre a nova lei britânica.

3.1 *Communications Act* 2003, *Digital Britain Report* e a primeira geração da regulação das comunicações via internet no Reino Unido.

3.1.1 Do *Communications Act* 2003 ao *Digital Economy Act* 2010.

Na esteira do *Telecommunications Act* de 1996, dos Estados Unidos, em 2003 o Parlamento publicou o *Communications Act* (CA 2003), o primeiro esforço legislativo britânico para pôr sua regulação nacional em sintonia com o crescente uso de meios eletrônicos e digitais pelas mídias de comunicação em geral. Abrangente, a lei se propunha a abarcar

regulação de redes, serviços de comunicação eletrônica e uso de espectros eletromagnéticos; regulação de *broadcasting*, televisão e serviços de rádio; limitações de fusões entre grupos jornalísticos e outras empresas de mídia (Reino Unido, 2003). O extenso aparato legal ganhou destaque por três elementos em particular. Primeiro, em razão da facilitação promovida, àquele tempo, para aquisição e constituição de empresas de mídia. Em segundo, pela criação do *Office of Communications* (OFCOM), a autoridade de maior relevância no contexto regulatório de mídias na atualidade, e a qual será abundantemente comentada ao fio deste trabalho. Por fim, pela criminalização do envio de mensagens maliciosas através de redes públicas de comunicação eletrônica, em sua Seção 127 - possivelmente o trecho mais famoso da referida lei. Sobre esse último, é interessante notar que, embora o CA 2003 não trate de regulação de plataformas digitais (demanda sobre a qual pouco se falava no âmbito legislativo àquele tempo), ele serve para categorizar mídias sociais em geral como "redes públicas de comunicação eletrônica", tipificando condutas como o envio de mensagens ofensivas, indecentes ou ameaças por meio de tais redes, como se em praça pública ocorressem (Reino Unido, 2003, seção 127). O CA 2003 não traz qualquer definição do que vem a ser ofensivo ou indecente, e a apreciação dos casos enquadrados na Seção 127, como bem advertira Douek, é casuística e feita pelas cortes judiciais. Ainda assim, a lei representa gérmen regulatório no processo de transposição de condutas condenáveis para o ciberespaço, bem como é um exemplo consolidado de tentativas de replicar – sem sucesso – o *modus operandi* do mundo real no mundo virtual. No tocante ao OFCOM, a autoridade regulatória de maior importância no movimento britânico para regulação de plataformas digitais, foi no momento de sua criação que lhe foi atribuída competência para promover alfabetização midiática, mantida até os dias atuais como parte da *Internet Safety Strategy*[17] e do próprio OSA.

Ao comentar sobre a estrutura legal escolhida pelo Parlamento para o *Communications Act 2003*, Mike Feintuck e Mike Varney, ainda em 2006, reconheceram o potencial para modernização da regulação de mídias de comunicação no Reino Unido aportado pela lei. Chamaram a atenção, no entanto, para o fato de que o texto legal, ao se voltar quase que exclusivamente a questões de consumo, propriedade e exploração comercial de mídias, negligencia interesses públicos inerentes às funções de empresas de comunicação, pouco fazendo para reverter o "declínio do domínio público" nessas searas. Muito embora a criação do OFCOM tenha colocado o interesse dos cidadãos como seu principal dever (Feintuck e Varney, 2006, p. 59), na prática isso tendia a ter resultados mínimos desde a publicação do CA

[17] Ver em https://www.ofcom.org.uk/research-and-data/media-literacy-research. Último acesso 06/09/2023.

2003, haja vista a ausência de critérios claros de quais seriam esses interesses. Além disso, a extensa lista de compromissos com direitos consumeristas, antitruste e de pouca interferência das autoridades nas atividades das companhias de comunicação era seguidamente conflitante com a defesa do interesse público estrito senso. Mais importante do que isso, a ausência de uma hierarquia clara de deveres do órgão regulador e das empresas reguladas relegava a segundo plano o papel da mídia na democracia, bem como os interesses comuns dos cidadãos. Para os autores, as funções democráticas exercidas por meio das mídias de comunicação deveriam ser formalmente reconhecidas no CA 2003[18], de forma a impor a essas empresas deveres claros e cobráveis pelas autoridades reguladoras (Feintuck e Varney, 2006, p. 167-168). Em que pese os autores não estivessem a se referir às plataformas digitais, menos ainda nos moldes e dimensões nas quais as conhecemos na atualidade, é interessante observar que o papel fulcral das mídias na democracia e a atribuição de deveres em decorrência de seu poder há tempos permeiam os debates regulatórios das comunicações. No cenário britânico é somente agora, como há de se ver adiante com o OSA, que o pleito ganha a roupagem legal outrora recomendada por Feintuck e Varney.

3.1.2 *Digital Britain Report* e o *Digital Economy Act 2010.*

Em outubro de 2008, após consecutivas falhas para responder às demandas da era digital e da tecnologia das comunicações, o governo britânico lançou iniciativa intitulada *Digital Britain.* Com essa, o Parlamento visava a estudar e analisar as condições de infraestrutura das comunicações no Reino Unido, assim como as demandas da economia digital naquele Estado. Os resultados da iniciativa foram organizados e publicados no Relatório *Digital Britain* de 2009[19], o qual, a sua vez, serviu de embasamento para a elaboração do próximo grande ato regulatório britânico na área (Coulter e Negishi e Foskett, 2013, p. 26). Na sequência do *Communications Act*, foi publicada em 2010 a primeira versão do *Digital Economy Act* (DEA 2010), produzida com base nas diretrizes traçadas no *Digital Britain*, e

[18] Pesquisa consolidada em *command paper*, produzida e publicada durante o governo do Partido Trabalhista Inglês, unificando propostas de políticas públicas, em linhas gerais, para a adaptação do Reino Unido à era digital. Muito embora *command papers* sejam produzidos como guia para a atividade parlamentar, o legislativo não é obrigado a segui-los em nenhuma medida. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf. Último acesso 07/06/2023.

[19] Ver em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf. Último acesso 26/06/2023.

destinada a cobrir uma vasta gama de temas. Apenas a título de exemplo, é possível citar a regulação de direitos de propriedade intelectual *online*, de serviços públicos de *broadcast*, de infraestrutura de rede e segurança digital.

O DEA 2010 consiste na primeira legislação britânica especificamente voltada a regular atividades humanas no ciberespaço, pensando-as de acordo com as particularidades do âmbito virtual, especialmente no que diz respeito ao resguardo de direitos autorais e de propriedade intelectual. É relevante mencionar aqui algumas das medidas de maior relevância do ato. Primeiramente, faz referência ao aumento dos deveres e funções do OFCOM, o qual, desde a publicação do DEA 2010, ficou incumbido de produzir relatórios trianuais sobre a estrutura de comunicação do Reino Unido, registros de domínios de internet, e sobre o modo com que conteúdos de mídia contribuem com (ou prejudicam) o interesse público. Por segundo, inaugurou a imposição de obrigações a provedores de serviços de internet, com o intuito de reduzir violações a direitos de propriedade e autoria *online.* Por terceiro, viabilizou o aumento da pena prevista para quem violar direitos de propriedade e autoria no ciberespaço. Quarto, instituiu a atribuição de poderes ao Secretário de Estado (cargo análogo, no Brasil, ao de Ministros de Estado na área das comunicações) para, mediante autorização judicial, requerer bloqueio de provedores que não estejam atuando de acordo com regras de propriedade intelectual fixadas no DEA 2010, além do poder de interferir no registro de domínios públicos (Reino Unido, 2010).

Aprovado a toque de caixa apenas um mês antes das eleições gerais que tiraram o Parlamento do controle do Partido Trabalhista e o devolveu aos conservadores, o DEA 2010 enfrenta, desde a gênese, uma série de críticas, em especial no tocante ao sistema de notificação imposto a provedores de internet. Sobre esse último, foi determinado que provedores de serviços de internet elaborassem lista de usuários que, por intermédio de suas plataformas, estivessem supostamente compartilhando arquivos e, com isso, violando direitos autorais ou de propriedade. O ato prevê que tais listas seriam fornecidas, anonimamente, àqueles cujos direitos de autoria ou propriedade intelectual fossem feridos, sob pena de multa de até 250.000 libras esterlinas caso os provedores de serviços de internet deixassem de cumprir com tais obrigações. Previu-se também que, para que um usuário fosse incluído nessa lista, ele deveria ter participado ativamente do compartilhamento de um número mínimo de arquivos, marco que seria supostamente definido em código de boas práticas de autoria da autoridade reguladora. Em adição a isso, o DEA 2010 estipulou que usuários envolvidos em compartilhamento indevido de artigos poderiam ser notificados pelo provedor de serviços de internet, caso esse

último fosse requerido pelo detentor de direitos autorais ou de propriedade intelectual para assim proceder (Reino Unido, 2010, seções 124A e 124B). Tais formulações legais, como é de se supor, resultaram atrapalhadas e pouco profícuas. De início, o DEA 2010 foi bastante vago ao definir o que seria um "provedor de serviços de internet"[20], até o ponto em que empresas prestadoras de serviços, como cafés ou hotéis que forneciam acesso à internet a seus clientes, mostraram-se receosos de serem enquadrados nos requerimentos fixados no DEA 2010. De modo semelhante, a vagueza da lei para determinar quais *sites* deveriam bloquear usuários em razão de compartilhamento indevido de arquivos tenderia a prejudicar portais cujo enfoque era não mais que facilitar o acesso de internautas aos diversos sites existentes na *web*, a exemplo do *Google*. Além disso, provedores de serviços de internet se puseram insatisfeitos com o dever de promover tal controle, especialmente em razão das listas, as quais, alegou-se, prejudicariam as plataformas junto a seus clientes (Digital [...], 2010).

A pressa com que se aprovou o texto deixou brechas na lei, hoje cristalizadas no texto promulgado, e sua ineficácia para contornar problemas de compartilhamento indevido de arquivos logo se revelou. O teor controverso e a pouca factibilidade técnica acabaram por tornar o DEA 2010 quase inócuo no tocante às regulações pró-direitos de propriedade intelectual e autoria (Garstka, 2012). O código de boas práticas, que segundo o texto do DEA 2010 deveria regulamentar o dever de notificação por compartilhamento indevido de conteúdo, nunca foi aprovado, e a proposta foi engavetada nos anos seguintes. Além disso, logo ficou claro que avanços tecnológicos posteriores permitiriam que mesmo os usuários menos hábeis pudessem driblar, com certa facilidade, as determinações do DEA 2010.

Em suma, no tocante às tentativas de retirar o controle de violação de direitos de autoria e propriedade das cortes judiciais, transferindo-as às agências reguladoras, o DEA 2010 não obteve sucesso (Mendis, 2013). Com isso não se está a acenar na direção de que regulação administrativa do ciberespaço é ineficaz ou fadada ao fracasso – pelo contrário, a literatura atual aponta fortemente no sentido de que a moderação de conteúdo em massa deve passar pelas vias administrativas. É possível indicar, isso sim, que a afobação com que se debateu o projeto do DEA 2010 pouco atentou a fatores técnicos e sociais que influenciam o vigor impresso em mecanismos regulatórios. A exemplo do que indica Andrew Murray (2015), a tecnicidade que pautou o projeto do DEA 2010 relegou a segundo plano elementos sociais, fazendo vista grossa a mecanismos que permitem a continuidade do compartilhamento

[20] Como se lê no DMA, seção 124N: "'provedor de serviço de internet' significa qualquer pessoa que provê serviço de acesso à internet" (tradução nossa).

irregular de arquivos. Em outras palavras, a popularidade do compartilhamento de arquivos, pulverizada por meio de incontáveis usuários, deslocaram (e seguem deslocando) o fluxo de informação para novos caminhos, explicitando a geografia particular do ciberespaço e seu potencial de tornar infrutífera qualquer regulação que não atente a isso.

3.1.3 O *Digital Economy Act* 2017.

Sete anos passados da publicação do *Digital Economy Act* 2010, o Parlamento ampliou o escopo regulatório do OFCOM no âmbito do ciberespaço e das mídias de comunicação tradicionais, dessa vez através da promulgação do *Digital Economy Act* 2017 (DEA 2017). Mais enxuto e de conteúdo diferente de seu antecessor, o DEA 2017 trouxe em seu bojo, dentre outros pontos: [1] regras para o compartilhamento de dados entre órgãos ligados ao governo, para fins de governança digital e política de dados; [2] a requisição para que provedores de serviços de internet disponibilizassem filtros para bloqueio de conteúdo adulto, excluídas plataformas de redes sociais; [3] o incremento da pena prevista para crime de violação de direitos autorais e de propriedade intelectual; [4] e a previsão de criação de um regulador britânico para verificação de idade de usuários, o qual seria responsável por orientar *sites* com conteúdo pornográfico a apenas admitir usuários maiores de 18 anos de idade, sob pena de multa, bloqueio e suspensão de propagandas comerciais que anunciassem nos portais que não cumprissem com os padrões determinados pela autoridade reguladora (também neste ponto excluídas plataformas de redes sociais); [5] ademais de outras regulações pertinentes às áreas de telefonia, televisão e telecomunicações em geral (Reino Unido, 2017)[21].

Dentre os pontos mais relevantes da lei (e pela primeira vez com enfoque específico em moderação de conteúdo) está a previsão de controle de acesso de pornografia por crianças e adolescentes através de sistema de verificação de idade. Isso na chamada Parte 3 do DEA 2017. Inicialmente, previa-se que autoridade reguladora – a qual se acreditava que seria a *British Board of Film Classification* (BBFC)[22] –, seria investida de poderes para coordenar a inclusão de sistema de filtro de idade em sites que veiculassem conteúdos pornográficos de maneira geral, à exceção de plataformas de redes sociais. Como já é possível supor, a efetivação do filtro de idade dependeria da aprovação de normatização secundária confeccionada pela

[21] Ver em https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted. Último acesso 20/06/2023.
[22] Ver em https://www.bbfc.co.uk/. Último acesso 20/06/2023.

autoridade reguladora, a qual nunca veio a ocorrer. Os portais que não se enquadrassem nas linhas gerais estipuladas pela BBFC estariam sujeitos a multa de até 250.000£ ou 6% de seu lucro, bloqueio e notificação de seus anunciantes e financiadores (Reino Unido, 2017).

No entanto, à semelhança do que ocorreu com o DEA 2010, o DEA 2017 foi aprovado a toque de caixa, logo após a votação pelo *Brexit* e às vésperas da eleição geral para troca de gabinetes no Parlamento. Isso fez com que seu texto final restasse pouco discutido tanto técnica quanto socialmente. Desde a publicação, abundaram comentários de que o sistema proposto seria facilmente burlado por internautas que assim o desejassem fazer, por meio de aplicativos VPN ou de navegadores Tor (Thurman e Obster, 2021, p. 420). Não bastasse o exposto, o fato de o DEA 2017 tentar combater o acesso de crianças e adolescentes a conteúdos pornográficos sem incluir em seu escopo a regulação de redes sociais, deixou enorme espaço ao insucesso da proposta, já que se estima que, no Reino Unido, cerca de um terço dos materiais sexualmente impróprios circulem por intermédio dessas redes (Thurman e Obster, 2021, p. 419). Outrossim, em que pese a proposta de controle do acesso de crianças a conteúdos indevidos não tenha enfrentado disputas do mesmo teor que o OSA enfrentou quanto à mitigação da liberdade de expressão, a Parte 3 do DEA 2017 foi desde sua gênese criticada por impor riscos à privacidade de usuários adultos em razão dos mecanismos de filtragem de idade. Desse modo, as dificuldades técnicas do DEA 2017 foram, ao fio dos anos, repetidas vezes retardando sua implementação.

Sobre o sistema de verificação de idade, após consulta pública, a BBFC chegou a anunciar sua efetivação para abril de 2018, a qual logo foi postergada para o final do ano, e, a seguir, transferida para a primavera seguinte. Quando a normatização secundária para o DEA 2017 foi finalmente publicada pela BBFC, então intitulada *Online Pornography (Comercial Basis) Regulations* (Reino Unido, 2019a), a implementação das linhas gerais foi inúmeras vezes posposta, até que, em outubro, a então Secretária do *Digital, Culture, Media and Sport* (DCMS), Nicky Morgan, anunciou a retirada da intenção do governo britânico de regular o acesso de conteúdo pornográfico por crianças por meio de mecanismos de verificação de idade. Em pronunciamento publicado no *site* do Parlamento[23], Morgan reconheceu as dificuldades técnicas e brechas do DEA 2017. Como àquele tempo já começava a ser engendrada a estratégia regulatória que hoje se consolida no OSA, a Secretária afirmou que passaria a investir nos chamados deveres de cuidado, então ventilados no *Online Harms White Paper* de 2019

[23] Ver em https://questions-statements.parliament.uk/written-statements/detail/2019-10-16/HCWS13. Último acesso 20/06/2023.

(OHWP). Em outubro de 2020, o governo britânico anunciou o engavetamento definitivo da Parte 3 do DEA 2017[24], o que se consolidou com a publicação do *Draft Online Safety Bill*, em 2021, onde se explicitou a revogação do ato anterior (Reino Unido, 2021a, Parte 7, Cláusula 131).

A fazer uso mais uma vez do comunitarismo de rede de Murray (2015), a mera imposição de regulação indireta, desatenta a fatores conjunturais e sociais, mostrou-se inapta para alterar de forma significativa o *modus operandi* da vida coletiva em rede. A geografia particular do ciberespaço demonstra que a imposição isolada de barreiras – filtros randômicos, a exemplo do sistema de verificação de idade pensado pelo DEA 2017 –, deixa brechas para que o fluxo de informação mude somente sua trajetória, e não a profusão na qual chega aos usuários. Isso especialmente ao se ter em conta que o DEA 2017 não abarcava conteúdos circulados em redes sociais. Ao mesmo tempo, conciliar valores basilares e o modo como esses são aplicados no mundo real com as demandas particulares do mundo virtual requer negociações e adaptações cuja medida ótima ainda se desconhece, a exemplo de uma maior mitigação, ou não, do que ordinariamente se entende por liberdade de expressão.

É sabido que, até o momento, o controle de conteúdo *online* no Reino Unido, como em tantas outras jurisdições, se dá mediante a combinação de ferramentas de *soft power* com o incentivo à autorregulação das *bigtechs,* com a possível apreciação judicial dos casos que logrem ser levados até esta instância (Catley, 2023, p. 23). Tal arranjo se mostra crescentemente incapaz de prevenir a circulação de conteúdos impróprios ou daninhos, a exemplo de desinformação *antivax* durante a crise sanitária da COVID-19, o livre acesso à pornografia por crianças, a desinformação política, e os crimes de ameaça ou de apologia ao terrorismo. Temas que, é de conhecimento público, são motivo de preocupação declarada para a administração britânica. As experiências regulatórias anteriores, juntamente com demandas contemporâneas, fizeram com que o governo britânico admitisse a ineficácia das ações até então empreendidas e, a exemplo de outros países - como Alemanha ou o bloco europeu -, passasse a investir em mecanismo de *hard law,* abrangente e administrativo, no qual a responsabilidade de agentes intermediários pudesse ser cobrada objetivamente. Adentrou-se, com isso, a era da Estratégia para Segurança na Internet para controle de conteúdo nas redes.

[24] Ver em https://hansard.parliament.uk/Commons/2020-10-08/debates/0F55F270-487C-4D1A-BE7E-63A3EABDEA97/BusinessOfTheHouse. Último acesso em 20/06/2023.

3.2 "Fazer do Reino Unido o lugar mais seguro do mundo para estar *online*": a Estratégia de Segurança na Internet britânica e os preâmbulos do *Online Safety Act.*

3.2.1 O *Internet Safety Strategy green paper.*

Na esteira dos receios lançados com o escândalo da *Cambridge Analytica* e a possível interferência, em 2016, nas eleições presidenciais norte-americanas e na votação do Brexit[25], o Parlamento acendeu uma luz quanto aos riscos em potencial acarretados pelo uso indevido de dados e pelo direcionamento de conteúdo por parte das plataformas. Esse fato, somado ao imbróglio técnico no qual se encontrava a estratégia de verificação de idade proposta pelo DEA 2017, bem como em vista da flagrância com que se encarava, já àquele tempo, a necessidade de regulação de atividades travadas por meio de redes sociais, deu ensejo a um novo momento no histórico regulatório britânico, marcado pelo lançamento do *Internet Safety Strategy green paper*[26] (ISSGP)[27] em 2017. Sob o lema de "fazer do Reino Unido o lugar mais seguro do mundo para estar *online*"[28] (Reino Unido, 2017a, p. 2) dava-se o primeiro passo em direção à elaboração do OSA.

No direito britânico, *green papers* consistem em documentos de consulta produzidos pelo governo, cujo objetivo é permitir que pessoas dentro e fora do Parlamento se manifestem sobre políticas públicas ou propostas legislativas pretendidas pela Administração[29]. No caso do ISSGP, a consulta pública esteve em aberto entre outubro e dezembro de 2017, indagando

[25]No início da década de 2010, dados de milhões de usuários do Facebook foram coletados sem sua anuência, para uso de publicidade eleitoral pela empresa de consultoria Cambridge Analytica. Após denúncia de ex-empregado da empresa, veio à tona que os dados coletados indevidamente teriam sido usados para interferência na campanha presidencial norte-americana de 2016, na qual Donald Trump saiu vencedor. A denúncia também indicou a manipulação de dados para direcionamento de propaganda eleitoral no curso da campanha do Brexit, em 2016, muito embora nunca tenha se provado que as infromações maliciosamente direcionadas tenham, de fato, servido a definir os rumos da votação. Ver em: https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal. Último acesso 03/03/2023.

[26] Ver em https://www.gov.uk/government/consultations/internet-safety-strategy-green-paper. Último acesso 21/06/2023.

[27] Em 2009 o Departamento de Educação, na esteira de relatório publicado pelo UK Council fo Child Internet safety (UKCCIS), lançou o primeiro plano de Estratégia de Segurança na Internet - intitulado "*click clever click safe*". A proposta, muito mais simples que a lançada na ISSGP, focava majoritariamente na instrução de pais e crianças sobre como identificar e denunciar conteúdos impróprios *online*. Ver em https://www.wired-gov.net/wg/wg-news-1.nsf/0/1BD7EBFBDC2E64F28025768600480009?OpenDocument. Último acesso 21/06/2023.

[28] Expressão utilizada pela então Secretária de Estado do DCMS, Karen Bradley, na introdução do ISSGP. Desde então a frase foi repetida em inúmeras ocasiões, por diversas autoridades e grupos midiáticos, servindo como mote do projeto regulatório britânico.

[29] Ver em https://www.parliament.uk/site-information/glossary/green-papers/. Último acesso 03/06/2023.

empresas, comunidade científica e acadêmica, sociedade civil e quem mais estivesse disposto a tomar parte no debate, quanto às intenções do Parlamento de produzir novo corpo legislativo que englobasse uma série de temas. Primeiramente, indagou-se sobre a possibilidade de responsabilização de plataformas de mídias sociais com relação a seus usuários; segundo, sobre a introdução de um código de boas práticas para mídias sociais e relatórios de transparência e a taxação de empresas de mídias sociais, para que estes tomem parte em movimento de conscientização de possíveis danos causados por atividades *online.* Terceiro, questionou-se sobre soluções tecnológicas para danos *online,* promoção de alfabetização digital de crianças e apoio a pais e educadores. Quarto, consultou sobre a implementação de políticas de combate a *bullying*, humilhação e outros comportamentos intimidatórios *online.* Por fim, a população interessada foi indagada sobre a contenção dos danos causados pela exposição de crianças a conteúdos pornográficos (Reino Unido, 2017a). A consulta inicial promovida pelo *green paper* foi bastante aberta, justamente para ouvir o maior número de interessados possível. A participação foi ampla, e, em resposta, o governo publicou, em maio de 2018, o "*Government Response to the ISSGP*" (GRISSGP). Nesse último, foram divulgados os resultados quanto à aprovação pelo público participante das linhas regulatórias sugeridas no *green paper.* Dentre os temas que tiveram maior respaldo do público participante, ganharam destaque os relatórios de transparência de empresas de mídias sociais; a criação de código de boas práticas com critérios claros e explícitos; a disponibilização de ferramentas tecnológicas para controle dos usuários; e a necessidade de elaboração de corpo regulatório com força de lei, com previsão de sanções, sob o comando de órgão regulador independente (Reino Unido, 2018). Apresentados os resultados do ISSGP, o governo comprometeu-se com a publicação de um *white paper*, no qual estabeleceria planos para a futura legislação. Nesse, seriam abordados danos *online* de toda sorte*,* aí incluídos conteúdos ilegais ou legais, porém potencialmente danosos.

3.2.2 O *Online Harms White Paper.*

Inicialmente previsto para ser lançado no mesmo ano que seu antecedente, o ISSGP, a elaboração do O*nline Harms White Paper* (OHWP) rendeu mais debates do que inicialmente se esperava. Em razão disso, o relatório foi publicado pelo governo britânico somente em abril de 2019, evento ao qual se seguiu novo período de consulta pública. Com teor mais complexo que os *green papers*, no direito britânico os *white papers* consistem em documentos de políticas

produzidos pelo governo, e representam o segundo passo para a escrita de projeto de lei. É no *white paper* que são apresentadas, de forma consistente, as propostas e intenções da legislação futura. Por fixarem princípios e objetivos, funcionam como espécie de "linhas mestras" para o processo legislativo, embasando discussões e servindo como material de consulta no curso dos debates próprios da atividade legiferante[30].

O OHWP reiterou a intenção britânica de tornar o Reino Unido "o lugar mais seguro do mundo para estar *online*", bem como "o melhor lugar do mundo para iniciar e desenvolver atividades empresariais digitais". Em seu bojo, o documento ressaltou dificuldades de equacionar liberdade de expressão com ações que combatam a circulação de conteúdos prejudiciais à saúde (aí incluídos uma gama de temas afins, como prevenção ao suicídio, à distúrbios alimentares, à desinformação, etc.). Também destacou os desafios envolvendo conciliar, no ciberespaço, valores democráticos, discursos de ódio e terrorismo, conteúdos impróprios para crianças, cultura de gangues, apologia à violência e assédio de diferentes tipos. Para combater os problemas listados, o OHWP propôs nova estrutura regulatória para a economia digital britânica, com enfoque nos conteúdos veiculados especificamente por meio de plataformas digitais (a ampliar de sobremaneira o escopo do DEA 2017). O OHWP estipulou um total de nove linhas mestras, as quais merecem ser brevemente comentadas. Primeiro, a observação, a todo tempo, do direito de liberdade de expressão. Segundo, a fixação de regras claras para plataformas digitais. Terceiro, o estabelecimento de deveres de cuidado, precisos e executáveis, para *bigtechs.* Quarto, a criação de entidade regulatória independente. Quinto, a exigência, com relação a empresas controladoras de portais *online*, de publicação de termos e condições que aportem clareza aos contratos de consumo entre essas e seus usuários. Sexto, a elaboração, pela autoridade reguladora, de código de boas práticas, a ser acrescido pelo Parlamento no que diz respeito a boas práticas concernentes à segurança *online* de crianças. Sétimo, o estabelecimento de políticas antiviolência e preventivas de comércio de serviços ou produtos ilegais, a exemplo de venda de armas. Oitavo, o fomento à cultura de transparência e *accountability* no tocante ao funcionamento de algoritmos. Por fim, o oitavo ponto é o direcionamento da nova lei a empresas e plataformas específicas, sejam elas ferramentas de buscas, sejam de comunicação, desde que se enquadrem em determinados padrões pré-estipulados pela autoridade reguladora (Reino Unido, 2019).

[30] Ver em https://www.parliament.uk/site-information/glossary/white-paper/. Último acesso 22/06/2023.

Foi no OHWP que, pela primeira vez de modo formal, o governo manifestou sua intenção de tornar *bigtechs* responsáveis pelos conteúdos danosos e/ou ilegais veiculados por meio de suas redes. Para atingir esse fim, o *white paper* propôs a fixação dos chamados *duties of care*, "deveres de cuidado", a serem fiscalizados e formalizados pela autoridade reguladora. A opção pela responsabilização das plataformas veio na esteira de um conjunto de diversos fatores e influências externas, aí incluídos a consolidação da Lei dos Mercados Digitais (LMD); a publicação da *NetzDG*, na Alemanha; e as sugestões feitas pela Professora Lorna Woods no relatório *Online harm reduction – a statutory duty of care and regulator*, publicado através da Carnegie UK[31]. A escolha pela possibilidade de responsabilizar agentes intermediários no ciberespaço foi também motivada por relatório de lavra do próprio DCMS, voltado a analisar os impactos da desinformação no Reino Unido. Nesse documento, o governo reconheceu que a nação enfrentava "crise democrática, baseada na manipulação sistemática de dados para apoiar o direcionamento implacável de cidadãos, sem seu consentimento, por campanhas de desinformação e mensagens de ódio" [tradução nossa] (Reino Unido, 2018, p. 40), e defendeu que empresas de tecnologia passassem a ser responsabilizadas pela circulação de "materiais danosos e de desinformação"[32]. Ao OHWP seguiu-se a publicação do *Draft Online Safety Bill* (DOSB), esboço do primeiro texto do *Online Safety Act* levado ao Parlamento, e que há de ser comentado amiúde nas seções seguintes. Por ora, no entanto, é relevante analisar a conjuntura política interna e externa na qual se encontrava o Reino Unido ao tempo do OHWP, pertinente à devida compreensão das opções legislativas que hoje se consolidam no OSA.

3.2.3 O *Brexit*, a conjuntura internacional e a agenda neorregulatória do *Digital Regulators Cooperation Forum.*

A saída do Reino Unido do bloco europeu, dentre tantos outros efeitos, deu azo a aspirações de liderança e de vanguarda em matéria de regulação da internet por parte de dirigentes britânicos. Uma vez consumada a votação pelo "sim", e tornado público o desejo da maioria dos eleitores de abandonar a União Europeia (sob auspícios de fortalecer sua

[31] Ver em https://carnegieuktrust.org.uk/publications/online-harm-reduction-a-statutory-duty-of-care-and-regulator/. Último acesso 26/06/2023.
[32] Ver em https://web.archive.org/web/20181207234021/https:/www.parliament.uk/business/committees/committees-a-z/commons-select/digital-culture-media-and-sport-committee/news/fake-news-report-published/ . Último acesso 26/06/2023.

soberania), tópicos relacionados à segurança nacional voltaram a ocupar lugar de destaque nas agendas políticas do país, dessa vez andando de mãos dadas com os debates regulatórios de empresas de tecnologia. Em março de 2021 foi lançado, pelo *Cabinet Office* do Parlamento, órgão ministerial vinculado diretamente ao Primeiro Ministro, relatório intitulado *Global Britain in a Competitive Age: the Integrated Review of Security, Defence, Development and Foreign Policy*[33] (GBCA 2021). Nesse, foram esboçadas metas de segurança nacional a serem atingidas até o ano de 2030, assinadas e introduzidas pelo então Primeiro Ministro Boris Johnson. Autodescrevendo-se como "o maior programa de investimento em defesa desde a Guerra Fria", o documento anunciou o aumento da contribuição do Reino Unido para a OTAN, o investimento em agências antiterrorismo, o combate ao aquecimento global e a intenção de consolidar o Reino Unido como "superpotência em matéria de ciência e tecnologia" (Reino Unido, 2021, p. 4). No tocante a esse último objetivo, cujo escopo é amplo, é importante mencionar dois movimentos que, hoje, já estão em execução e guardam relação próxima com a formulação do OSA. O primeiro é a adesão, por parte do governo britânico, da proposta de governança ágil para fins de regulação de plataformas *online*, recomendada pela Organização para Cooperação e Desenvolvimento Econômico (OCDE) e pelo Fórum Econômico Mundial (FEM). O segundo é o reconhecimento de que políticas de controle de conteúdo devem se dar de modo concomitante a outros movimentos regulatórios, especialmente no tocante ao direito da concorrência e à proteção de dados *online.* Esse último ponto vem amiúde ganhando espaço na agenda regulatória britânica, a qual se esforça por atuar conjuntamente nas três áreas.

Muito embora a trajetória regulatória do Reino Unido seja original e atenta a particularidades nacionais específicas, pretendendo compreender a mais ampla gama regulatória da internet no Ocidente, a agenda de políticas públicas para transposição da Administração à sociedade em rede não é única, e se alinha ao consenso internacional de que atitudes *ex ante* são necessárias. Além disso, tratando-se a regulação de mídias e plataformas digitais de tema transnacional, leis como o LMD, da União Europeia, o *NtezDG*, da Alemanha, ou o *Online Safety Act*, da Austrália, são a todo tempo observadas pelo Parlamento na elaboração de suas políticas regulatórias para as atividades no ciberespaço. O mesmo ocorre com relação aos debates sobre medidas antitruste em face das *bigtechs* nos Estados Unidos, as quais são igualmente acompanhadas de perto pelas autoridades britânicas. Não à toa, no momento de escrita deste trabalho o Parlamento discute, também, a aprovação da chamada

[33] Ver em Global Britain in a competitive age (publishing.service.gov.uk). Último acesso em 29/06/2023.

Digital Markets, Competition, and Consumers Bill[34]. Nesse cenário, a produção legislativa para fins de regulação conta a todo tempo com a influência de agentes externos que, em boa medida, pautam o modo e as prioridades para atuação do Parlamento, fornecendo modelos pertinentes e outras ferramentas de apoio à atividade legiferante. A OCDE e o FEM são dois desses agentes e sua influência no espaço britânico se destaca pela adoção da acima mencionada "governança ágil" por parte de *Westminster*. Nessa toada, "o pensamento de ambas as corporações, aplicável às plataformas digitais, tem sido influente no Reino Unido, que em novembro de 2020 tornou-se signatário do *Agile Nations* da OCDE" (Schlesinger, 2022, p. 49)[35].

A governança ágil e a preocupação com as diferentes demandas regulatórias da internet fizeram com que, no início de 2020, três agências britânicas passassem a protagonizar os debates nacionais para regulação de plataformas, cada uma delas se relacionando com uma seara específica das atividades no ciberespaço. São elas: a *Competition and Markets Authority* (CMA)[36], para questões ligadas a Direito da Concorrência; o *Information Commitioner's Office* (ICO)[37], entidade pública independente voltada a questões de proteção de dados e liberdade de expressão; e o *Office of Communications* (OFCOM), o órgão regulatório oficial do Reino Unido para regulação dos meios de comunicação, diretamente envolvido com a atual *Internet Safety Strategy*. Não há dúvida, o OFCOM é a autoridade de maior relevância no cenário regulatório britânico da atualidade, e consta, de momento, como principal órgão para implementação e controle das regulações previstas no OSA. O OFCOM é fruto da convergência de outros cinco órgãos predecessores – o *Broadcast Standards Commision;* o *Office of Telecommunications;* a *Independent Television Commision;* a *Radio Authority;* e a *Radiocommunications Agency –,* e foi originalmente pensado para regular TV, TV a cabo, rádio, telefonia fixa e móvel, serviços postais e provedores de internet sem fio. Há pouco, em 2020, o governo estendeu os poderes regulatórios do OFCOM, que passou a ser também o

[34] Ver em https://bills.parliament.uk/bills/3453. Último acesso 05/07/2023.
[35] Ver "Agile Nations: nações assinam primeiro acordo para destravar o potencial de tecnologias emergentes", disponível em https://www.oecd.org/gov/regulatory-policy/agile-governance-for-the-post-pandemic-world-wef-oecd-joint-event.htm. Último acesso 24/05/2023.
[36] O CMA é o órgão regulador da concorrência, autoridade nacional que busca promover a concorrência, tanto dentro como fora do Reino Unido, em benefício dos consumidores. A CMA investiga fusões, conduz estudos de mercado e faz investigações sobre comportamento anticompetitivo. Seu alcance se estende aos mercados digitais, tanto diretamente quanto por meio de seu órgão afiliado, a Unidade de Mercados Digitais (*Digital Markets Unit* - DMU) [tradução nossa] (Schlesinger, 2022, p. 51)
[37] O ICO consiste em organismo público independente, financiado pelo Departamento de assuntos Digitais, Cultura, Mídia e Esporte (DCMS). O Comissário de Informação, que é sempre um oficial indicado pela Coroa, é o regulador independente do Reino Unido par proteção de dados e liberdade de expressão, com responsabilidades-chave fiadas pelo *Data Protection Act* de 2018 e pelo *Freedom of Information Act* de 2000. [tradução nossa] (Schlesinger, 2022, p. 52).

órgão regulador responsável por "ofensas *online*" (Schlesinger, 2022, p. 51). A partir da vigência do OSA, o órgão está também incumbido de formular códigos de boas práticas, os quais deverão ser confirmados pelo Parlamento. Apenas a título de menção, é importante pontuar que, recentemente, a *Financial Conduct Authority* (FCA), órgão público independente, responsável pela supervisão de cerca de 50.000 firmas do mercado financeiro britânico, vem ganhando espaço para fins de proteção a consumidores e mercado na promoção de políticas antitruste para o ciberespaço (Schlesinger, 2022, p. 52).

No cenário britânico, a existência de órgãos paralelos, cada qual voltado a pensar uma área especial de regulação do mundo virtual, é consequência óbvia da complexificação da vida social na internet, a qual se estendeu às mais diversas searas e passou a exigir regulações de crescente especificidade. A despeito das particularidades de cada agência reguladora do Reino Unido, e justamente em razão da ciência de que se trata de movimento multidisciplinar e orquestrado, há uma moção conjunta para que o processo de regulação do ciberespaço, independentemente da área, dê-se de forma harmoniosa e coerente. Para ilustrar essa dinâmica, basta observar que os debates sobre o texto do *Online Safety Act* mantiveram proximidade com os debates da *Digital Markets, Competition and Consumers Bill*, e vice-versa. A fim de tornar o processo ainda mais coeso, em julho de 2020, o CMA, o OFCOM e o ICO anunciaram a criação da *Digital Regulation Cooperation Forum* (DRCF), com a posterior adesão da FCA. O objetivo da criação do fórum, assim anunciaram os órgãos envolvidos, é de construir relações de trabalho entre as organizações membro, "em vista dos desafios impostos pela regulação das plataformas *online*"[38]. A criação do DRCF veio na esteira das políticas que visam a tornar o Reino Unido uma "superpotência em matéria de ciência e tecnologia" (Reino Unido, 2021, p. 5), e é também fruto de manifestação da Casa dos Lordes. Sobre a manifestação dessa Casa, ao criticar o estado fragmentário e moroso do processo regulatório no Reino Unido, foi sugerida a criação de autoridade digital "neorregulatória", com poder para supervisionar todos os processos regulatórios concomitantes conduzidos pelo Parlamento e demais autoridades britânicas (Schlesinger, 2022, p. 55). Em que pese a DRCF não goze desse poder, e esteja mais para fórum de debate paralelo, não há dúvida que representa a resposta administrativa dada ao pleito dos Lordes (Schlesinger, 2022, p. 58).

Em meio a tal conjuntura, a todo tempo orientada pela autoatribuição de fazer do Reino Unido referência na regulação da internet a nível mundial, que foi publicado, em maio

[38] Disponível em https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum. Último acesso em 26/05/2023.

de 2021, o *Draft Online Safety Bill* (DOSB), lançando uma série de debates que ainda hoje seguem sendo travados no Parlamento. Muito embora o texto do *draft* tenha sido bastante alterado desde sua publicação, é nele que a pretensiosa estrutura regulatória divulgada no OHWP é, pela primeira vez, apresentada em formato de texto legal. Os pormenores dessa nova etapa do processo regulatório britânico são trabalhados na seção que segue.

3.3 O *Draft Online Safety Bill* e a oficialização dos *Duties of Care.*

3.3.1 Breves notas explanatórias sobre o processo legislativo britânico.

Para melhor compreensão dos estágios do OSA, calha iniciar este subcapítulo elucidando algumas particularidades do processo legislativo britânico. Uma vez publicado o *white paper* que deu origem ao projeto de lei do OSA, foi divulgado o *Draft Online Safety Bill* (DOSB). No direito britânico, *drafts* não consistem em projetos de lei propriamente ditos, porquanto ainda não foram levados para a apreciação do Parlamento. É somente após a publicação e consulta prévia do d*raft* que o texto é levado para escrutínio em *Westminster* – no caso do OSA, primeiro na Casa dos Comuns e, depois, na Casa dos Lordes –, quando passa a ser denominado "*Bill"*. Neste ponto, é conveniente mencionar que, durante todo tempo que esteve no Parlamento, até antes de receber assentimento real em 26 de outubro de 2023, o OSA era chamado de *Online Safety Bill* (OSB). Durante a feitura deste trabalho, inclusive, lidou-se quase todo tempo com a OSB, ao invés do OSA.

Segundo o *Oxford Dictionary of Law*, *bills* consistem em "esboços de proposta de *Acts of Parliament*, os quais devem passar pelas duas casas antes de serem aprovados" (Oxford [...], 2015, p. 67). Uma vez vencidas as etapas legislativas nas duas casas, a *Bill* prossegue para assentimento real, quando finalmente passará a ser, oficialmente, um *Act of Parliament* e gozar de força de lei (abandonando, então, a forma de *bill)*. No caso da *Online Safety Bill*, após a conclusão dos trâmites nas duas casas e concedida a aquiescência da Coroa, o projeto ganhou força de lei e passou a ser denominado "*Online Safety Act*"[39].

[39] Denominação homônima à lei australiana que trata de matéria similar. Ver em https://www.legislation.gov.au/Details/C2021A00076. Último acesso 17/10/2023.

3.3.2 O *Draft Online Safety Bill.*

Já à época de sua primeira publicação, ainda em formato de esboço, o DOSB propunha extenso aparato legislativo, totalmente voltado à regulação de plataformas e controle de conteúdo *online.* O *draft* tratava pontualmente de matérias como proteção a crianças, combate a fraudes e discurso de ódio, e resguardo da democracia e da liberdade de expressão[40]. O texto se dividia em sete partes, todas subdivididas em capítulos, que a sua vez se subdividiam em cláusulas e subseções. A parte 1 continha definições técnicas dos serviços aos quais o DOSB se aplica. A parte 2 fixava deveres de cuidado a serem seguidos por provedores de plataformas digitais, estabelecendo quais tipos de responsabilidade deveriam recair sobre os diferentes tipos de mídias. Na parte 3 havia a fixação de deveres adicionais, relativos a taxas e relatórios de transparência. A parte 4 era dedicada a delinear os deveres e poderes do OFCOM como autoridade reguladora. A parte 5 tratava dos recursos contra decisões do OFCOM. Na parte 6 eram fixados poderes ao Secretário de Estado, chefe do OFCOM, para definir estratégias e prioridades na regulação de mídias de internet, além de revisar determinações estipuladas no DOSB e evitar sua obsolescência. Por fim, na parte 7, foram estabelecidas provisões gerais e finais (Reino Unido, 2021a).

É relevante ressaltar que foi no DOSB que, pela primeira vez, três aparatos regulatórios para fins de controle de conteúdo foram pela primeira vez propostos no Reino Unido – alguns deles ainda vigentes no atual OSA, outros substituídos. De início, é a fixação dos chamados "serviços de Categoria 1", onde são enquadrados os grandes portais de serviço "usuário-a-usuário"[41], diferenciação por meio da qual o DOSB buscava regular de forma diversa grandes plataformas globais e serviços de menor envergadura. Segundo, é a possibilidade de responsabilização direta de empresas intermediárias pela veiculação de conteúdo *online* danoso – seja para adultos seja para crianças, ou que ofereçam risco à ordem democrática –, mediante a imposição dos chamados *Duties of Care* (deveres de cuidado[42]).

---

[40] Ver nota de lançamento do DOSB no site do governo britânico. Disponível em https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published. Último acesso 07/07/2023.

[41] Qual há de ser esmiuçado mais adiante, a Online Safety Bill se volta a regular os "serviços de busca" e os "serviços de usuário-a-usuário". Por ora, basta esclarecer que, por usuário-a-usuário, o DOSB se refere ao "serviço através do qual um conteúdo que é gerado por um usuário do serviço, ou subido ou compartilhado no serviço através de um usuário do serviço, possa ser acessado por outro(s) usuário(s) do serviço" (Reino Unido, 2021a, parte 1; 2; 1), independentemente das dimensões que a divulgação desse conteúdo assuma.

[42] De modo semelhante, foi posteriormente formalizada no Digital Services Act, da União Europeia, a fixação de obrigações e responsabilidades específicas para plataformas de grande porte - para fins de análise de riscos,

Segundo Lorna Woods, professora na Universidade de Essex e uma das acadêmicas envolvidas nos debates sobre regulação junto ao Parlamento, o dever de cuidado no direito britânico tem origem em contextos jurídicos diversos, e consiste, grosso modo, na "obrigação imposta de exercer cuidado razoável, ou habilidade necessária, a fim de evitar o risco de danos a terceiros". De acordo com a autora, não há necessidade de "proteção perfeita", já que usualmente o padrão demandado é o de uma pessoa ordinária e razoável (Woods, 2019, p. 7). Por terceiro, e último, o DOSB trouxe em seu bojo a proposta de dever de controle, para serviços de Categoria 1, de conteúdos ilegais e legais, porém nocivos. Em outros termos, o DOSB atribuiu às grandes plataformas a obrigação adicional de especificar em seus termos de serviço como temas legais, porém danosos, seriam tratados em suas redes (Reino Unido, 2021a, parte 2, capítulo 2; 11). Dessa forma, qualquer conteúdo identificado como "potencialmente nocivo para adultos" deveria ser removido e reportado ao OFCOM, sob pena de responsabilização. Para fins de elencar o que era "nocivo", as plataformas deveriam analisar os riscos de dano físico, social e psicológico promovidos por cada tipo de conteúdo. Tratou-se, seguramente, do trecho mais polêmico do projeto apresentado, porquanto a apreciação do que é nocivo, via de regra subjetiva, estava a ser depositada sobre agentes privados transnacionais. A proposta induziu uma série de questionamentos por parte da sociedade civil e entidades observadoras (Jennings, 2021) (Internet [...], 2021) e acabou por ser retirada no curso dos debates na Casa do Comuns, sendo ora substituída pelo sistema de checagem em três etapas, o qual será explorado subsequentemente.

O DOSB foi levado à Casa dos Comuns em março de 2022, quando passou a atender pelo nome de *Online Safety Bill* (OSB). Após sua segunda leitura em abril do mesmo ano[43], foi

transparência de design, observação de direitos de liberdade de expressão, controle de conteúdo ilegal, dentre outros. Disponível em https://ec.europa.eu/commission/presscorner/detail/en/ip_22_6906. Último acesso 07/07/2023. Outrossim, a proposta de deveres de cuidado de provedores de grande porte foi igualmente ventilada no Brasil, nas recentes deliberações sobre o PL 2630/2020, e vêm consolidadas no substitutivo proposto no Parecer Preliminar de Plenário, de lavra do relator Deputado Orlando Silva. Disponível em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2265334&filename=Tramitacao-PL%202630/2020. Último acesso 07/07/2023.

[43] No processo legislativo britânico, as leis que iniciam pela apreciação da Casa dos Comuns devem passar, antes de serem levadas para assentimento real, pelos seguintes estágios: 1) Primeira leitura na Casa dos Comuns, a qual consiste em rápida apresentação do projeto aos membros do Parlamento e não costuma tomar mais que um encontro. 2) Segunda leitura na Casa dos Comuns, na qual o texto é lido ao plenário e os partidos debatem os pontos que, assim entendem, deverão ser modificados. Nesta etapa emendas ainda não podem ser propostas. 3) Comissões: o plenário ou comissão representativa da composição geral da Casa dos Comuns analisa o projeto de lei amiúde, linha por linha, e propõe emendas. 4) *Report Stage*: as emendas são discutidas pelo plenario da Casa dos Comuns. 5) Terceira leitura na Casa dos Comuns. Discussão do projeto em linhas gerais, antes de ser enviado para a Casa dos Lordes. Emendas não podem ser propostas nesta etapa. 6) Primeira leitura na Casa dos Lordes. 7) Segunda leitura na Casa dos Lordes. 8) Comissões na Casa do Lordes. 9) Report Stage na Casa dos Lordes. 10) Terceira leitura na Casa dos Lordes, onde pequenos ajustes podem ser feitos no texto. 11) Envio do

deliberado pelo Parlamento a prorrogação[44] do cronograma previsto para apreciação da lei naquela Casa. Em razão da complexidade e das polêmicas envolvendo o projeto, esse teve seu calendário reprogramado e repetido na sessão legislativa seguinte. Em maio de 2022 houve, então, novas Primeira e Segunda leituras, seguidas de inúmeras emendas na conseguinte fase de Comissões. As modificações propostas foram tantas, e de tamanha minúcia, que nova prorrogação teve de ser aprovada, de forma que o projeto somente deixou a Casa dos Comuns em janeiro de 2023[45], quando finalmente rumou para a Casa dos Lordes. No curso dos trâmites na Casa dos Comuns, a proposta de responsabilidade de *bigtechs* pelo controle de conteúdo "legal, porém nocivo" foi abandonada e substituída por outras ferramentas regulatórias que hão de ser exploradas no próximo subcapítulo. De modo bastante alterado em comparação à proposta original da DOSB, a OSB foi paulatinamente se voltando ao controle de conteúdo impróprio para crianças, com a retomada e revigoramento da proposta de checagem de idade e identidade de usuários, em retorno parcial ao DEA 2017. Em janeiro de 2023 o texto foi levado a casa dos Lordes, onde em setembro de 2023 completou o último estágio de discussão das emendas propostas. Novamente, qual ocorrera com o texto inicial do projeto, os debates envolvendo a OSB levaram mais tempo do que o previsto[46], de modo que sua consolidação em lei coincide com o final da escrita deste trabalho. Em 19 de julho de 2023[47], novo texto substitutivo integral foi publicado pela Casa dos Lordes, o qual sofreu pequenas emendas pela Casa dos Lordes e, a seguir, pela Casa dos Comuns, quando foi finalmente enviado para assente real.

3.4 O *Online Safety Act* em seu estado mais atual: deveres de cuidado, deveres especiais, deveres de transparência e o OFCOM como autoridade reguladora.

texto para assentimento real. Ver em https://www.gov.uk/guidance/legislative-process-taking-a-bill-through-parliament#parliamentary-stages. Último acesso 10/07/2023.

[44] Prorrogado através de mecanismo procedimental intitulado "*programme motion*", através do qual o governo pode estabelecer cronograma de apreciação e discussão de projeto de lei na Casa dos Comuns, definindo o tempo limite para debate em cada uma de suas etapas. Ver em https://www.parliament.uk/site-information/glossary/programme-motion/. Último acesso 10/0/2023.

[45] Para maiores detalhes quanto a tramitação do projeto ver https://bills.parliament.uk/bills/3137/stages. Último acesso 10/07/2023.

[46] Imaginava-se que a bula seria encaminhada para assentimento real a tempo da coroação, em maio de 2023. No entanto, quando esta ocorreu, a OSB ainda se encontrava em estágio de segunda leitura. Diferentemente do que ocorre com as prorrogações e limitação de tempo de apreciação para cada etapa legislativa na Casa dos Comuns, na Casa dos Lordes não existe o instituto da *Programme Motion,* e a bula pode ser discutida nesta casa por tempo indeterminado.

[47] Disponível em https://bills.parliament.uk/publications/52368/documents/3841 Último acesso em 15/08/2023.

O presente subcapítulo e a conseguinte análise crítica do modelo regulatório britânico, essa última a ser desenvolvida ao longo do capítulo 4, têm como recorte a mais recente versão integral do projeto da *Online Safety Bill*, publicada em 19 de julho de 2023 e referenciada na bibliografia deste trabalho. Tratando-se da última edição antes de serem juntadas manifestações dos Comuns às emendas feitas pelos Lordes, poucos detalhes foram modificados antes do texto ganhar força de lei. Uma vez que o OSA, nesse momento, consiste em extenso texto legal, com o qual se busca abranger ampla série de detalhes técnicos que extravasam o campo de interesse aqui proposto, optou-se por introduzir brevemente conceitos-chave da lei, e, a seguir, explorar quatro pontos sensíveis que deverão ser analisados criticamente. São eles: [1] os deveres de cuidado e os deveres especiais; [2] os deveres de transparência e de disponibilização de dados de usuários, por parte das plataformas, especialmente para proteção de crianças; [3] a possibilidade de responsabilização de agentes intermediários por conteúdos de terceiros divulgados em suas redes, em decorrência dos deveres de cuidado e dos deveres especiais; [4] e os poderes conferidos à autoridade reguladora, o OFCOM.

3.4.1. Notas introdutórias e conceitos-chave no OSA.

Subdividida em 12 partes (as quais, como antes mencionado, se subdividem em capítulos, que a sua vez se subdividem em seções), o OSA consolida texto de enorme abrangência, aportando disposições gerais para controle de conteúdo, e disposições especiais para controle de conteúdos específicos. Dentre esses conteúdos específicos, com os quais a lei é especialmente rigorosa, destacam-se os conteúdos potencialmente nocivos a crianças, os conteúdos terroristas, os conteúdos que façam apologia à violência de qualquer espécie, os conteúdos que incitam ódio, os conteúdos que incentivam comportamentos autodestrutivos ou suicidas, os conteúdos que incentivam violência sexual ou de gênero e os conteúdos que veiculam pornografia de qualquer tipo[48].

Na sua Parte 2, o atual texto do OSA traz definições-chave para delimitar e recortar quais agentes e atividades devem ser regidos pela nova lei. De início, o projeto volta-se a definir os tipos de serviço que deverão ser regulados, e separa os serviços de "usuário-a-usuário" dos

[48] Ver comentários gerais ao formato final da OSB publicados pelo governo britânico em: https://www.gov.uk/government/news/britain-makes-internet-safer-as-online-safety-bill-finished-and-ready-to-become-law. Último acesso 03/10/2023.

serviços de busca. Por serviços de "usuário-a-usuário", a lei refere-se àquele "serviço de internet por meio do qual o conteúdo gerado diretamente por um usuário, ou carregado ou compartilhado no serviço por um usuário do serviço, pode ser encontrado por outro usuário, ou outros usuários, do serviço" (Reino Unido, 2023, p. 14). Sobre esses serviços, é indiferente se o conteúdo em discussão é efetivamente compartilhado com outros usuários, não importando também qual a relevância desse material em comparação aos demais conteúdos da mesma rede[49]. Por serviços de busca, o OSA volta-se a regular qualquer serviço de internet "que consiste ou inclui mecanismo de busca" (Reino Unido, 2023, p. 15). A lei prevê também a possibilidade de alguns serviços serem enquadrados como mistos, em especial quando serviços de "usuário-a-usuário" disponibilizam mecanismos de busca, e vice-versa.

Tratando-se as plataformas de internet de portais transnacionais, cuja sede administrativa comumente se encontra fora do território britânico, o OSA define seu escopo geográfico ao delimitar que os serviços regulados serão aqueles que mantêm "vínculos com o Reino Unido", salvo exceções arroladas em lei. Por vínculos com o Reino Unido, compreende-se os "serviços com número significativo de usuários no Reino Unido"; ou aqueles serviços nos quais "o Reino Unido forma um de seus alvos de mercado"; ou "serviços possíveis de serem utilizados por indivíduos no Reino Unido", ou aqueles sobre os quais há razões suficientes para acreditar que existe risco material de dano significativo a indivíduos no Reino Unido em razão de conteúdos presentes em serviços de "usuário-a-usuário" ou serviços de busca (Reino Unido, 2023, p. 16).

Crucial para compreender a estrutura regulatória do OSA é a definição dos intitulados "serviços de Categoria 1", "serviços de Categoria 2A", e "serviços de Categoria 2B". Foi por meio dessas classificações que o Parlamento procurou isolar grandes plataformas de busca e de "usuário-a-usuário", separando-as regulatória e administrativamente de portais de menor envergadura. Serviços de categorias especiais, desse modo, têm deveres adicionais em relação aos serviços de menor porte. O Parlamento também buscou, com isso, proteger pequenos empresários que tentem inovar no ramo virtual. O projeto prevê que, uma vez que o OSA ganhasse força de lei, a autoridade reguladora – no caso, o OFCOM – deverá empreender pesquisa e, posteriormente, divulgar parâmetros a fim de esclarecer quais plataformas se enquadram em cada uma das categorias. Para isso, o OFCOM terá de levar em conta o número de usuários de cada serviço, as funcionalidades específicas de cada um deles, bem como outros

[49] Serviços de SMS, e-mail, ou conversa por vídeo são excetuados e enquadrados como serviços de busca, observadas o especificado nos parágrafos 1, 2, 3, 4 e 7 da Schedule 1 da OSB (Reino Unido, 2023, p. 250).

elementos que o Secretário de Estado entenda relevantes para a categorização. É interessante observar que o OSA não vai mais a fundo do que isso para definir quais padrões mínimos deverão ser observados para categorizar plataformas, delegando boa parte dessa tarefa à autoridade reguladora. Prevê-se que os serviços de *Categoria 1 serão aqueles de "usuário-a-usuário" de maior relevância, os de Categoria 2A serão os serviços de busca de maior relevância, e os serviços de Categoria 2B serão parte de plataformas que, apesar de voltadas a outras finalidades, prestem serviços de "usuário-a-usuário"* (Reino Unido, 2023, p. 265-266). Uma vez fixados os parâmetros que determinam quais os requisitos para cada categorização, o OFCOM deverá publicar e manter atualizada lista de quais plataformas enquadram-se em cada categoria. A autoridade reguladora deverá manter, também, lista de quais plataformas estão a emergir como de Categoria 1, 2A, ou 2B (Reino Unido, 2023, p. 100), para fins de controle público do tamanho e influência que cada plataforma atuante no ciberespaço britânico tende a assumir.

3.4.2 Deveres de cuidado.

Todos os provedores de serviços de internet com ligações com o Reino Unido deverão, a partir da vigência do OSA e da fixação de códigos de boas práticas pelo OFCOM, observar uma série de deveres de cuidado estipulados no corpo da lei. É mediante o estabelecimento desses deveres de cuidado e de deveres especiais que o Parlamento busca atribuir responsabilidade direta a plataformas de internet, com evidente esforço por responsabilizar provedores em diferentes graus e medidas, a depender de sua relevância e do tipo de serviço prestado. A rigidez desses deveres é ainda mais severa para serviços passíveis de serem acessados por crianças. Sobre esse ponto, é de notoriedade pública o quanto o OSA, desde a publicação do DOSB, vem enveredando no sentido de se tornar uma lei para proteção especialmente de usuários menores de idade, em claro movimento de substituição da estratégia outrora proposta no DEA 2017 (The Cyberlaw [...], 2023). Para alcançar tal objetivo, o texto legal elenca deveres a serem cumpridos a depender da categorização que o OFCOM fizer caber a cada plataforma, trabalhando amiúde cada uma delas e delegando à autoridade reguladora a elaboração dos critérios administrativos e técnicos para sejam cumpridas essas determinações. Nesse ponto, é importante observar que o OSA separa deveres de cuidado (estes que estamos a tratar, dispostos na Parte 3 do OSA), dos deveres especiais (a serem comentados mais adiante,

dispostos quase todos na Parte 4 da lei). Não obstante a separação consolidada no OSA entre deveres de cuidado e deveres especiais seja consideravelmente confusa, é certo que ambas as categorias têm o condão de ensejar a responsabilização de provedores de plataformas.

Tratando-se o OSA de projeto extenso e minimalista, não há espaço neste trabalho para esmiuçar, um a um, todos os deveres ali impostos. Desse modo, serão tratadas apenas as mais relevantes atribuições fixadas nas Partes 3 e 4, para posterior análise crítica. No tocante aos deveres de cuidado, serão aqui referidos os deveres de cuidado gerais para serviços de "usuário-a-usuário" e os deveres de cuidado especiais para serviços de busca, de Categoria 1 e de Categoria 2A. A seguir, serão elencados o que se julgou serem os mais relevantes deveres especiais trazidos pela nova lei. Para melhor compreensão da exposição que aqui se constrói, segue tabela onde estão dispostos os deveres ora trabalhados.

{1} Deveres de Cuidado.	**[1] Deveres de Cuidado de serviços "usuário-a-usuário".** a) Dever de avaliação periódica de riscos de conteúdos ilegais. b) Deveres de segurança sobre conteúdos ilegais, com atribuições especiais aos serviços de Categoria 1. c) Deveres de avaliação de riscos para crianças para todos os serviços de "usuário-a-usuário" passíveis de serem utilizados por crianças. d) Deveres para segurança e proteção de crianças. e) Deveres de reportar conteúdos. f) Deveres sobre liberdade de expressão e privacidade, com atribuições especiais aos serviços de Categoria 1. g) Deveres de manutenção de registros e revisão, com atribuições especiais aos serviços de Categoria 1.
	[2] Deveres de Cuidado para serviços de busca e serviços de Categoria 2A. a) Dever de avaliação de riscos de conteúdos ilegais. b) Dever de segurança com relação a conteúdos ilegais, com atribuições especiais a serviços de Categoria 2A. c) Dever de reportar conteúdos específicos ao OFCOM. d) Dever de produzir e disponibilizar procedimento de reclamação para usuários. e) Deveres de cuidado relacionados à liberdade de expressão e privacidade dos usuários. f) Deveres de manutenção de registros e revisão de políticas. g) Serviços de busca passíveis de serem utilizados por crianças deverão, em adição ao exposto, comprometer-se com a avaliação periódica de riscos para crianças e com o dever de atuar em prol da garantia da segurança *online* de crianças.
	[3] Deveres de Cuidado para serviços de Categoria 1.

	a) Dever de avaliação de riscos para empoderamento de usuários e implementação de mecanismos para filtragem de conteúdo. b) Dever de proteção de conteúdo de importância democrática. c) Dever de proteção de conteúdos de empresas de edição de notícias. d) Dever de proteção de conteúdos jornalísticos. e) Todos os demais deveres de cuidado para serviços de usuário-a-usuário e deveres especiais.
{2} Deveres Especiais.	**[1] Deveres Especiais para serviços passíveis de serem utilizados ou acessados por crianças.** a) Dever de realização de avaliação do serviço para demonstrar se é utilizável por crianças, e em qual medida. b) Dever de avaliação periódica de riscos para crianças, para serviços de Categoria 1 e 2A. c) Dever de reportar conteúdos abusivos e de exploração sexual infantil à *National Crime Agency*. d) Dever de divulgação de dados de usuários infanto-juvenis falecidos.
	[2] Deveres Especiais de identificação de usuários para serviços de Categoria 1. a) Dever de Serviços de Categoria 1 de oferecer a opção de verificação de identidade para aceder ao portal.
	[3] Deveres Especiais de transparência, com atribuições especiais para serviços de Categoria 1, 2A e 2B. a) Dever de não atuar contra usuários, com exceção das condições expressamente previstas em termos de serviços. b) Dever, para Serviços de Categoria 1, Categoria 2A e Categoria 2B, de apresentar relatórios anuais de transparência.
	[4] Deveres Especiais de pagar taxas.

3.4.2.1 Deveres de cuidado de serviços "usuário-a-usuário".

No tocante aos deveres de cuidado gerais para serviços de "usuário-a-usuário", o OSA fixa as seguintes obrigações, que vão aqui listadas. [a] Dever de avaliação periódica de riscos de conteúdos ilegais[50], a ser empreendida e publicada nos termos e prazos estipulados pelo

[50] Uma avaliação de conteúdo ilegal de risco significa uma avaliação dos seguintes quesitos, levando em conta o perfil de risco do tipo de serviço: (1) a base do usuário; (2) o nível de risco de indivíduos usuários do serviço quando encontrando os seguintes: [a] cada tipo de conteúdo ilegal prioritário, [b] outros tipos de conteúdo ilegal. Levando em consideração os algoritmos usados pelo sistema e seu poder de difusão/velocidade de difusão de

OFCOM, [b] e deveres de segurança sobre conteúdos ilegais[51], com a determinação especial para serviços de Categoria 1 resumirem, em seus termos de serviço, os achados de sua avaliação de risco mais recente. [c] São também fixados deveres de avaliação de riscos para crianças para todos os serviços de "usuário-a-usuário" passíveis de serem utilizados por crianças[52]; [d]

conteúdo; [c] o nível do risco de o serviço ser utilizado para cometimento ou facilitação de uma *priority offence*; [d] o risco de dano contra indivíduos expostos a conteúdos ilegais através do serviço, para fins de cometimento ou facilitação de uma *priority offence*; [e] o risco de as funcionalidades do serviço facilitarem a presença ou disseminação de conteúdo ilegal, ou o uso desse serviço para cometimento de ofensas, identificando e avaliando as funcionalidades que permitem tais riscos; [f] os diferentes modos através dos quais o serviço é utilizado, e o impacto de tais usos nas chances de possíveis danos causados aos usuários; [g] a natureza e a severidade do dano que pode ser causado aos indivíduos usuários; [h] como o design e a operacionalização do serviço (incluindo o modelo de negócio, governança, uso proativo da tecnologia, meio de promover a alfabetização digital dos usuários e uso seguro do serviço, além de outros sistemas) podem servir a reduzir ou aumentar os riscos identificados [tradução nossa] (Reino Unido, 2023, p. 18).

[51] Por dever sobre conteúdos ilegais, entenda-se: [1] o dever, em relação ao serviço, de usar ou tomar as medidas proporcionais e necessárias com relação ao design ou operacionalidade do serviço para: [a] prevenir que indivíduos encontrem conteúdos ilegais prioritários através do uso do serviço; [b] efetivamente mitigar e gerenciar o risco de o serviço ser utilizado para o cometimento ou facilitação de *priority offence*, como identificado na mais recente avaliação de risco e; [c] efetivamente mitigar e gerenciar os riscos de dano a indivíduos, como identificado na mais recente avaliação de risco. [2] O dever de operar o serviço utilizando sistemas proporcionais e processos desenhados para: [a] minimizar o tempo durante o qual qualquer conteúdo ilegal prioritário é disponibilizado e; [b] quando o provedor for alertado por uma pessoa sobre a presença de qualquer conteúdo ilegal, rapidamente retirá-lo do ar. [3] Os deveres mencionados acima se aplicam a todas as áreas de operação do serviço, incluindo seu design, operação e modos de uso, bem como os conteúdos disponibilizados, e (entre outras coisas) requer que o provedor tome medidas nas seguintes áreas, caso necessário e proporcional: [a] compliance regulatória e arranjos para gerenciamento de riscos; [b] design de funcionalidades, algoritmos e outras ferramentas; [c] políticas nos termos de uso; [d] política de acesso a determinados tipos de conteúdo, incluindo o bloqueio de usuários para determinados conteúdos; [e] moderação de conteúdo, incluída sua supressão; [f] funcionalidades para que o usuário controle os conteúdos que chegam até ele; [g] medidas de apoio ao usuário; [h] políticas e práticas para funcionários. [4] O dever de incluir provisões nos termos de serviço especificando como indivíduos serão protegidos de conteúdo ilegal, endereçando cada parágrafo da subseção 3, com especial endereçamento ao que se refere a CSEA e outros conteúdos ilegais prioritários. [5] O dever de incluir previsões nos termos de serviço sobre qualquer tecnologia proativa utilizada para fins de *compliance* com os deveres mencionados em 1 e 2, incluindo o tipo de tecnologia empregada e como ela funciona. [6] Para fins de determinar o que é proporcional com relação aos deveres mencionados, considerar os seguintes fatores: [a] todas as conclusões da avaliação de risco de conteúdos ilegais mais recente e; [b] o tamanho e a capacidade do provedor de serviços [tradução nossa] (Reino Unido, 2023, págs. 19-23).

[52] A avaliação de risco para crianças usuárias de um serviço significa uma avaliação dos seguintes aspectos, levando em consideração o perfil de risco de cada serviço: [a] a base de usuários, incluindo o numero de usuários que são crianças e seus diferentes grupos de idade; [b] o nível de risco de usuários crianças encontrarem os seguintes conteúdos através do serviço: [b.1] cada tipo de conteúdo de prioridade primária que é danoso para crianças; [b.2] cada tipo de conteúdo de prioridade que é danoso para crianças; [b.3] conteúdos danosos para crianças não designados, sempre levando em consideração os diferentes grupos de idade, os algoritmos utilizados pelo serviço, e a possibilidade de disseminação desses conteúdos; [c] o nível de risco de dano de diferentes tipos de conteúdos danosos para crianças; [d] o nível de risco de alguns conteúdos para determinados grupos ou tipos de indivíduos; [e] o nível de risco das funcionalidades do serviço para facilitar a presença ou disseminação de conteúdo danoso para crianças, avaliando cada uma dessas funcionalidades (com destaque para as ferramentas que permitem que adultos encontrem e contatem outros usuários do serviço, inclusive crianças); [f] os diferentes modos que o serviço é utilizado e seus impactos; [g] a natureza e a severidade dos danos que podem ser sofridos por usuários crianças; [h] como o design e a operacionalização do serviço (incluindo o modelo de negócio, governança, uso proativo da tecnologia, meio de promover a

deveres para segurança e proteção de crianças[53]; [e] deveres de reportar conteúdos[54]; [f] e deveres sobre liberdade de expressão e privacidade[55]. Com relação a esse último ponto, o OSA prevê atribuições especiais para serviços de Categoria 1 de realizar e manter atualizada avaliação de impactos, sempre que medidas de segurança alterem o *design* da plataforma. [g] Por fim, o OSA impõe deveres de manutenção de registros e revisão[56], com atribuição especial aos serviços de Categoria 1 de manter registro de métodos e achados de cada uma de suas avaliações de risco (Reino Unido, 2023).

3.4.2.2 Deveres de cuidado para serviços de busca e serviços de Categoria 2A.

alfabetização digital dos usuários e uso seguro do serviço, além de outros sistemas) podem servir a reduzir ou aumentar os riscos identificados [tradução nossa] (Reino Unido, 2023, págs. 23-25).

[53] O dever, em relação ao serviço, de usar ou tomar as medidas proporcionais e necessárias com relação ao design ou operacionalidade do serviço para: [a] mitigar e gerenciar os riscos de danos a crianças de diferentes grupos de idade, conforme a avaliação de riscos para crianças mais recente; [b] mitigar o impacto do dano para crianças de diferentes grupos de idade impostos por conteúdos presentes no serviço; [c] evitar que crianças de qualquer idade encontrem conteúdo de prioridade primária que é danoso para crianças (através de mecanismos de verificação de idade, por exemplo); [d] proteger crianças em grupos de idade específicos, os quais se entendem que estariam em risco de dano se em contato com determinados conteúdos, de ter acesso a estes [tradução nossa] (Reino Unido, 2023, p. 25).

[54] Dever de operar um serviço usando sistemas e processos que permitem aos usuários e pessoas afetadas denunciar facilmente o conteúdo que consideram ser conteúdo de um tipo especificado abaixo (com o dever se estendendo a diferentes tipos de conteúdo, dependendo do tipo de serviço). Todos os serviços têm o dever de reportar conteúdos ilegais. Serviços passíveis de serem acessados por crianças têm o dever adicional de remoção de conteúdos potencialmente danosos a crianças [tradução nossa] (Reino Unido, 2023, p.33).

[55] "Ao decidir e implementar medidas e políticas de segurança, dever-se-á ter particular atenção à importância de proteger o direito à liberdade de expressão dos utilizadores dentro da lei. Outrossim, ao decidir e implementar medidas e políticas de segurança, o dever de ter atenção especial à importância de proteger os usuários de uma violação de qualquer disposição estatutária ou regra de direito relativa à privacidade que seja relevante para o uso ou operação de um usuário para - atendimento ao usuário [tradução nossa] (Reino Unido, 2023, p. 36).

[56] O dever de produzir e manter registro escrito, de forma facilmente compreensível, sobre todos os aspectos de cada avaliação de risco, incluindo detalhes sobre como a avaliação foi realizada e suas conclusões. Dever de fazer e manter um registro escrito de quaisquer medidas tomadas ou em uso para cumprir um dever relevante que (a) sejam descritas em um código de prática e recomendadas para fins de cumprimento do dever em questão, e (b) aplicam-se em relação ao prestador e ao serviço em questão. Especificar e tornar público se medidas alternativas foram tomadas ou estão em uso para cumprir um dever relevante, bem como o dever de fazer e manter um registro escrito contendo as seguintes informações: (a) as medidas aplicáveis em um código de prática que não foram tomadas ou não estão em uso, (b) as medidas alternativas que foram tomadas ou estão em uso, (c) como essas medidas alternativas equivalem ao cumprimento do dever em questão, e (d) como o provedor cumpriu a seção 49 (liberdade de expressão e privacidade). Por fim, há o dever de revisar a conformidade com os deveres relevantes em relação a um serviço: (a) regularmente, e (b) assim que razoavelmente praticável após fazer qualquer alteração significativa em qualquer aspecto do projeto ou operação do serviço [tradução nossa] (Reino Unido, 2023, p. 38).

De modo semelhante, para serviços de busca, o OSA estabelece dever de cuidado de [a] proceder avaliação de riscos de conteúdos ilegais[57]; [b] dever de segurança com relação a conteúdos ilegais[58], com atribuições especiais a serviços de Categoria 2A para resumir e publicar as conclusões de sua mais recente avaliação de risco de conteúdos ilegais. [c] Há também o dever de reportar conteúdos específicos ao OFCOM[59]; [d] o dever de produzir e disponibilizar procedimento de reclamação para usuários[60]; [e] os deveres de cuidado

[57] De modo diverso do fixado para serviços de usuário-a-usuário, para serviços de busca em geral a OSB define que avaliação de riscos "de um serviço de um tipo específico significa uma avaliação dos seguintes assuntos, levando em consideração o perfil de risco relacionado a serviços desse tipo: (a) o nível de risco de indivíduos que são usuários do serviço encontrando conteúdo de pesquisa dos seguintes tipos [i] cada tipo de conteúdo ilegal prioritário (com cada tipo avaliado separadamente) e [ii] outro conteúdo ilegal, levando em conta (em particular) os riscos apresentados por algoritmos usados pelo serviço, e a forma como o serviço indexa, organiza e apresenta os resultados da pesquisa; (b) o nível de risco das funcionalidades do serviço que facilitam que os indivíduos encontrem conteúdo de pesquisa que seja ilegal, identificando e avaliando as funcionalidades que apresentam níveis de risco mais elevados; (c) a natureza e a gravidade dos danos que podem ser sofridos pelos indivíduos em decorrência dos assuntos identificados de acordo com os parágrafos (a) e (b); e (d) como o design e a operação do serviço (incluindo o modelo de negócios, governança, uso de tecnologia proativa, medidas para promover a alfabetização midiática dos usuários e o uso seguro do serviço e outros sistemas e processos) podem reduzir ou aumentar os riscos identificado [tradução nossa] (Reino Unido, 2023, p. 40).

[58] De forma diversa do fixado para serviços de usuário-a-usuário, a OSB aqui determina que o dever de segurança é o "dever de operar um serviço usando sistemas e processos proporcionais projetados para minimizar o risco de indivíduos encontrarem conteúdo de pesquisa dos seguintes tipos: (a) conteúdo ilegal prioritário; (b) outro conteúdo ilegal de que o provedor tenha conhecimento (tendo sido alertado por outra pessoa ou tomado conhecimento de qualquer outra forma). As obrigações definidas nas subseções (2) e (3) se aplicam a todas as áreas de um serviço, incluindo a forma como o mecanismo de pesquisa é projetado, operado e usado, bem como o conteúdo de pesquisa do serviço e (entre outras coisas) exigir que o provedor de um serviço tome ou use medidas nas seguintes áreas, se for apropriado fazê-lo (a) conformidade regulatória e arranjos de gerenciamento de risco, (b) design de funcionalidades, algoritmos e outros recursos relacionados à pesquisa mecanismo, (c) funcionalidades que permitem aos usuários controlar o conteúdo que encontram nos resultados de pesquisa, (d) priorização de conteúdo, (e) medidas de suporte ao usuário e (f) políticas e práticas de equipe. Há também o dever de incluir provisões em uma declaração publicamente disponível especificando como os indivíduos devem ser protegidos de conteúdo de pesquisa que seja conteúdo ilegal. Bem como o dever de incluir disposições em uma declaração publicamente disponível dando informações sobre qualquer tecnologia proativa usada por um serviço para fins de cumprimento de um dever estabelecido na subseção (2) ou (3) (incluindo o tipo de tecnologia, quando é usado e como funciona). O dever de garantir que as disposições da declaração publicamente disponível referidas nas subseções (5) e (7) sejam claras e acessíveis" [tradução nossa] (Reino Unido, 2023, p. 40-41).

[59] "Dever de operar um serviço usando sistemas e processos que permitam aos usuários e pessoas afetadas denunciar facilmente conteúdo de pesquisa que considerem ser conteúdo do tipo especificado abaixo (com o dever se estendendo a conteúdo que seja prejudicial às crianças, dependendo do tipo de serviço, conforme indicado pelos títulos)". Para qualquer tipo de serviço de busca, a lei se refere apenas a "conteúdos ilegais", para serviços de busca passíveis de serem utilizados por crianças, a lei se refere a "conteúdos potencialmente danosos para crianças" [tradução nossa] (Reino Unido, 2023, p. 45).

[60] "Dever de operar um procedimento de reclamação em relação a um serviço que: (a) permita a apresentação de tipos relevantes de reclamação, (b) preveja quais medidas apropriadas devem ser tomadas pelo fornecedor de o serviço em resposta a reclamações de tipo relevante, e (c) seja de fácil acesso, fácil de usar (inclusive por crianças) e transparente." Este dever inclui "o dever de tornar as políticas e processos que regem o tratamento e resolução de reclamações de um tipo relevante, publicamente disponível e facilmente acessível (incluindo para crianças)" [tradução nossa] (Reino Unido, 2023, p. 45-46). Por "tipos relevantes de reclamação", o OSB privilegia conteúdos regulados por ela mesma - a exemplo de conteúdos ilegais, deveres de cuidado com

relacionados à liberdade de expressão e privacidade dos usuários[61]; [f] e os deveres de manutenção de registros e revisão de políticas[62]. Serviços de busca passíveis de serem utilizados por crianças deverão, em adição ao exposto, [g] comprometer-se com a avaliação periódica de riscos para crianças[63] e [h] com o dever de atuar em prol da garantia da segurança *online* de crianças (Reino Unido, 2023, p. 38-39).

3.4.2.3 Deveres de cuidado especiais para serviços de Categoria 1.

Com relação aos serviços de Categoria 1, gênero no qual as plataformas mais populares da internet tendem a ser enquadradas pelo OFCOM (a exemplo de *WhatsApp*, *TikTok*, *Instagram* e *Discord*), o OSA se mostra muitíssimo criterioso, fixando uma série de deveres específicos. Isso é, além dos deveres mencionados na subseção 3.4.2.1 , e à parte dos deveres especiais para serviços passíveis de serem utilizados por crianças (3.4.3.1), o

liberdade de expressão, deveres de cuidado com transparência e avaliação de riscos, serviços passíveis de serem acessados por crianças, etc.

[61] "Ao decidir e implementar medidas e políticas de segurança, é dever ter especial atenção à importância de proteger os direitos dos utilizadores e pessoas interessadas à liberdade de expressão dentro da lei." Outrossim, "ao decidir e implementar medidas e políticas de segurança, o dever de ter especial atenção à importância de proteger os utilizadores de uma violação de qualquer disposição legal ou norma jurídica relativa à privacidade que seja relevante para a utilização ou operação de um serviço de pesquisa (incluindo, mas não limitado, a qualquer disposição ou regra relativa ao processamento de dados pessoais)" [tradução nossa] (Reino Unido, 2023, p. 47).

[62] Idênticos aos deveres de manutenção de registros e revisão fixados para serviços de usuário-a-usuário (Reino Unido, 2023, p. 47).

[63] Diversamente da avaliação devida por serviços de usuário-a-usuário, serviços de busca deverão atentar aos seguintes pontos para avaliação de risco para usuários crianças: "significa uma avaliação das seguintes questões, tendo em conta o perfil de risco relacionado com serviços desse tipo: (a) o nível de risco das crianças utilizadoras do serviço encontrar conteúdo de pesquisa dos seguintes tipos: (i) cada tipo de conteúdo de prioridade primária que é prejudicial às crianças (com cada tipo avaliado separadamente), (ii) cada tipo de conteúdo prioritário que é prejudicial às crianças (com cada tipo avaliado separadamente) , e (iii) conteúdo não designado que seja prejudicial às crianças, dando atenção à parte às crianças de diferentes faixas etárias, e tendo em conta os riscos apresentados pelos algoritmos utilizados pelo serviço e a forma como o serviço indexa, organiza e apresenta resultados de pesquisa; (b) O nível de risco de as crianças que utilizam o serviço encontrarem conteúdos de pesquisa prejudiciais para as crianças, que afetam particularmente indivíduos com uma determinada característica ou membros de um determinado grupo; (c) O nível de risco das funcionalidades do serviço que facilitam às crianças o encontro com conteúdos de pesquisa que são prejudiciais para as crianças, identificando e avaliando as funcionalidades que apresentam níveis de risco mais elevados; (d) a natureza e a gravidade dos danos que podem ser sofridos pelas crianças devido às questões identificadas de acordo com os parágrafos (a) a (c), dando consideração separada às crianças em diferentes faixas etárias; (e) De que forma a concessão e o funcionamento do serviço (incluindo o modelo de negócio, governança, utilização de tecnologia proativa, medidas para promover o letramento digital dos utilizadores e a utilização segura do serviço, e outros sistemas e processos) podem reduzir ou aumentar os riscos identificado" [tradução nossa] (Reino Unido, 2023, p. 43).

Parlamento dedicou seção à parte para definição de deveres de cuidados específicos para as companhias que forem classificadas como de Categoria 1, as quais vão referenciadas a seguir.

O polêmico "dever de remoção de conteúdos legais, porém nocivos", antes mencionado e outrora proposto no DOSB para provedores de Categoria 1, foi substituído por mecanismo ora intitulado "triplo escudo"[64]. Esse último é composto pela combinação de três fatores que, atuando conjuntamente, deverão inibir a circulação de conteúdos potencialmente nocivos pelas redes. O triplo escudo, desse modo, é formado pela soma do dever de remoção de conteúdos ilegais, com o dever de remoção de conteúdo declarado como nocivo nos termos de serviços de cada companhia, e o dever de empoderamento de usuários adultos, a fim de que esses últimos tenham a seu dispor ferramentas que viabilizem a filtragem de conteúdos. Como consequência dos deveres fixados pelo triplo escudo, houve o estabelecimento, pelo OSA, de uma série de deveres de cuidado, direcionados especificamente aos servidores de Categoria 1. Dentre esses, ganham destaque [a] o dever de avaliação de riscos para empoderamento de usuários adultos[65] e implementação de mecanismos de empoderamento de usuários para filtragem de conteúdo; [b] o dever de proteção de conteúdo de importância democrática[66]; [c]

[64] Ver em https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill. Último acesso em 29/08/2023.

[65] Uma avaliação de um serviço para os fins desta seção [15(2)] significa "uma avaliação dos seguintes assuntos: (a) a base de usuários; (b) a incidência de conteúdo relevante no serviço; (c) a probabilidade de utilizadores adultos do serviço encontrarem, através do serviço, cada tipo de conteúdo relevante (sendo cada tipo avaliado separadamente), tendo em conta os algoritmos utilizados pelo serviço e a facilidade, rapidez com que o conteúdo pode ser divulgado por meio do serviço; (d) a probabilidade de utilizadores adultos com uma determinada característica ou que sejam membros de um determinado grupo encontrarem conteúdos relevantes que os afetem particularmente; (e) a probabilidade de as funcionalidades do serviço facilitarem a presença ou difusão de conteúdos relevantes, identificando e avaliando as funcionalidades mais suscetíveis de o fazer; (f) as diferentes formas como o serviço é utilizado e o impacto dessa utilização na probabilidade de os utilizadores adultos encontrarem conteúdos relevantes; (g) como a concepção e o funcionamento do serviço (incluindo o modelo de negócio, a governança, a utilização de tecnologia proativa, as medidas para reforçar o controlo dos utilizadores adultos sobre a sua interação com conteúdos gerados pelos utilizadores e outros sistemas e processos) podem reduzir ou aumentar a probabilidade de usuários adultos que encontram conteúdo relevante" [tradução nossa] (Reino Unido, 2023, p. 26).

[66] " O dever de operar um serviço usando sistemas e processos proporcionais projetado para garantir que a liberdade expressão de conteúdos de importância democrática seja levada em consideração na tomada de decisões sobre: (a) como tratar esse conteúdo (especialmente decisões sobre removê-lo ou restringir o acesso dos usuários a ele), e (b) tomar medidas contra um usuário que gera, carrega ou compartilha tal conteúdo. Dever de garantir que os sistemas e processos mencionados se apliquem da mesma forma a uma ampla diversidade de opiniões políticas. Dever de incluir disposições nos termos de serviço especificando as políticas e processos concebidos para levar em conta o princípio mencionado na subseção (2), incluindo, em particular, como esse princípio é aplicado às decisões mencionadas nessa subseção. Dever de garantir que: (a) as disposições dos termos de serviço referidos sejam claras e acessíveis, e (b) essas disposições sejam aplicadas de forma consistente. Ao determinar o que é proporcional, a dimensão e a capacidade do prestador de um serviço, em particular, são relevantes" [tradução nossa] (Reino Unido, 2023, p. 29).

o dever de proteção de conteúdos de empresas de edição de notícias[67]; [d] e o dever de proteção de conteúdos jornalísticos.

3.4.3 Deveres especiais para serviços regulados de "usuário-a-usuário" e serviços regulados de busca.

3.4.3.1 Deveres para serviços passíveis de serem acessados por crianças, dever de reportar conteúdo de abuso e exploração sexual infantil e dever de divulgação de dados pessoais de usuários infanto-juvenis falecidos.

Os meios regulatórios mais eficazes para controle de conteúdo da internet, é sabido, são ainda desconhecidos. Tratando-se de fenômeno novel e dinâmico, o debate sobre como abordar o tema segue longe de pacificado, e, de momento, nenhuma solução proposta ou imposta se mostra inequivocamente promissora. Ao transitar por terreno de tamanha instabilidade, o OSA já passou por inúmeras alterações estruturais, de sorte que a proposta apresentada em 2021 pouco guarda em comum com a forma final do projeto regulatório. No curso do processo legislativo, o OSA foi paulatinamente cedendo em sua rigidez para fins de controle de conteúdo geral, passando a focar no controle de conteúdo nocivo para crianças em medida muito superior ao controle de conteúdo adulto. Com a finalidade de colocar em prática esse objetivo, o OSA atribuiu a qualquer plataforma o [a] dever especial de realização de avaliação do serviço para demonstrar se essa é, ou não, utilizável por crianças, e em qual medida. A partir desse ponto, é interessante observar que não se está mais a tratar de deveres de cuidado e da responsabilização objetiva dos atores regulados, mas sim da atribuição de obrigações práticas e pontuais, os chamados deveres especiais. A avaliação deve buscar informar se é possível que crianças acedam ao serviço ou à parte dele, e, se for possível o acesso de crianças, em qual parte do serviço isso ocorre. Deve-se investigar, ainda, o quão provável é que crianças venham a utilizar o serviço ou parte dele, analisando o potencial de a plataforma ser alvo de usuários crianças, levando em consideração o número de usuários menores de idade e o quão atrativo é o portal para o público infanto-juvenil. Os achados deverão ser depositados junto ao OFCOM, e qualquer modificação estrutural nesta seara deverá ser estudada e informada à autoridade reguladora. Além disso, é somente após a realização de tal avaliação e

[67] Dever de notificar e comunicar ao editor de notícias antes de: "(a) tomar medidas em relação ao conteúdo presente no serviço que seja conteúdo de editor de notícias, ou (b) tomar medidas contra um usuário que é um editor de notícias reconhecido" [tradução nossa] (Reino Unido, 2023, p. 30).

mediante a implementação de sistemas de verificação de identidade (ver subcapítulo 3.4.3.2) que será possível para uma plataforma comprovar, ante o OFCOM, que as determinações do OSA para serviços passíveis de serem acessados por crianças não devem incidir sobre seus respectivos portais (Reino Unido, 2023, p. 48-49). Serviços que provem não serem de provável acesso por crianças deverão repetir a avaliação regularmente, com periodicidade não superior a um ano, ou anteriormente a qualquer mudança de *design* da plataforma.

Ademais da análise específica para avaliar a utilização do serviço por crianças, há no OSA determinações para fixação de [b] deveres específicos para serviços de busca, de "usuário-a-usuário", de Categoria 1 e de Categoria 2A, os quais periodicamente deverão realizar avaliação de riscos para crianças. Eles também deverão atuar *ativamente*, por meio de ferramentas de *design*, a fim de prevenir de que usuários infanto-juvenis tenham acesso a conteúdos nocivos por intermédio de suas plataformas.

O OSA traz, ainda, a conceituação de Conteúdo Abusivo e de Exploração Sexual Infantil[68] (CAESI), com o objetivo de exigir que toda plataforma de serviços "usuário-a-usuário" [c] implemente sistema que permita que qualquer CAESI[69] seja reportado pela plataforma diretamente à *National Crime Agency* (NCA), "na medida do possível". A proposta, ao determinar o contato direto entre *bigtechs* e a principal agência criminal do Reino Unido, se esforça por imprimir agilidade no controle de conteúdos sensíveis direcionados a crianças usuárias da rede. Na mesma senda, há a determinação para que todo serviço de busca regulado implemente sistemas e processos que garantam, "na medida do possível", que qualquer CAESI detectado e ainda não reportado, dentre aqueles passíveis de serem localizados na base de dados do sistema de busca, seja denunciado por usuários à NCA (Reino Unido, 2023, p. 75). A prestação de informações falsas ou parciais, mediante dolo ou culpa, configura crime sob o OSA, com previsão de pena de multa e de até 2 anos de encarceramento[70] (Reino Unido, 2023, p. 77). Por fim, e apenas a título de menção, o OSA estabelece o [d] dever de plataformas prestarem informações pessoais, inclusive criptografadas, sobre usuários infanto-juvenis falecidos, caso as autoridades britânicas assim requererem ao OFCOM (Reino Unido, 2023, p. 105).

[68] *Child Sexual Exploitation and Abuse Content (CSEA)*.
[69] Determinação válida somente para os CAESIs relacionados a usuários no Reino Unido.
[70] As penas variam a depender da jurisdição - se escocesa, galesa ou inglesa.

3.4.3.2 Deveres de identificação de usuários.

Em continuidade aos projetos outrora ventilados no DEA 2017, o OSA propõe, dentre os deveres adicionais para serviços regulados de "usuário-a-usuário" e serviços regulados de busca, o [a] dever de Serviços de Categoria 1 oferecerem a todos seus usuários a opção de verificação de identidade para aceder ao portal. Para esses últimos, a lei também traz o dever de apresentar em seus termos de serviço como ocorrerá tal processo de verificação. O OSA dispensa que o procedimento de identificação se dê mediante uso de documentos formais, emitidos pelo Estado, bem como esclarece que o procedimento certificatório deverá ser exigido apenas para usuários que acessem o serviço desde o Reino Unido. A elaboração da estrutura de *design* que servirá a identificar usuários estará a critério das próprias plataformas, detentoras do poder direto sobre o código. De outro lado, o OFCOM estará incumbido de orientar plataformas e serviços na elaboração do mecanismo de verificação, já que esse não vem explanado amiúde no OSA (Reino Unido, 2023, p. 74).

3.4.3.3 Deveres de transparência.

Com a finalidade de aportar transparência à relação entre *bigtechs*, usuários e governo, o OSA pormenoriza uma série de exigências que visam tornar menos turvas decisões e procedimentos adotados por cada plataforma. Dentre essas medidas, duas ganham destaque. São elas: [a] o dever de não atuar contra usuários, com exceção das condições expressamente previstas em termos de serviços; e o [b] dever, para Serviços de Categoria 1, Categoria 2A e Categoria 2B, de apresentar relatórios anuais de transparência, conforme os critérios e o calendário especificados pelo OFCOM.

No tocante ao dever de não atuar contra usuários, à exceção do previsto em termos de serviço, trata-se de dever atribuído especialmente a serviços de Categoria 1. A fim de cumprir com a determinação, esses servidores terão de oferecer sistemas e procedimentos proporcionalmente desenhados para garantir que suas plataformas não (1) removam conteúdo regulado gerado por usuários do serviço; (2) não restrinjam o acesso de usuários a conteúdos regulados gerados por usuários do serviço; (3) e não suspendam ou expulsem usuários, a não ser que esses atuem em desacordo com condições pré-estipuladas nos termos de serviço. Como é de se supor, há uma série de escusas previstas para esse dever, o qual não pode ser invocado

como justificativa para que plataformas deixem de remover conteúdo ou deixem de punir usuários em decorrência de outros deveres de cuidado estipulados no OSA (Reino Unido, 2023, p. 84). O dever de atuar pró-usuários e zelar por sua liberdade, à exceção do previsto em lei, consiste em um dos principais mecanismos de equilíbrio entre liberdade de expressão e controle de conteúdo adotados pelo legislador britânico. Além disso, plataformas de qualquer tipo deverão trazer em seus termos de serviço disposições claras e acessíveis, informando usuários sobre seu direito de apresentar reclamação por violação de contrato se qualquer conteúdo gerado, carregado ou compartilhado for removido ou restringido, bem como caso usuários sofram algum tipo de punição por parte do portal. Para os serviços de Categoria 1, há a atribuição de dever especial para garantir que o *design* da plataforma faça cumprir estritamente as punições e o controle de conteúdo previstos em seus termos de serviço[71]. Há, também, a exigência de ampliação dos mecanismos de reclamação de usuários, a fim de que os mesmos possam reportar, com facilidade e eficiência, conteúdos que julguem ofensivos (Reino Unido, 2023, p. 80).

Com relação ao dever de prestar relatório anual de transparência, é importante frisar que se trata de atribuição destinada somente "a serviços de relevância", os quais serão notificados anualmente pela autoridade reguladora a fim de produzir referido demonstrativo. Esse relatório deverá ser entregue nos termos, na forma, e na data determinados pelo OFCOM[72]. Uma vez que o OSA apenas fixa linhas gerais, a autoridade reguladora estará responsável por esclarecer amiúde o que deve constar em cada documento[73].

---

[71] Um provedor deve operar seu serviço usando sistemas e processos proporcionais projetados para garantir que: (a) se os termos do serviço indicarem (em quaisquer palavras) que a presença de um tipo específico de conteúdo gerado pelo usuário é proibida no serviço, o provedor deverá efetivamente remover esse conteúdo; (b) se os termos de serviço estabelecerem que será restringido o acesso a um determinado tipo de conteúdo, o fornecedor restringirá o acesso dos utilizadores a esse conteúdo na forma prevista; (c) se os termos de serviço indicarem casos em que o fornecedor irá suspender ou proibir um usuário de utilizar o serviço, o fornecedor suspenderá ou proibirá o usuário nesses casos [tradução nossa] (Reino Unido, 2023, p. 79-80).

[72] Em resposta a uma notificação, o prestador do serviço relevante deve produzir relatório de transparência que deve: (a) conter informações do tipo especificado ou descrito na notificação, (b) estar no formato especificado na notificação, (c) ser submetido ao OFCOM até a data especificada no edital, e (d) ser publicado na forma e na data especificada no edital. O provedor do serviço deve garantir que as informações fornecidas no relatório de transparência sejam: (a) completas e (b) precisas em todos os aspectos relevantes [tradução nossa] (Reino Unido, 2023, p. 83-84).

[73] O OFCOM deve produzir orientações sobre: (a) como o OFCOM determinará quais informações os relatórios de transparência deverão conter, incluindo: (i) os princípios que eles aplicarão em relação a cada um dos fatores mencionados no parágrafo 37 do Anexo 8, e (ii) as medidas que tomarão para interagir com prestadores de serviços relevantes antes de exigirem informações num aviso ao abrigo da secção 78(1); (b) como as informações dos relatórios de transparência produzidos por prestadores de serviços relevantes serão usadas para produzir os relatórios de transparência do OFCOM (ver seção 160); e (c) qualquer outro assunto que o OFCOM

3.4.3.4 Dever de pagar taxas.

O OSA prevê a possibilidade de o OFCOM exigir o pagamento de taxas anuais por parte de serviços regulados, as quais serão revertidas para financiamento e manutenção das atividades de segurança *online* desempenhadas pela agência. O montante devido por cada serviço deverá ser calculado com base na renda mundial do provedor no período, levando em consideração outros fatores que o OFCOM julgue apropriados. Nessa senda, está prevista a necessidade de serviços de relevância prestarem contas ao OFCOM quanto a seu faturamento global anual. A seleção de quais plataformas deverão pagar tais taxas e quais estarão isentas – ademais de exceções arroladas na OSA – é incumbência da autoridade reguladora, a qual deverá estabelecer um marco mínimo de lucros obtidos por cada serviço a fim de separar as plataformas pagadoras de taxa daquelas dispensadas da obrigação. Os marcos e calendários para pagamento fixados pelo OFCOM deverão ser confirmados pela figura do Secretário de Estado, Ministro chefe da autoridade reguladora, quem, a qualquer tempo, poderá rever as determinações da agência. De outro lado, o Secretário de Estado deve ditar ao OFCOM guias-mestras e princípios a serem seguidos na fixação dos marcos para pagamento de taxas, os quais somente poderão ser alterados mediante consulta à autoridade reguladora (Reino Unido, 2023, p. 89-94). A inadimplência total ou parcial das taxas está sujeita a notificação e penalidades pecuniárias por parte do OFCOM, qual comentado abaixo.

É interessante observar que o dever de pagar taxas é uma das previsões de textura mais aberta do OSA. A nova lei se restringe a prever uma espécie de sistema de freios e contrapesos para fixação de quais empresas estarão obrigadas ao pagamento das taxas, através de atribuições complementares entre OFCOM e Secretário de Estado. O OSA também traz a

considere relevante para a produção e publicação de relatórios de transparência nos termos da seção 78 ou 160. (2) Antes de produzir a orientação (incluindo orientação revisada ou de substituição), o OFCOM deve consultar os seguintes atores, como considere apropriado: (a) prestadores de serviços de usuário-a-usuário e de serviços de busca, (b) pessoas que pareçam ao OFCOM representar esses provedores, (c) pessoas que pareçam ao OFCOM representar os interesses das crianças (em geral ou com referência particular a questões de segurança *online*), (d) pessoas que o OFCOM considere ter experiência em questões de igualdade e direitos humanos, em particular— (i) o direito à liberdade de expressão estabelecido no Artigo 10 da Convenção, e (ii) o direito ao respeito pela vida privada e familiar, pelo domicílio e pela correspondência de uma pessoa, estabelecido no Artigo 8 da Convenção, (e) o Comissário de Informação, (f) pessoas que pareçam ao OFCOM representar os interesses daqueles com características protegidas (na acepção da Parte 2 da Lei da Igualdade de 2010), e (g) pessoas que o OFCOM considera ter experiência na aplicação do direito penal e na proteção da segurança nacional que seja relevante para questões de segurança *online*, e OFCOM também deverá consultar outras pessoas que o OFCOM considere apropriadas [tradução nossa] (Reino Unido, 2023, p. 84-85).

exigência de publicação prévia dos princípios e dos marcos utilizados pelas autoridades para fixação do montante devido por cada serviço. No entanto, não há, no texto da lei, qualquer detalhamento quanto aos ritos e os processos que deverão ser seguidos, de forma que sua regulamentação caberá, mais uma vez, à legislação secundária produzida pela autoridade reguladora.

3.4.4 Poder de controle do OFCOM, poder de requerer informações e penalidades.

Como pode ser percebido, o OSA atribui enorme carga de poderes ao OFCOM (Kira e Schertel Mendes, 2023). Com a vigência da lei, o órgão passou a estar encarregado não apenas do controle administrativo da segurança *online* no Reino Unido, como também de elaborar manuais de procedimentos, fixar calendários de execução, fiscalizar atividades de provedores de serviços *online* no Reino Unido, denunciar casos de serviços infratores ao Judiciário, dentre outras incumbências. A título de exemplo, o OFCOM será responsável, com a coparticipação do Secretário de Estado e após a aprovação do Parlamento, pela elaboração de uma série de códigos de boas práticas e normatizações secundárias. Por meio dessas, o OFCOM deverá recomendar medidas para que serviços regulados cumpram com deveres de cuidado estabelecidos na OSA. Para cada dever de cuidado ou dever especial, e para cada tipo de serviço regulado, será necessário um código de boas práticas à parte (Reino Unido, 2023, p. 53-56). Além disso, a autoridade reguladora deverá orientar serviços de Categoria 1, 2A e 2B sobre como cumprir com deveres de cuidado, bem como orientar serviços em geral quanto à avaliação de conteúdos potencialmente nocivos para crianças. O OFCOM está também incumbido de orientar serviços de relevância durante a implementação de sistemas de verificação de identidade; de promover avaliações periódicas de impacto; e de manter registros de serviços de categorias especiais e de serviços emergentes de categorias especiais. Deverá, ainda, analisar e manter registro das avaliações de risco feitas periodicamente pelas plataformas. Em suma, é o OFCOM que irá orquestrar a implementação e manutenção de todas as disposições do OSA, tanto para o setor público quanto para o setor privado. Essas novas incumbências alteram o texto do CA 2003 para fins de delimitação dos poderes do OFCOM, os quais passam a ser expandidos após o OSA ganhar força de lei (Reino Unido, 2023, p. 94-96).

Ademais do exposto, para fins da análise que se seguirá no Capítulo 4, é importante ressaltar que o OFCOM passará a gozar de discricionariedade para, caso julgue pertinente, requerer informações a provedores de serviços[74] – sejam serviços de busca, sejam serviços de "usuário-a-usuário". Não obstante o OSA faça constar que o poder de requerer informações deva "ser exercido de modo proporcional", essa possibilidade vem rendendo acirrados debates na sociedade britânica, a tal ponto que se chegou a aventar rumores de que, caso aprovado o dispositivo, empresas como o WhatsApp poderiam encerrar suas atividades naquela jurisdição[75]. Em seção apartada, o OSA também atribui ao OFCOM o poder de requerer informações a servidores de qualquer espécie para fins de investigação em caso de falecimento de usuário criança, se a autoridade reguladora assim for requisitada por outras autoridades de outras esferas da administração[76]. A prestação de informações de qualquer tipo deve ser feita mediante notificação do OFCOM ao serviço requisitado, em que serão especificados os motivos, a forma e os meios pelos quais a autoridade reguladora requer o acesso a dados

[74] "O OFCOM pode, mediante notificação nos termos desta subseção, exigir que uma pessoa [servidor] forneça qualquer informação necessária para exercer ou decidir se deseja exercer qualquer uma de suas funções de segurança *online*. O poder conferido inclui o poder de exigir que uma pessoa — (a) obtenha ou gere informações; (b) forneça informações sobre o uso de um serviço por um indivíduo nomeado. O poder conferido também inclui o poder de exigir que uma pessoa dentro de qualquer um dos parágrafos (a) a (d) da subseção (5) tome medidas para que o OFCOM possa acessar remotamente o serviço fornecido pelo pessoa, ou aceder remotamente ao equipamento utilizado pelo serviço prestado pela pessoa, a fim de visualizar, nomeadamente: (a) informações que demonstrem em tempo real o funcionamento dos sistemas, processos ou funcionalidades, incluindo funcionalidades e algoritmos, utilizados pelo serviço; (b) informações geradas em tempo real pela realização de um teste" [tradução nossa] (Reino Unido, 2023, p. 103).

[75] A criptografia de ponta a ponta do *WhatApp*, aduz a empresa, é incompatível com a determinação de prestar informações da OSB. Mesmo que esta valha apenas para o território britânico, o caráter transnacional da comunicação via aplicativo, somado às adaptações no *design* que seriam acarretadas pela nova lei, poderiam comprometer a privacidade de todos os usuários da rede WhatsApp no mundo. Ver em https://www.theguardian.com/technology/2023/may/08/whatsapp-could-disappear-uk-over-privacy-concerns-ministers-told. Último acesso 03/09/2023.

[76] O OFCOM pode, mediante notificação nos termos desta subseção, exigir que uma pessoa relevante lhes forneça informações com a finalidade de: (a) responder a uma notificação dada por um legista sênior nos termos do parágrafo 1 (2) do Anexo 5 da Lei dos legistas e justiça de 2009 em conexão com uma investigação sobre a morte de uma criança, ou preparação de um relatório sob a seção 164 em conexão com tal investigação; (b) responder a um pedido de informação relacionado com a investigação de um procurador fiscal, ou um inquérito realizado ou a ser realizado em relação à morte de uma criança, ou preparar um relatório nos termos da secção 164 em conexão com tal investigação; (c) responder a uma notificação dada por um legista nos termos da seção 17A (2) do Coroners Act (Irlanda do Norte) 1959 (c. 15 (N.I.)) em conexão com— (i) uma investigação para determinar se um inquérito sobre a morte de uma criança for necessária, ou (ii) um inquérito em relação à morte de uma criança, ou preparar um relatório nos termos da secção 164 em conexão com tal investigação ou inquérito. (2) O poder conferido inclui o poder de exigir que uma pessoa relevante forneça ao OFCOM informações sobre o uso de um serviço regulamentado pela criança cuja morte está sob investigação, incluindo, em particular— (a) conteúdo encontrado pela criança por meio do serviço, (b) como o conteúdo foi encontrado pela criança (incluindo a função de algoritmos ou funcionalidades específicas), (c) como a criança interagiu com o conteúdo (por exemplo, visualizando, compartilhando ou armazenando, ampliando ou pausando) e (d) conteúdo gerado, carregado ou compartilhado pela criança" [tradução nossa] (Reino Unido, 2023, p. 105).

privados. Nesses casos, é possível que o OFCOM determine que pessoa física seja formalmente indicada como responsável pela entrega dos dados requisitados.

Prevê-se, ainda, que o OFCOM está intitulado a abrir investigações caso um provedor de serviço tenha falhado, ou esteja a falhar, com requerimentos arrolados no OSA[77]. Nessas ocasiões, o servidor estará explicitamente obrigado a colaborar com as investigações, sob pena de sanções. No curso das investigações, a autoridade reguladora gozará de poderes para requerer e conduzir entrevistas com pessoas de interesse, bem como deterá a discricionariedade para entrar, inspecionar e auditar empresas no território britânico (Reino Unido, 2023, p. 109-111). A ausência de resposta à notificação do OFCOM, assim como a prestação de respostas falsas, inverídicas, ou incompletas, implica crime sob a legislação britânica. Caso o indivíduo nomeado como responsável pela plataforma, mediante a notificação do OFCOM para prestar informações, preste informações falsas, inverídicas, ou com qualquer tipo de desídia, ele poderá ser igualmente responsabilizado na esfera criminal. A obstrução da atuação do OFCOM na busca por informações que julgue necessárias vem tipificada no OSA. Os delitos relacionados à requisição de informações têm pena prevista de multa e, a depender da gravidade da ação, conforme especificado na nova lei, de até dois anos de encarceramento (Reino Unido, 2023, p. 111-115).

A autoridade reguladora terá poder para *notificar e/ou emitir avisos* a provedores de serviços regulados, de forma fundamentada e caso entenda que esses não estão a cumprir satisfatoriamente com suas obrigações, intimando-os para que usem de tecnologia ou de medidas administrativas a fim de alcançar os padrões de segurança *online* exigidos pelo OSA. Se o primeiro aviso não surtir efeitos, a autoridade reguladora detém a discricionariedade de decidir sobre emitir um segundo aviso ou, caso entenda apropriado, emitir *nota provisória de contravenção.* É nessa última que as penalidades e sanções cabíveis serão informadas ao serviço em questão, e o prazo para resposta será fixado. Decorrido o prazo da nota provisória de contravenção, o OFCOM deverá decidir se as medidas adotadas pelo serviço notificado são

[77] Avaliações de risco de conteúdo ilegal; Conteúdo ilegal; Avaliações de risco das crianças; Segurança *online* das crianças; Empoderamento do usuário; Conteúdo de importância democrática; Conteúdo de editores de notícias; Conteúdo jornalístico; Relatórios de conteúdo; Procedimentos de reclamações; Liberdade de expressão e privacidade; Manutenção e revisão de registros; Avaliações de risco de conteúdo ilegal; Conteúdo ilegal; Avaliações de risco das crianças; Relatórios de conteúdo sobre segurança on-line infantil; Procedimentos de reclamações; Liberdade de expressão e privacidade; Manutenção e revisão de registros; Avaliações de acesso das crianças; Publicidade fraudulenta; Publicidade fraudulenta; Verificação de identidade do usuário; Relatar CAESI a NCA; Agir contra os usuários apenas de acordo com os termos de serviço; Termos de serviço; Informações sobre a utilização do serviço por crianças falecidas; Relatórios de transparência; Provedor de conteúdo pornográfico; Honorários: notificação do OFCOM; Avisos informativos; Assistência a pessoa qualificada; Cooperação com investigação [tradução nossa] (Reino Unido, 2023, p. 127-128).

suficientes para sanar o descumprimento do dever causador da advertência. Julgando, a autoridade reguladora, que as ações foram insuficientes, ela deve emitir *nota de confirmação de decisão*, na qual relatará ao serviço regulado seu parecer e opinião sobre o caso. Na nota de confirmação de decisão, o OFCOM também deverá informar a medida adotada para solução do caso, as quais, assim prevê o OSA, podem resultar em três soluções distintas. A primeira possibilidade é o OFCOM requerer que a empresa tome uma medida determinada (para esses casos, a OSA prevê a possibilidade de requerer ações específicas, requerer nova avaliação de risco, ou requerer o desenvolvimento de tecnologias proativas). A segunda possibilidade é impor à empresa pagamento de multa. Por fim, o OSA prevê que ambas as alternativas anteriores podem ser aplicadas concomitantemente. O descumprimento de medidas específicas solicitadas pelo OFCOM, sob nota de confirmação de decisão, consiste em ofensa e deverá ser tratado na esfera criminal (Reino Unido, 2023, p. 125-129).

A fixação do valor devido a título de multa estará a critério do OFCOM. Para isso, a autoridade reguladora deverá observar os esforços feitos pelo provedor penalizado e a extensão dos danos causados pelo descumprimento dos deveres de cuidado não honrados, de forma que a pena preencha critérios de proporcionalidade e de apropriação. Para cada serviço regulado, o valor máximo em penalidades a ser cobrado é de 18 milhões de libras esterlinas ou 10% do total da renda mundial qualificável no período de um ano[78], "o que for maior"[79]. Caso a pena pecuniária incida sobre grupo empresarial, os 10% do total da renda mundial qualificável deve recair sobre os rendimentos do conglomerado, e não apenas da plataforma causadora da penalidade (Reino Unido, 2023, p. 258).

Por fim, o OFCOM estará intitulado a ingressar com pedido de restrição de serviço de internet ante a cortes de justiça, caso o prestador não cumpra e insista em não cumprir com as requisições da autoridade reguladora. Dentre os motivos previstos que autorizam a agência a levar casos ao Judiciário, quatro ganham destaque. Primeiro, quando houver descumprimento contínuo de ações requeridas em nota de confirmação de decisão. Segundo, quando não for

[78] Critérios para determinar o que compõe a renda anual qualificável de provedores de serviços transnacionais deverão ser fixados após o assente real da OSB, a encargo do OFCOM, que observará padrões e princípios gerais dispostos no corpo da lei.

[79] "Quando uma penalidade for imposta a uma pessoa em relação a um serviço regulamentado prestado por essa pessoa, o valor máximo da penalidade é o maior entre: (a) £ 18 milhões, e (b) 10% da receita mundial qualificada da pessoa para o período contábil completo mais recente da pessoa (sujeito ao subparágrafo 5). (...) (5) Se a duração do período contabilístico com base no qual é calculado um montante de receita mundial elegível for inferior a um ano, o montante mencionado no subparágrafo (1)(b) deverá ser aumentado proporcionalmente. Se a duração desse período contabilístico for superior a um ano, esse montante será reduzido proporcionalmente" [tradução nossa] (Reino Unido, 2023, p. 278).

realizado o pagamento de multa decorrente de punição imposta pelo OFCOM. Terceiro, ante o descumprimento de nota de confirmação de decisão. E, quarto, em caso de alto risco de dano a indivíduos no Reino Unido, dispensada a necessidade de emissão de nota provisória de contravenção ou de confirmação de decisão[80].

Chama a atenção o quanto a última hipótese de judicialização é aberta e permissiva. Ela consiste em claro resguardo do legislador britânico para que, em caso de necessidade, o OFCOM possa agir com considerável margem de discricionariedade e rapidez, o que também serve a aumentar em enorme medida os poderes da autoridade reguladora. O OFCOM também passará a contar com a possibilidade de pleitear, ante o sistema judiciário, a restrição de acesso de determinado perfil de usuário à parte de um serviço. Em qualquer situação, o OFCOM estará obrigado a publicar o mérito e os critérios que motivaram a judicialização do caso. Há também previsão, no próprio OSA, de implementação de sistema de apelo e recurso das decisões do OFCOM para qualquer nível e para qualquer tipo de usuário (Reino Unido, 2023, p. 120).

Este capítulo cuidou de, com o maior fôlego que o tempo e o espaço disponíveis permitiam, esmiuçar alguns pontos de relevância do OSA. Foram aqui descritos os deveres de cuidado e os deveres especiais, as penalidades possíveis, e os novos poderes atribuídos ao OFCOM. Tratando-se de legislação bastante recente, a bibliografia que comenta o novo aparato regulatório britânico não é abundante. Dessa forma, o texto da lei nua acabou sendo a principal fonte aqui utilizada (ressalta-se que, na maior parte do tempo de escrita, o OSA sequer havia ganhado força de lei no Reino Unido). Ainda assim, apesar de seu caráter novel, o texto consolidado pelo Parlamento, bem como a conjuntura na qual aprovado, permitem uma série de reflexões. Com base nisso é que se inicia, a partir de agora, a análise crítica do OSA à luz da literatura apresentada no capítulo 2.

[80] [...] os riscos de danos para os indivíduos no Reino Unido são tais que é apropriado apresentar o pedido sem ter emitido nota provisória de contravenção, sem ter emitido nota de confirmação de decisão, ou (tendo dado uma confirmação de decisão impondo requisitos) sem esperar para verificar a conformidade com esses requisitos [tradução nossa] (Reino Unido, 2023, p. 139).

4. Deveres de cuidado, transparência e responsabilização de agentes intermediários: a retomada de espaço do Estado racional por intermédio do OSA.

Na esteira do desconcerto causado pelo crescimento das atividades sociais em rede, e envolto pela inexistência de alternativas para coordenar o fluxo de informação no ciberespaço, o governo britânico promulgou o OSA com o intuito de trazer, para sob o controle da Administração Pública, a ingerência firme, embora indireta, sobre a circulação de conteúdos em plataformas digitais. Não há dúvidas, o caso britânico consiste em não mais que um recorte de um amplo pano de fundo. Nesse, os Estados soberanos, ciosos do empoderamento das ora chamadas *bigtechs*, buscam se reinventar para conviver com tais empresas. No que tange a essas últimas, por se fazerem crescentemente necessárias nos cotidianos de cidadãos mundo afora, acabam por produzir uma série de desequilíbrios na ordem estatal dominante (até então dominante, ao menos). Essa dinâmica tem reflexos diretos na capacidade do governo de se pôr a par de atividades públicas por excelência, a exemplo da manifestação das ideias e a livre associação entre cidadãos, as quais têm se mostrado acompanháveis mais pelos detentores do código do que pelas autoridades. A profusão de abordagens propostas nas mais diversas jurisdições - para o que basta pensar em um simples comparativo entre o tratamento dispensado pelo governo norte-americano e o bloco europeu à responsabilização de provedores de serviços digitais por conteúdos circulantes em suas redes -, escancara que não há, até o momento, qualquer definição sobre como lidar com a situação.

A inexistência de regulações de sucesso, a nível global, não poderia ser menos inesperada. No atual processo de acomodação entre as ações de Estados e de *bigtechs*, os gargalos e conflitos de interesses são inúmeros, alguns já mencionados no curso deste trabalho, de sorte que harmonizar tamanha gama de fatores dificulta de sobremaneira a proposição de soluções regulatórias e/ou legislativas efetivamente profícuas. Conciliar valores de liberdade de expressão, princípios organizacionais de concorrência, a velocidade de desenvolvimento de novas tecnologias, interesses comerciais, meios de garantir a propriedade intelectual e direitos de autoria, bem como os obstáculos decorrentes da concentração de estruturas digitais nas mãos de empresas privadas, estão entre os principais desafios impostos pelo novo rearranjo de poder transnacional, no qual a ordem de Westfália já não goza do prestígio que outrora gozava (Leiser e Murray, 2017). O OSA, como se pode observar, é parte de grande investida do governo britânico, o qual vem atuando de forma orquestrada para recuperar a soberania administrativa em áreas como circulação de conteúdo, proteção de dados, regulação trabalhista, direito da

concorrência, defesa do consumidor e mercados digitais, investindo em diversas ferramentas regulatórias para atingir tais fins (qual mencionado no capítulo anterior, além do OSA, o Parlamento discute ações de regulação de concorrência, direito do consumidor, regulação das atividades profissionais de *influencers*[81], alfabetização digital, entre outros projetos). Original pela abrangência e pela presença forte da autoridade reguladora, o OSA responde ao cenário mediante incremento da presença do Estado nas atividades políticas das *bigtechs,* ao mesmo tempo que busca interferir o mínimo possível em assuntos pertinentes à organização financeira dos atores privados regulados.

No presente capítulo, em conclusão aos dados e aparatos teóricos apresentados até o momento, será empreendida análise das opções regulatórias do OSA à luz da literatura apresentada no capítulo 2, buscando compreender a nova lei como recurso lançado pelo Estado na tentativa de aumentar sua ingerência no ciberespaço. Por questões de recorte e espaço, bem como em vista do caráter novel do OSA, percorrer a totalidade das propriedades e potencialidades da lei seria tarefa irrealizável. Decidiu-se, assim, recair sobre três enfoques pontuais, os quais devem ser suficientes para dissertar com robustez sobre o embate político ora empreendido por *Westminster*. [1] De início, a análise dos deveres de cuidado impostos aos provedores de serviços de internet e o empoderamento do OFCOM como autoridade reguladora. Pontos por meio dos quais se busca explorar a opção do governo britânico de tratar o problema do controle do fluxo de conteúdo desde o viés administrativo – ao menos em sua maior extensão -, bem como a tentativa de compassar todas as variáveis em jogo desde uma abordagem sistêmica, de modo semelhante ao aventado por Evelyn Douek (2022). [2] O segundo ponto a ser explorado recai sobre as determinações do OSA voltadas a incrementar a transparência por parte de plataformas *online*, consolidadas sobretudo na exigência periódica de relatórios de avaliação de riscos e relatórios de transparência. Deve-se comentar, também neste ponto, sobre a possibilidade de o OFCOM requerer informações a provedores de serviços *online*, inclusive àqueles que oferecem aplicativos de mensageria com criptografia de ponta a ponta. A partir dos exemplos pinçados se procurará analisar o modo como o governo britânico encara os espaços de troca no ciberespaço como espaços de diálogo públicos, e busca, por intermédio do OSA, resgatar sua ingerência sobre estes ambientes. Para isso serão retomadas as reflexões de Lawrence Lessig (1996, 1997, 1999 e 2006), Paul Shiff Berman (2000) e Cass Sunstein (2017). [3] Por fim, será analisada a possibilidade de responsabilização de plataformas

[81] Ver em https://ukparliament.shorthandstories.com/influencer-culture-DCMS-report/index.html?utm_source=committees.parliament.uk&utm_medium=referrals&utm_campaign=influencer-culture-report&utm_content=organic. Último acesso 17/10/2023.

de serviços *online* estabelecida no OSA, em caso de descumprimento dos deveres de cuidado ou dos deveres especiais. Nesse ponto, o presente trabalho se esforçará por vincular a opção legislativa britânica à tentativa daquele Estado de retomar seu protagonismo no ciberespaço. O abandono parcial da autorregulação das plataformas de redes sociais e a escolha do legislador de exercer o poder coator estatal tradicional, por meio de penas pecuniárias e privativas de liberdade, são fortes indícios da reação do Estado tradicional racional ante o empoderamento das *bigtechs.* Para a análise de tal movimento esse trabalho deve se pautar, sobretudo, no trabalho de Vili Lehdonvirta (2022).

4.1 Os *Duties of Care* e o OSA como projeto regulatório administrativo.

Na esteira do que vinha sendo discutido desde os preâmbulos do *Online Harms White Paper*, o OSA formalizou a possibilidade de plataformas serem responsabilizadas por conteúdos veiculados e acessados por meio de suas redes. A responsabilização proposta pelo OSA, no entanto, põe de lado a análise individual e casuística, e se dá com base na definição do conceito de deveres de cuidado (os ora comentados *Duties of Care*). Em outros termos, não é necessária a apreciação de casos específicos para se decidir pela responsabilidade de um provedor, bastando para isso que esse descumpra deveres gerais impostos pelo OSA. O foco da proposta está em incentivar mudanças estruturais nas plataformas de redes sociais, encaminhando-as a promover reformas em seu *design* e política de funcionamento mediante análise e avaliação periódicas de riscos. O projeto difere de outros tipos de abordagem, especialmente daqueles voltados a especificar tipos pontuais de conteúdo a serem tidos como problemáticos - este último, conhecido como o modelo tradicional de responsabilização de intermediários, via de regra se reduz à mera remoção de publicações de teor danoso (Woods, 2019). Nessa toada, o OSA optou por delimitar categorias gerais de conteúdos a serem controlados, elencando diferentes matérias que deverão ser observadas pelos provedores de serviços (conteúdos ilegais, conteúdos de relevância democrática, conteúdos potencialmente danosos para usuários crianças, dentre outras espécies descritas no capítulo 3, são exemplos das matérias reguladas). A avaliação do que recairá, ou não, em cada categoria, continuará a critério das plataformas, e a avaliação da efetividade das políticas adotadas pelas plataformas estará a critério da autoridade reguladora. É interessante observar que o OSA põe de lado a simples conceitualização dualista de conteúdo legal e conteúdo ilegal, elencando uma série de espécies de conteúdos-alvo a serem observados pelas plataformas. A promoção de uma

estrutura saudável e vigilante *ex ante* para a circulação de conteúdos, assim é esperado, deverá tornar a remoção de publicações menos frequente, e um dos últimos recursos a serem dispendidos pelas plataformas.

Ao estudar os deveres de cuidado do OSA desde a perspectiva do direito continental, qual ora fazemos neste trabalho, é compreensível que seja feita certa confusão entre os deveres de cuidado e o que entendemos, no direito brasileiro, por responsabilidade civil. De fato, são institutos que guardam considerável semelhança entre si, mas que não por isso devem ser tomados por idênticos. Originalmente, o *landmark case* que inaugurou os deveres de cuidado no direito britânico foi o caso *Donoghue v Stevenson*, de 1932. Nesse, as cortes entenderam que a empresa *Stevenson*, fabricante de bebidas, foi responsável pela intoxicação da senhora *Donoghue*, quem havia consumido cerveja contaminada por restos de moluscos, bebida esta produzida pela empresa condenada (Hutchinson, 2014). O caso deu ensejo à possibilidade de responsabilização de empresas com relação a consumidores dispensando a necessidade de relação contratual explícita entre estes, de modo semelhante ao que temos hoje com o instituto da responsabilidade civil direta em nosso Código de Defesa do Consumidor. Os deveres de cuidado preceituados pelo OSA, no entanto, já não são os mesmos do caso originário, e consistem em ferramenta bastante mais específica, juridicamente evoluída desde a tese original (Woods, 2019). Inspirados no *Health and Safety at Work Act 1974* (HSWA – no inglês, Lei de Saúde e Segurança no Trabalho), os deveres de cuidado do OSA se propõem a encarar as plataformas de redes sociais como extensão do espaço público, visando a regular e garantir a segurança nesses âmbitos do ciberespaço *como se público fosse,* e investindo em abordagem sistêmica para tanto (Woods et al, 2021). Em explicação muito enxuta, a HSWA impõe o dever legal de cuidado no âmbito específico das relações de trabalho, determinando que todo empregador deverá garantir, na medida do razoavelmente praticável, a saúde, a segurança e o bem-estar no trabalho de todos os seus empregados" (HSWA, Seção 2 – 1, 1974), elencando situações específicas a serem observadas, e impondo o dever de avaliação de riscos e de diligência para cumprimento dessas obrigações. Nesse âmbito, é de se salientar que a responsabilidade atribuída aos empregadores é coletiva, já que casos isolados de danos sofridos por negligência continuarão a ser analisados individualmente. Em que pese a HSWA 1974 trate de matéria totalmente alheia ao abordado pelo OSA, foi a proposta de cuidado sistêmico da lei, com a especificação das matérias amplas a serem zeladas pelos agentes regulados, que inspirou os deveres hoje atribuídos às plataformas. Esse tema foi fartamente discutido em comissão

parlamentar[82] e posteriormente aventado no relatório do *Carnegie Hall UK* (2019), o qual serviu como base teórica para os debates legislativos que optaram pela adoção dos deveres de cuidado (Woods et al, 2021) (Kira e Schertel Mendes, 2023).

A exigência de prestação periódica de avaliação de riscos ao OFCOM, com critérios específicos a depender do tipo de conteúdo e público de cada plataforma, foram os meios definidos pelo legislador para delimitar e explicitar aos provedores os recortes do ciberespaço nos quais os deveres de cuidados deverão ser observados, e em quais pontos as plataformas poderão ser cobradas pela autoridade reguladora. Em vista disso, é possível enxergar a imposição do dever de prestar avaliações de risco periódicas como delimitação espacial/conteudista do fluxo de informação regulado no mundo virtual. Ao mesmo tempo, a imposição dos deveres de cuidado pode ser interpretada como elemento vinculativo do compromisso dos atores regulados para com o OSA e, por conseguinte, com o Estado britânico. Mediante a definição de espaços a serem zelados e comportamentos a serem controlados – ou censurados -, o OSA fixa de antemão os pontos onde a autorregulação das *bigtechs*, até agora o *modus operandi* predominante no Reino Unido, deverá ser substituída total ou parcialmente pela autoridade reguladora. Esse movimento traz para sob a égide estatal a ingerência indireta do fluxo de alguns conteúdos no ciberespaço, aqui entendido como espaço público de trocas. Isso faz com que se invoque, mais uma vez, a metáfora que projeta no ciberespaço a cidade moderna como espaço público, bem como a importância dos intercâmbios que aí ocorrem para a ordem democrática. Através dessa sistemática o OSA revela o intuito do legislador de tornar o cuidado sistemático e *ex ante* a regra para o controle de fluxo de conteúdo nas redes, adotando estratégias regulatórias e administrativistas para tanto. Abandona-se, aqui, a perspectiva de inspiração jurisdicional para moderação de conteúdo e se parte para abordagem sistêmica do controle do fluxo de dados nas redes.

A regulação de base sistêmica deve ser entendida, concomitantemente, de dois modos. Primeiro, o foco da regulamentação está no sistema de *software* em si (ou, mais amplamente, no serviço, incluindo o modelo de negócios), e não no conteúdo hospedado no serviço. Segundo, os prestadores de tais serviços devem ter um sistema implementado para avaliar o risco do serviço e suas características individuais, tomando as medidas adequadas para resolver as preocupações que surjam (Woods et al, 2021). O deslocamento dos cuidados com ações e danos individuais, ora praticado de forma *ex post* pelas cortes britânicas, devem

[82] Ver Comitê de evidências orais em https://committees.parliament.uk/event/15985/formal-meeting-oral-evidence-session/. Último acesso 18/10/2023.

ser reposicionados em macro escala, forçando empresas a investirem em *design* e modelos capazes de abalizar e avaliar sistematicamente conteúdos circulantes no ciberespaço sob seu domínio. Essa estrutura se volta a prevenir que conteúdos indesejados circulem, e busca controlar, de modo sistemático, o surgimento de novos materiais de potencial danoso. A negligência dos operadores de serviços *online,* a qual em matéria consumerista tenderia a ser trabalhada caso a caso, com o OSA passa a ser tratada a nível estrutural.

A adoção do modelo de abordagem sistêmica dialoga a todo tempo com a extensão com que se passará a encarar a liberdade de expressão e suas balizas constitucionais no Reino Unido. À parte da nova possibilidade de responsabilização de intermediários por materiais veiculados por meio de suas redes, a transposição do controle de conteúdo para o modelo preventivo deve, em boa medida, esvaziar a apreciação de casos afins pelas cortes britânicas, retirando o protagonismo dos órgãos judiciários para tratar do tema (Neudert, 2023). Tal afastamento encontra respaldo em grande parte da literatura que discute a liberdade de expressão na era digital, dentre autores como Lawrence Lessig e Cass Sunstein, obras trabalhadas no capítulo teórico desta dissertação. Em cima disso, qual preceituado por Evelyn Douek ao discorrer sobre as adaptações regulatórias necessárias à era da informação, o modelo atual de controle de conteúdo firma pé em assunções equivocadas, os quais equivocadamente têm na liberdade de expressão bastião da democracia. Para a autora, a "moderação automatizada tornou o controle dos discursos mais possível, tratável e regulável do que nunca", de forma que "novas tecnologias exigem um novo pensamento sobre o que significa fazer valer e proteger direitos" de expressão (Douek, 2023, p. 34-35). Nessa senda, ao preceituar valores para controle de conteúdo por intermédio dos deveres de cuidado, o OSA, se bem sucedido em sua implementação, tende a criar maior equilíbrio entre o zelo à liberdade de expressão e outras preocupações do governo britânico (a exemplo do acesso de crianças a conteúdos impróprios ou a circulação de materiais que atentem contra a democracia no Reino Unido). É certo que a lei reserva seção especial para determinar às plataformas deveres de cuidado com a liberdade de expressão dos usuários. Ainda assim, trata-se de seção de teor pouco específico, com clara ressalva de que os valores ali resguardados não poderiam servir de justificativa para descumprimento dos demais deveres de cuidado previstos em lei.

A perda de protagonismo do princípio da liberdade de expressão para tratar do fluxo de conteúdo nas redes guarda relação próxima com a visão que enxerga no ciberespaço extensão do espaço público do mundo real. Ao escrever sobre as propostas regulatórias aportadas pelo CA 2003 – ao tempo em que pouco se poderia antever o crescimento em

relevância das redes sociais –, Feintuck e Varney (2006) já debatiam a necessidade de reconhecer mídias de comunicação como ferramentas cruciais para a saúde da democracia de uma nação. Em vista da era das mídias digitais que se inaugurava, os autores, já àquele tempo, alertavam sobre a importância de manter sob influência do Poder Público pontos sensíveis da estrutura comunicacional do Reino Unido. Para eles, ao passo que se reconhece que tecnologias de comunicação e mídias digitais consistem em elementos centrais à vida em sociedade, é fundamental reconhecer, também, que alguns pontos de sua infraestrutura são partes elementares dos sistemas de comunicação e, por consequência, da democracia. O caráter essencial de alguns desses pontos justifica, segundo os autores, que esses sejam considerados patrimônio público, antes que a iniciativa privada os tome para si (Feintuck e Varney; 2006). Ao comentar sobre a tendência de concentração dos veículos de comunicação em oligopólios, Feintuck e Varney defendem que

> o fato de falhas na regulação poderem resultar na privatização da democracia, através da privatização corporativa dos fluxos de informação, sugere que a regulação dos meios de comunicação social é ainda mais importante do que a regulação de outros serviços públicos e mercadorias [tradução nossa]. (Feintuck, Varney, 2006, p. 251).

É com base nesse pensamento que os autores sugerem que, a fim de resguardar infraestruturas elementares para manutenção da saúde da democracia britânica, valores e prioridades têm de ser traçados pela administração. Essa última, em nome do interesse público, a sua vez deve atuar a fim de manter a ingerência estatal sobre partes fulcrais das mídias de comunicação atuantes em seu território (Feintuck e Varney; 2006). Nesse cenário, a liberdade de expressão, em que pese sua importância principiológica, não deve gozar de primazia absoluta. Isso porque negar toda e qualquer regulação em nome da livre manifestação das ideias é discurso que pode ser facilmente manipulado por agentes privados em posição de poder sobre estruturas comunicacionais, em movimento similar ao outrora denunciado por Cass Sunstein (2017). Desse modo, a opção pelos deveres de cuidado e por tratar o espaço de troca das plataformas como espaço público, priorizando o interesse coletivo, é não somente o embasamento do OSA para entregar à autoridade reguladora parte do cuidado com o direito a livre manifestação nas redes, como também consiste em posicionamento político que opta por reduzir o arbítrio da iniciativa privada nessa seara, intencionando resguardar, justamente, o direito à informação e à livre manifestação das ideias de seus cidadãos.

Ao analisar os liames entre democracia e equidade política[83], Jacob Rowbottom alerta para a relação direta entre a privatização de determinados espaços públicos e a capacidade do cidadão ordinário para tomar parte na vida política de seu país. O autor reconhece o peso que o dinheiro tem para fazer ouvir as opiniões daqueles que detêm poder financeiro, mas refuta a ideia de que a riqueza, isoladamente, é capaz de moldar as escolhas públicas (Rowbottom, 2010). Para Rowbottom, é a garantia de acesso equânime aos meios de comunicação que pesa mais para fazer com que os debates políticos sejam efetivamente democráticos e a liberdade de expressão se aproxime do ponto ótimo. Com base nisso, o autor julga mais eficaz "procurar desenvolver as capacidades das pessoas para participarem na política, em vez de equalizar os recursos financeiros" (Rowbottom, 2010, p. 12). Em sua obra, ele afirma que equidade política tem relação próxima com a liberdade de expressão, e que é por meio da possibilidade de comunicação que os cidadãos, no Estado democrático, têm como manifestar e propor o que acharem acertado. Pondo-se de acordo com Sunstein (2017), ele não confunde regulação com restrição ao direito a livre manifestação das ideias, e demonstra preocupação com o fato de que "a liberdade de expressão possa ser usada como uma barreira que impede a prossecução do objetivo da igualdade política e uma garantia de que aqueles com maior riqueza possam falar mais" (Rowbottom, 2010, p. 34). O autor defende a importância do espaço público de comunicação para a democracia e para a equidade política, e se posiciona contra o entendimento do mercado aberto das ideias. Pelo contrário, para ele é a presença do Estado regulador que tende a dar azo a um mercado efetivamente competitivo de ideias e trocas, firmando pé na elementariedade da existência de estruturas de comunicação públicas e acessíveis para fins de equidade política (Rowbottom, 2010, p. 226). Também em vista da proposta do autor, é possível interpretar o OSA como tentativa de equalização da capacidade comunicativa do usuário de internet no Reino Unido. Isso pois a imposição de reestruturação algorítmica e de *design*, através dos deveres de cuidado, visa a mitigar os efeitos do direcionamento de conteúdo por afinidade (para além de evitar o acesso a fóruns de conteúdos ilegais ou nocivos). Isso em tese tende a aumentar a circulação de matérias de espectros ideológicos diversos para todos os perfis. Tal movimento, caso seja de fato efetivado, de modo algum serve a restringir o direito a livre manifestação das ideias, senão o contrário, e tem o potencial de privilegiar a ação do governo britânico de recuperar sua ingerência sobre estruturas comunicacionais virtuais.

[83] Por equidade política leia-se a capacidade dos cidadãos de se engajar e contribuir com atividades políticas no Estado democrático.

A escolha legislativa pelos deveres de cuidado também evidencia que, em que pese o direito constitucional siga pautando a base do movimento regulatório britânico, os mecanismos propostos pelo OSA que são colocados em prática estão sob a égide do direito administrativo. Ao comentar sobre as possibilidades de recuperação de estruturas cruciais de comunicação pelo Poder Público, Feintuck e Varney assim pontuam:

> Embora se pudesse esperar que os valores constitucionais fornecessem tais fundamentos, as evidências comparativas são um tanto inconclusivas. Em alguns países, como a Alemanha e a Itália, as constituições e as declarações dos respectivos tribunais constitucionais parecem, por vezes, prometer muito, mas na prática não conseguiram travar a concentração total de propriedade nos meios de comunicação comerciais. Nos EUA, há mesmo um sentido em que a constituição parece ter servido como um obstáculo à intervenção relativa à obtenção da diversidade na produção, a garantia constitucional da liberdade de expressão, destinada a proteger o indivíduo contra o potencial de poder do estado, sendo solicitado por gigantes da mídia corporativa para resistir à regulamentação de suas atividades (Feintuck 2004: 141–52). Isto é o que McChesney (1999) descreveu poderosamente como a "Primeira Emenda Comercializada". Na Grã-Bretanha, os valores constitucionais relevantes permanecem irremediavelmente mal definidos. No entanto, embora nem as disposições existentes nem o programa de reforma constitucional que o governo trabalhista empreendeu forneçam respostas diretas a este problema, ainda pode se argumentar que tanto os valores constitucionais como os conceitos jurídicos fornecem apenas assistência limitada [tradução nossa] (Feintuck e Varney, 2006, p. 272).

A corroborar a opção regulatória do OSA, Evelyn Douek alertou para o fato de que a mera transposição do sistema de controle de conteúdo *offline* para o ciberespaço não é suficiente para atender a vazão do fluxo de informação *online*, incluído aí o controle de conteúdo nas redes. Segundo a autora, moderação de conteúdo "não é a simples soma de muitas decisões binárias de manter certo conteúdo no ar ou removê-lo. É um vasto sistema de administração que inclui uma gama enorme de decisões e tomadores de decisões" (Douek, 2022, p. 4). É em vista disso que o controle posterior e casuístico não é suficiente para a complexidade da tarefa, a qual demanda a adoção das medidas sistêmicas ora em comento. O OSA, desse modo, se aproxima da proposta de Douek esmiuçada no capítulo 2, e a opção pelos deveres de cuidado é elemento essencial do modelo regulatório sistêmico aportado pela nova lei. Nesse ponto, é interessante observar como o OSA não toma para a administração britânica a tarefa direta da moderação de conteúdo *online*, o que denota o reconhecimento, por parte do regulador, de suas limitações práticas e estruturais (Lessig, 1996) (Douek, 2022) - "plataformas podem e irão se engajar na moderação de conteúdo muito mais do que a lei pode prever", afinal (Douek, 2022, p. 6). Em vista disso, é inteligente que o regulador britânico não assuma o dever de fiscalizar diretamente os conteúdos circulantes, os quais seguirão sendo analisados de forma direta pelas plataformas, e, diversamente do que ocorre com o controle dos discursos pelas vias judiciais, foque na regulação procedimental em macro escala.

Ao impor deveres de cuidado, deveres de transparência e a possibilidade de responsabilização de agentes intermediários por danos decorrentes de conteúdos veiculados por intermédio de suas redes, o OSA abre as portas a sistema regulatório complexo e compreensivo. Nesse, o Estado se põe a par da atuação das plataformas por meio da possibilidade de exigir informações e avaliações periódicas de risco, ao mesmo tempo em que condiciona comportamentos, imprime valores e direciona condutas empresariais mediante a determinação de controlar conteúdos de natureza específica, arrolados no corpo da lei. Trata-se de sistema muitíssimo abrangente e aberto, "de abordagem sistêmica" como dissera Douek, no qual o Poder Público se esforça por tomar parte no processo de moderação de conteúdo no ciberespaço, e no qual, como consequência do afastamento da atuação das cortes na valoração dos discursos, o direito administrativo ganha protagonismo ímpar. Princípios e práticas administrativas são postos em prática, e, mediante a exigência de determinados dados e comportamentos dos provedores de internet, entregam ao governo visão abrangente do quadro geral da moderação de conteúdo no Reino Unido, colocando-o em posição de efetivo controlador desse sistema. Na mesma toada, os deveres atribuídos pelo OSA às plataformas contribuem para que elas atuem de modo mais próximo à administração pública, engajando-as a valores que o legislador fez incluir no projeto regulatório. Isso deve facilitar a interação entre público e privado, qual há de ser explorado no subcapítulo seguinte.

Por sua natureza e detalhamento, o OSA tende a permitir que a moderação de conteúdo operada pelas plataformas se descole de preceitos inspirados na atuação das cortes, os mesmos que vêm pautando a resolução casuística e autorregulatória ora praticada pelos provedores até aqui. Nesse ponto, é interessante retomar as críticas de Douek com relação ao modo como plataformas costumam definir critérios para moderação de conteúdo *online*, a fim de enxergar com maior clareza as inovações do OSA. Para a autora, ante a ausência de delimitações legais e regulatórias claras quanto aos procedimentos desejáveis para moderação de conteúdo, plataformas em geral acabam por desempenhar papel "auto legislativo". Elas criam regras próprias para remoção e supressão de determinados conteúdos, e se valem de casos isolados para elaborar tais normas – sem qualquer preocupação com uma visão ampla e concatenada dos conteúdos circulantes. Nesse sistema, os inúmeros casos de remoção equivocada são, em tese, corrigidos a partir a disponibilização aos usuários de ampla gama de ferramentas de apelo, o que consiste em clara reprodução do modelo judiciário padrão. Nos termos da autora, ao comentar a lógica que sacramenta o modelo *ex post* ora em funcionamento:

> [...] esta concepção de 'moderação de conteúdo' é a de uma burocracia hierárquica privatizada que aplica regras de estilo legislativo elaboradas pelos decisores políticos da plataforma a casos individuais e ouve recursos dessas decisões [tradução nossa] (Douek, 2022, p. 9-10).

A partir da vigência do OSA, no entanto, esse quadro deve mudar. A proposta de imposição de deveres de cuidado *ex ante* tende a incentivar plataformas a desenvolver seu *design* e estrutura de modo a prevenir a propagação dos tipos de conteúdos danosos arrolados pelo OSA. A ação é profilática e uniformizadora, pois, muito embora os servidores seguirão gozando de autonomia para decidir *como* cumprir com a lei, todos eles estarão legalmente comprometidos com os resultados por ela exigidos. Em outros termos, plataformas tenderão a se alinhar de modo sistêmico às determinações trazidas pela nova regulação, valendo-se de soluções tecnológicas e de *design* para isso. No que diz com a autoridade reguladora, essa não deverá analisar os processos empregados pelos atores regulados, mas tão somente seus resultados. A complexificar a máxima de Lessig – *code is law* – (2006), o OSA, se bem sucedido, se voltará a influenciar a estrutura do ciberespaço por meio da imposição, no mundo real, de deveres legais, os quais por sua vez influenciarão diretamente a arquitetura das plataformas.

A atribuição de poderes à autoridade reguladora é também elemento chave para compreender a estratégia do OSA e sua perspectiva administrativa-sistêmica. De início, calha repisar que o fortalecimento do OFCOM como agência responsável pela implementação e fiscalização do OSA reflete a tentativa de afastar a orquestração regulatória do agente privado, ao mesmo tempo em que se reconhece que o governo não goza dos meios estruturais para proceder, ele mesmo, à moderação de conteúdo *online*. É mediante o empoderamento da autoridade reguladora que a administração pública, valendo-se de expertise e de tradição burocrática, busca organizar e fazer valer as determinações previstas em lei. O fato de os poderes do OFCOM e sua estrutura terem sido ampliados justamente para consecução do OSA, bem como a previsão de cobrança de taxas das plataformas para financiamento das atividades da agência regulatória, denota o vigor com que o Parlamento busca trazer a ingerência sobre o processo de controle de conteúdo executado pelos atores privados para o Poder Público. Além disso, a fixação de uma agência reguladora independente para executar tais tarefas é também signo da transposição do cuidado com o fluxo de conteúdo *online* para a esfera administrativa. Isso é revelado ao se ter em vista, especialmente, que eventuais descumprimentos do OSA somente serão levados a juízo após o exaurimento dos processos administrativos desenvolvidos e executados pelo próprio OFCOM, e isso se a autoridade reguladora entender que se trata de caso de judicialização.

É certo que não há como saber, de momento, se a atribuição da enorme quantidade de papéis ao OFCOM permitirá o sucesso do OSA. Alguns especialistas, a exemplo de Laura Schertel Mendes e Beatriz Kira, bem como Lisa Maria Neudert, entendem que a pendência de elaboração de legislações secundárias e a vagueza do texto da nova lei abrem margem a uma considerável chance de insucesso da mesma (Kira e Schertel Mendes, 2023) (Neudert, 2023). Ainda assim, a estratégia de transposição do tratamento do controle de conteúdo para a esfera administrativa consiste em aposta de relevância, cujo êxito tem o potencial de mudar globalmente as relações entre governos e *bigtechs*. Novamente nos inspirando nas ideias de Douek, atribuir tal tarefa à autoridade reguladora auxilia na separação entre as atividades políticas de moderação de conteúdo e atividades propriamente empresariais das plataformas (Douek, 2022), as quais deverão, com o OSA e com a atuação do OFCOM, passar a dedicar parte de sua energia exclusivamente para pensar seu *design* e o tipo de conteúdo que esse privilegia e/ou desfavorece. Ao defender a utilidade da separação de funções adminsitrativas das financeiras, dentro das empresas provedoras de serviços de internet, a autora diz:

> Uma preocupação generalizada sobre a moderação de conteúdos — talvez a mais universal e persistente — é que as plataformas perseguem os seus próprios interesses políticos e financeiros, apesar dos seus compromissos públicos de aplicar as suas regras de forma neutra. Em vez de depender de uma revisão individualista *ad hoc ex post* para revelar e corrigir todos esses preconceitos na aplicação, os reguladores deveriam impor separações estruturais que visem "eliminar os incentivos que tornariam a conduta [tendenciosa] possível ou provável em primeiro lugar" [tradução nossa] (Douek, 2023, p. 61).

Posto isso, é confortável afirmar que o legislador não tenta ir contra o poderio das plataformas, bem como não ignora seus objetivos mercadológicos e de lucro. Pelo contrário, ao levar em conta tais características dos atores regulados, o Parlamento se esforça por fixar deveres de cuidado e deveres especiais mediante determinações amplas, visando aos resultados e não aos processos específicos, em clara tentativa de conferir longevidade ao OSA. A opção legislativa também serve ao propósito de dar legitimidade às estratégias procedimentais e de *design* das plataformas. Sob o atual modelo de controle de conteúdo *ex post* e autorregulação, e em vista da discricionariedade com que as plataformas escolhem quais conteúdos remover e quais manter no ar, muito se comenta sobre falta de legitimidade desses agentes para decidir sobre os discursos de seus usuários. A partir da constância dos deveres de cuidado, essa suposta ilegitimidade tende a ser mitigada, muito embora não extinta de todo. Sobre a dificuldade de aliar legitimidade e interesses financeiros das *bigtechs*, Douek assim comenta:

> Um tema subjacente e uma motivação deste artigo é que os limites da regulação governamental direta do discurso *online* são instransponíveis, tornando necessário encontrar uma abordagem que aproveite e legitime a autorregulação das plataformas.

> A supervisão governamental das plataformas deve ter como objetivo maximizar os recursos, conhecimentos e dinamismo do setor privado na descoberta de métodos inovadores e eficazes para enfrentar os desafios da moderação de conteúdos, exigindo ao mesmo tempo que as plataformas expliquem, justifiquem e verifiquem esses métodos. Ao permitir que as plataformas façam experiências, a supervisão do governo evitaria fixar o *status quo* nas principais plataformas [tradução nossa] (Douek, 2022, p. 78).

Por fim, cabe pontuar que, muito embora o OSA consista em mudança paradigmática para fins de regulação de controle de conteúdo *online*, ele não abandona por completo a estratégia regulatória anterior, e sim busca o equilíbrio entre o modelo sistêmico-administrativo e algumas ferramentas de controle *ex ante*. O "triplo escudo" (*triple shield*) de proteção a usuários adultos, o qual foca na prevenção de circulação de conteúdos danosos para maiores de idade, é o maior exemplo disso. Qual mencionado, o triplo escudo consiste na combinação do dever de remoção de conteúdos ilegais com o dever de provedores de Categoria 1 removerem conteúdos expressamente proibidos por seus termos e serviços, e mais a disponibilização, ao usuário adulto, de ampla gama de ferramentas de filtragem e denúncia de conteúdos. Sobre essa última, é interessante observar que consiste em ampliação e aperfeiçoamento de mecanismos já existentes hoje em dia, os mesmos que possibilitam o controle *ex post* de discursos. Esses, combinados com deveres de manter estrutura de *design* própria para prevenção à circulação de conteúdos danosos ou proibidos, visam a compor um arranjo complexo para verificação de conteúdos, aumentando as chances de eficácia do sistema proposto pelo OSA. A combinação de ambos modelos é, também, a proposta de Douek:

> Ao sublinhar a importância da responsabilização ex ante, o argumento deste artigo não é que todas as revisões ex post sejam ineficazes. Pelo contrário: a revisão de erros pode ser uma forma importante de diagnosticar falhas sistêmicas. Embora a revisão ex post de casos individuais que a maioria dos modelos regulamentares actuais favorece não consiga trazer uma reforma sistémica significativa ou responsabilização, a revisão de reivindicações agregadas poderia fazer exactamente isso [tradução nossa] (Douek, 2023, p. 77).

Postas as reflexões acerca da relação entre os deveres de cuidado e a abordagem administrativa do OSA, passa-se a analisar os deveres de transparência e sua relação com a dualidade conceitual entre o que é público e o que é privado no ciberespaço.

4.2 Deveres de transparência e o oxímoro 'público versus privado'.

Em recente entrevista, o especialista em tecnologia e sociedade Evgeny Morozov, ao comentar o estado da arte da regulação da internet no Brasil, alertou para a necessidade de focar não apenas na regulação sobre a atuação de grandes empresas, como Facebook ou TikTok,

como também investir de forma robusta em infraestrutura digital (Mello, 2023). Para o autor, a orquestração regulatória das atividades comerciais das *bigtechs*, muito embora seja de importância ímpar, deve vir acompanhada da consciência de que a exploração das estruturas midiáticas, as mesmas que permitem o uso e propagação das redes, é fato social de interesse público.

> A regulamentação é importante, mas não podemos apenas discutir o que fazer com WhatsApp ou Facebook. Precisamos pensar o que fazer a respeito dessas enormes infraestruturas digitais que empresas privadas estão vendendo de volta às instituições públicas e aos cidadãos. (...) assumir que a infraestrutura digital é um bem público, não é um custo, é um bem facilitador (Morozov, in: Mello, 2023.).

A proposição de retomada das estruturas comunicacionais pelo Poder Público, ora feita por Morozov, é parte de debate que ecoa para além das fronteiras do processo de digitalização da vida em sociedade, a exemplo do equilíbrio entre desenvolvimentismo e dependência externa no movimento industrializador do Brasil nos anos 60, ou da abertura para investimento estrangeiro em tecnologia 5G nos anos recentes[84]. No tocante ao atual movimento em prol da regulação das plataformas *online*, a discussão segue gozando de relevância, e guarda relação próxima com a confusão comum entre quem vê o ciberespaço e as trocas que ali ocorrem como questões de direito privado, e quem as encara como matéria pertinente ao direito público.

Com respeito ao OSA e à moderação de conteúdo, os deveres de transparência trazidos pela nova lei consistem em exemplos bastante interessantes para refletir sobre a relação entre público e privado no espaço regulado da internet, motivo pelo qual esse subcapítulo se volta a analisá-los. É importante lembrar, aqui, que os deveres de transparência consistem em seção apartada dos deveres de cuidado e foram assim elencados no capítulo 3: [1] dever de provedores de serviços de internet não atuarem contra usuários; [2] dever especial, para provedores de Categoria 1, 2A e 2B, de prestar relatório anual de transparência; [3] dever de entregar informações para usuários que tiveram suas postagens de algum modo alteradas pelas plataformas, nos casos especificados em lei, como meio de controle *ex post* de moderação de conteúdo; [4] e o dever de prestar informações mediante requerimento do OFCOM, este último

[84] Os preâmbulos do leilão público que concedeu o direito de exploração de faixas da tecnologia 5G no país, na ocasião arrematado por 5 empresas privadas, foi marcado por debates que questionavam o quanto a entrega destes mercados a agentes privados ia contra o interesse público, a vez que o Estado se abstinha de investir ele mesmo em tal tecnologia.

visando ao controle, por parte da autoridade reguladora, do efetivo cumprimento dos deveres de cuidado e dos deveres especiais pelas plataformas.

Qual aventado por Cass Sunstein (2017) e Paul Shiff Berman (2000), empresas prestadoras de serviços de internet, como todas demais exploradoras de atividades econômicas de qualquer natureza, dependem de aparato público para fazer valer sua ingerência sobre o seu patrimônio e negócios. Em outros termos, as estruturas legais que garantem a propriedade e o lucro são seguradas pela existência de um corpo legal estatal vinculativo da sociedade como um todo. É esta raiz comum, originada no direito público, que faz supor que, em seu cerne, a separação entre público e privado é quimérica - e que torna justificável o afastamento dos direitos plenos de propriedade em nome do interesse comum. Em meio a tal simbiose conceitual, e novamente a invocar Paul Shiff Berman, definir com clareza os limites de público e privado "reflete a ordem social dominante", e acaba sendo mais uma questão cultural-ideológica do que uma demarcação teórica concludente (Shiff Berman, 2000). No caso do ciberespaço, a ambiguidade dos conceitos se mostra especialmente interessante ao somarmos a isso à proposta de Feintuck e Varney, de que manter partes sensíveis da infraestrutura comunicacional sob domínio público é uma questão de segurança democrática e de priorização do interesse público, para muito além da mera imposição da autoridade estatal (Feintuck e Varney, 2006) (Feintuck, 2010).

Em vista do exposto, ao interpretar parte das estruturas que permitem o fluxo de conteúdo *online* como matéria de interesse público, é praticamente impossível evitar a discussão sobre os limites da ingerência do Estado e as garantias legais devidas aos agentes privados envolvidos. Como ocorreu com o OSA, a tentativa de ingresso do Estado na regulação do ciberespaço, de modo mais efusivo do que vinha acontecendo até então, é seguidamente vista com ressalvas pelos agentes regulados e por parte da sociedade. Isso ocorre porque esses tendem a interpretar a imposição de deveres de prestação de informações e de transparência como tentativa do governo de enxugar, em boa medida, a liberdade de atuação das *bigtechs* naquele território, para além das críticas que veem no OSA ferramenta de censura dos discursos políticos. Na opinião deste trabalho, no entanto, tal movimento não deve ser rasamente interpretado como simples tomada autoritária de poder. Muito menos pode ser visto como colidente com a ciência, por parte do Parlamento, de que a ingerência direta sobre o ciberespaço segue concentrada nas mãos de atores privados transnacionais – o código é a lei, afinal. Se o Parlamento estivesse a simplesmente usurpar o controle dos meios de comunicação, o processo de produção legislativa do OSA não teria contado com a participação do setor privado na

proporção que foi (o que, desde a perspectiva do embate de forças, mais aparenta ser um sintoma da ciência do administrador britânico de sua impotência procedimental e da utilidade, para as *bigtechs*, da existência de respaldo regulatório legal). Tampouco as mudanças com relação ao projeto original, que previa maior incidência de mecanismos de controle de conteúdo para usuários adultos, teriam ocorrido (nesse ponto, é de conhecimento público que a proposta inicial do OSA foi bastante alterada, com o texto final da lei voltado de forma muito mais incisiva a combater conteúdos nocivos para crianças e outros públicos pontuais).

Pelo contrário, os debates legislativos que trataram das propostas do OSA, sobretudo entre Parlamento e agentes regulados, denotam, de um lado, a aceitação por parte das plataformas da conveniência de ter o processo de moderação de conteúdo orquestrado pelo Estado (Kafka, 2019). Mesmo Evgeny Morozov, na mesma entrevista que inicia as reflexões deste subcapítulo, menciona que regulação, até certa medida, é atualmente encarada como elemento útil às empresas de tecnologia. Isso pois essas últimas, em vista da dificuldade de obter sucesso no controle de conteúdo via autorregulação, encontram na normatização estatal espécie de resguardo contra eventuais responsabilizações (Mello, 2023). De outro lado, representando o interesse público, a opção por exigir mais transparência de provedores de serviços de internet consiste no meio eleito pela administração para se pôr a par do que acontece no ciberespaço, ainda que parcialmente. Estando o controle direto do código sob a ingerência de companhias transnacionais, e sendo a disponibilidade de informação condição mínima para o Poder Público levar adiante políticas institucionais e administrativas, a exigência de prestação de informações torna-se elementar para consecução de estratégia regulatória da envergadura do OSA. Trocando em miúdos, sem a possibilidade de exigir dados e relatórios de transparência, a regulação pretendida pelo OSA não seria sequer possível.

É interessante, nesse ponto da reflexão, observar que a conveniência de projeto regulatório para as *bigtechs* não significa que, para suas atividades empresariais, a transferência de informações à autoridade reguladora seja encarada sem objeções. Não é surpresa que acomodar interesses públicos e privados não consiste em tarefa simples. Como um dos exemplos mais drásticos disso, constantes no próprio OSA, tem-se o dever de prestar informações mediante requerimento do OFCOM. De acordo com a nova lei, a autoridade reguladora passará a gozar de poder para requerer, mediante notificação, que provedores de

serviços de internet[85] prestem informações de qualquer tipo caso essas sejam condizentes com os deveres de cuidado ou deveres especiais implementados e fiscalizados pelo OFCOM, nas ocasiões que esse entender que há motivos para tal requisição. Não é preciso ir longe na exposição da lei para o leitor perceber, aqui, que conteúdos relacionados com os deveres de cuidado e deveres especiais perfazem um extenso conjunto de possibilidades - em sentido amplo, inclusive, é possível enquadrar quase qualquer conteúdo em uma das espécies de cuidado devidas pelas plataformas. A gama é tamanha que, em alguns casos, é possível que as informações pretendidas pelo OFCOM estejam protegidas por criptografia de ponta a ponta, dados até então intocados a nível internacional. Nesse ponto, o OSA, em que pese tenha cedido em boa medida na sua rigidez para controle de conteúdo nocivo para adultos, reservou à autoridade reguladora poder de textura bastante aberta, invocável sempre que o órgão entender cabível. O exemplo ilustra a complexidade de tentar equilibrar interesses privados, possibilidades factíveis de regulação, e objetivos administrativos da parte do governo, bem como consiste em um dos aparatos que melhor refletem a importância atribuída ao OFCOM a partir da vigência do OSA. Muito embora não seja possível prever se, com a lei em vigor, o governo terá poder político de colocar em prática tal possibilidade, desde já é possível perceber que o exemplo em comento representa consistente sobreposição do interesse público sobre as atividades privadas.

O dever de elaborar relatórios de transparência, cujos critérios a serem publicizados e entregues ao OFCOM deverão ser definidos amiúde pela própria autoridade reguladora, é igualmente revelador da dificuldade de dissociar o ciberespaço e a agência das *bigtechs* de seu caráter público. Ele também ilustra o quanto a transparência das plataformas é elementar para o Estado atuar da forma que pretende fazer através do OSA. São enumerados, a seguir, dois argumentos para ilustrar essa afirmação. Primeiro, que a exigência de dados e informações, juntamente com o dever de disponibilizá-los à administração, é condição *sine qua non* para tratamento adequado do direito à liberdade de expressão na era digital. Segundo, que é somente por meio do acesso a dados de operacionalização e estruturação do *design* das plataformas que estas poderão ser responsabilizadas de forma justa e em observância do devido processo legal, pondo de lado o atual modelo de "teatro de transparência" (Douek, 2022, p. 47).

[85] A OSB especifica quais pessoas, jurídicas ou não, poderão ser questionadas pelo OFCOM, em lista detalhada que menciona não apenas as empresas reguladas, como também representantes nomeados e intermediários (REINO UNIDO, OSB, 2023, p. 95).

No curso deste trabalho, em mais de uma ocasião, foi comentado que o direito à livre manifestação das ideias representa um dos principais entraves para a implementação de sistema de moderação de conteúdo *online*, especialmente nos casos em que esses sistemas advêm de propostas do Poder Público. Desde os debates iniciais entre ciberlibertários e ciberpaternalistas, a liberdade de expressão, ainda que se admita seu caráter de direito fundamental, ocupa papel central nas discussões sobre a medida ideal para participação estatal na moderação dos discursos no ciberespaço. Em vista do controle do código pelas plataformas, no entanto, e em matéria de transparência, não há dúvida que a falta de acesso a dados que demonstrem os critérios, a quantidade e a incidência da remoção de conteúdos pelas plataformas fere sistematicamente a liberdade de expressão como direito individual - porquanto a opacidade informacional impede que se saiba, publicamente, qual tratamento é dispensado pelos agentes privados a este direito. A discricionariedade com que os discursos são suprimidos nas redes, juntamente à inexistência de parâmetros claros para tal moderação, não deixa margem para a sociedade e as autoridades avaliarem se a livre manifestação das ideias no ciberespaço é tratada de modo justo e equânime. Essa sistemática resulta em um turvo sistema de dois pesos e duas medidas para remoção de conteúdo. Diante desse quadro, é confortável afirmar que é somente na posse de dados – claros, corretos e abrangentes -, concentrados junto a uma autoridade centralizadora, que será viável conciliar liberdade de expressão e preceitos democráticos nas redes. Essa máxima mais uma vez reitera a natureza pública do controle dos discursos nesses espaços, bem como a necessidade de abordá-la desde a perspectiva do interesse coletivo.

Esse trabalho está de acordo com a afirmação de Douek de que "transparência é um meio, não um fim, e precisa ser direcionada para ser eficaz " (Douek, 2022, p. 47). Em vista disso é que se entende que a mera predisposição das plataformas a prestarem informações e serem mais transparentes não é suficiente para satisfazer parâmetros efetivamente democráticos. Veja-se o exemplo a seguir. Por iniciativa própria, a Meta, por intermédio do Facebook, propôs a produção de relatórios de transparência periódicos das suas atividades[86], os quais vêm efetivamente sendo entregues pela empresa. Tais relatórios, no entanto, não são produzidos por outras plataformas de envergadura semelhante, e, ainda que o fossem, ante a ausência de corpo regulatório uno para definir quais informações *devem* ser arroladas, não é possível traçar comparativo entre as agências de cada uma delas em matéria de controle de conteúdo, menos ainda estabelecer balizas legais a serem observadas por todos os provedores

[86] Periodicamente o Facebook publica relatórios com dados referentes a propriedade intelectual, respostas da empresa a requerimentos de governos, tipos de conteúdos mais acessados, políticas de conteúdos vedados pela Meta, dentre outros dados. Ver em https://transparency.fb.com/reports/. Último acesso 04/10/2023.

atuantes no mercado. É somente mediante a definição, por parte de autoridade reguladora, de quais informações devem ser publicadas, e em qual grau de detalhamento, que será possível estimar e avaliar o tratamento dispensado à liberdade de expressão nas redes. Neste ponto, é interessante fazer constar que não se está a defender a imposição estática de critérios a serem divulgados - pelo contrário, isso apenas acentuaria o atual modelo de reprodução *online* do controle dos discursos feito pelas cortes, e contribuiria para a obsolescência prematura de leis como o OSA -, mas sim postula-se a conveniência da uniformização mínima das informações prestadas por cada plataforma quanto aos resultados e procedimentos de suas políticas de moderação de conteúdo. Por fim, do exposto se conclui que políticas de transparência, no caso do OSA concretizadas sobretudo nos relatórios periódicos de transparência, serão essenciais para a responsabilização das plataformas por conteúdos hospedados e circulados por meio de suas estruturas. Sem informação não há administração, afinal, e menos ainda a possibilidade de responsabilização de pessoas jurídicas no estado democrático de direito.

Em consideração às reflexões até aqui empreendidas, torna-se interessante observar que a aventada simbiose entre público e privado, no OSA e em matéria de deveres de transparência, encontrou caminho por vias da prevalência do direito público. Em que pese outras seções da lei sigam bastante divididas e equilibrando de forma equânime as esferas pública e privada, na imposição dos deveres de transparência o OSA reserva poderes de monta ao OFCOM, que terá a discricionariedade de exigir das plataformas informações dos mais variados tipos, invocáveis sempre que necessário para garantir o cumprimento das atividades da agência - opção estratégica do legislador para conferir eficácia e longevidade ao projeto regulatório. Nesse sentido, a abordagem do OSA vai ao encontro da obra de Sarlet e Martins Hartmann, os quais ponderam sobre as relações entre direito privado e direitos fundamentais no ciberespaço:

> [...] os direitos fundamentais, pelo menos de acordo com o entendimento prevalente na ordem jurídico-constitucional brasileira, geram efeitos diretos *prima facie* no âmbito das relações privadas, o que, além de pressupor uma metódica diferenciada, inclusive no âmbito das plataformas de mídia social, também implica o reconhecimento de uma relação de complementariedade entre a vinculação dos órgãos estatais e a vinculação dos atores privados aos direitos fundamentais, que também se verifica em relação ao modo pelo qual se opera essa eficácia. Nesse contexto, importa relembrar aqui as sempre atuais lições de Vasco Pereira da Silva, no sentido de que, independentemente do modo pela qual se dá, em concreto, a eficácia dos direitos fundamentais nas relações privadas, entre as normas constitucionais e o direito privado o que se verifica não é um abismo, mas uma relação pautada por um contínuo fluir (1987, p. 46) (Martins Hartmann e Sarlet, 2019, p. 105).

Voltando novamente ao OSA, a faculdade do OFCOM para requerer informações representa um dos pontos onde mais explicitamente o interesse público foi colocado como prioridade pelo legislador. Em vista das particularidades do ciberespaço que vêm sendo comentadas neste trabalho, é difícil dizer que a lei poderia ser muito diferente do que se convencionou ser. Caso não fosse possível à autoridade reguladora requerer informações para se pôr a par de eventuais descumprimentos dos deveres de cuidado e dos deveres especiais pelos atores regulados, o OSA facilmente perderia sua razão de ser, e tenderia a repetir o fracasso do DEA 2017. Isso porque não haveria como embasar ordens do OFCOM para que empresas se adequassem (fosse mediante tecnologia, fosse mediante medidas administrativas) aos padrões de segurança *online* da nova lei. Outrossim, as possibilidades de a autoridade reguladora requerer informações, intimar a depor, proceder vistorias *in loco*, requerer nomeação de pessoa responsável, dentre outros poderes previstos (e especificados no subcapítulo 3.4.3.3) devem ser interpretados como reflexo da dificuldade do regulador de dissociar o caráter público do ciberespaço. Dito traço é signo de que as trocas aí realizadas extrapolam em muito a seara comercial e adentram a vida em sociedade em suas mais ricas facetas, de forma que os contratos aí firmados devem servir, ao fim e ao cabo, a valores de direito público (Lessig, 1999).

Em meio às negociações legislativas entre agentes regulados, sociedade civil, academia e governo, manter tamanho poder discricionário concentrado junto ao OFCOM representa vitória dos que defendem a ingerência do Poder Público no ciberespaço como meio de resguardar liberdades individuais. Ainda assim, como desfecho deste subcapítulo, importante ressalva deve ser feita. Os relatórios de transparência aqui mencionados devem ser entregues ao OFCOM, e não há previsão no OSA de que estes sejam disponibilizados à comunidade de forma geral. Em que pese a opção seja compreensível, em razão dos riscos envolvidos em revelar estruturas de *design* e criptografia das plataformas no mundo todo, para fins de efetiva transparência social e *accountability,* o quadro é desastroso. Qual mencionado, transparência de dados é pré-requisito para responsabilização de plataformas. Contudo, para isso, é fundamental que uma audiência crítica, coletiva, e representativa dos mais diversos estratos da sociedade britânica tenham acesso a estas informações. Além disso, concentrar o acesso às informações sobre as soluções de *design* e tecnologia adotadas pelas plataformas junto à autoridade reguladora, sem prever se esses dados poderão ser acessados pela comunidade interessada, tende a prejudicar o desempenho do próprio OSA – a exemplo do triplo escudo, em que um dos pilares consiste justamente em munir o usuário de informações

sobre a estrutura algorítmica e dados técnicos da empresa provedora. Sobre o ponto, está-se de acordo com as críticas que defendem que os relatórios de transparência sejam traduzidos para linguagem acessível e postos à disposição da sociedade (Fowler-Mason, 2023).

4.3 Responsabilização de plataformas e a retomada de espaços de poder pelo Estado.

Este trabalho foi iniciado com metáfora proposta por Cass Sunstein (2017). Nessa, a concentração dos indivíduos em bolhas de afinidade no ciberespaço foi contrastada com a profusão de trocas própria das cidades democráticas, no mundo real, onde o convívio entre sujeitos de posicionamentos díspares é elementar para a saúde da sociedade. De outra senda, mas guardando simetrias com a metáfora das cidades, foi explorada, por intermédio da obra de Vili Lehdonvirta (2022), a reprodução de comportamentos estatais tradicionais como estratégia institucional de grandes plataformas. Isso pois *bigtechs* crescentemente mimetizam características próprias do Estado Moderno como mecanismo de tomada de espaço e controle sobre os ambientes virtuais por elas criados, em um movimento que acaba por ensejar a tomada de espaço do Estado tradicional por essas empresas. A notória discrepância entre o arranjo das comunidades em redes sociais, afinadas e isoladas pela agência de algoritmos direcionadores de conteúdo, e o convívio, ainda que superficial, entre cidadãos de orientações diversas ocupantes de uma mesma cidade no mundo de carne e osso, somados à conduta governamental das plataformas, desenha quadro que pauta a análise proposta neste subcapítulo. Vincular a metáfora de Sunstein ao comportamento estatista atribuído por Lehdonvirta às *bigtechs* permite enxergar (e complexificar) as estratégias institucionais dos provedores de grandes portais da internet, ao mesmo tempo que explica, ao menos em parte, as propostas do Poder Público que buscam reaver parte do controle sobre a infraestrutura de mídias e fluxo de dados. Para refletir sobre esse cenário, com enfoque no OSA, será explorada a possibilidade de responsabilização de plataformas como agentes intermediários de conteúdos danosos ou ilegais veiculados por meio de suas redes, a qual deve ser interpretada como reação do Estado britânico para recuperar sua ingerência sobre espaços públicos virtuais, bem como restaurar o equilíbrio de trocas entre cidadãos de posicionamento antagônico, próprio da cidade democrática.

A fim de realizar o exercício ora proposto, é interessante que sejam repassados, de início, os três casos descritos na obra de Lehdonvirta para exemplificar a agência das *bigtechs* ao tomar para si comportamentos próprios do Estado nacional moderno. O autor menciona os

casos do [1] *EBay*, que ante o crescimento da plataforma teve de adotar medidas de controle do fluxo de comércio e regras de garantias consumeristas. [2] Menciona também o caso da *SilkRoad*, com o qual bem ilustra a importância de mecanismo de identificação pública dos indivíduos presentes no espaço administrado pela plataforma, a fim de fazer valer normas sociais básicas de ordem sobre esses sujeitos. [3] E, por fim, narra o caso da *UpWork*, a qual, em vista do aumento da comunidade usuária da plataforma, se viu obrigada a adotar normas de mercado, regulação de trabalho e regras para demarcar territorialidade. Em todos os exemplos pinçados, tratou-se de plataformas cujas origens tinham inspiração libertária, desejosas de se verem livres da ingerência estatal, mas que acabaram, ao cabo, por emular estratégias de controle utilizadas pela mesma autoridade coercitiva que se empenhavam em abolir (Lehdonvirta, 2022) - para retomar os casos com maior detalhamento, ver subcapítulo 2.5.

Os exemplos em comento foram motivados, sem exceção, pela necessidade de manter a ordem nos espaços criados pelas plataformas, em decorrência do aumento do número de pessoas usuárias e frequentadoras destes locais – em movimento similar ao da cidade moderna, crescentemente populada por indivíduos das mais diversas origens e condutas. Ante às ações de indivíduos nem sempre identificáveis e sem vínculos entre si para além das atividades ali travadas, provou-se que a coordenação unificada de autoridade hierarquicamente superior era a ferramenta mais eficaz para evitar o caos administrativo daqueles universos virtuais. Em retorno à analogia das cidades modernas, efervescentes pelo crescimento das trocas comerciais e individuais que ali ocorriam, foi justamente a unificação do controle sobre exércitos, comércio e administração pública em geral que ensejou a centralização da autoridade estatal na Idade Moderna, gênese dos Estados nacionais racionais, em movimento que permite substanciosas analogias com o aumento em número e complexidade das transações executadas no ciberespaço. Qual posto na obra de Lehdonvirta, a fixação de normas para frequentar o ciberespaço e a capacidade das *bigtechs* de conquistarem tamanho poder administrativo sobre a vida pública guardam próxima relação com o repasse a agentes privados, no início do século XXI, do controle sobre o processamento de dados eletrônicos (Lehdonvirta, 2022). A concentração de pontos fulcrais da estrutura de mídias junto a atores da iniciativa privada, processo ocorrido ao longo do século XX, comentado nos subcapítulos antecedentes e denunciado por autores como Feintuck (2006 e 2010) e Rowbottom (2010), é também contribuidor para dito quadro de distribuição de poderes.

Apresentado esse cenário, resta analisá-lo criticamente. Em razão do caráter quase essencial dos serviços oferecidos pelas grandes empresas de tecnologia, os quais se

popularizaram e são cada vez mais tratados como espaços de uso público, a atuação administrativa seletiva das plataformas deve ser vista com cautela. Caso a situação se reduzisse a simples reprodução de mecanismos de controle e administração estatal por atores privados, não muito haveria a ser acrescentado, e o debate possivelmente se voltaria à controvérsia ideológica que discute os limites administrativos ideais entre o Estado e a iniciativa privada. No entanto, para além da falta de legitimidade de plataformas transnacionais para se comportarem como se autoridades estatais fossem, há de se destacar que essas estão em larga medida desvinculadas de preceitos constitucionais e de direito público para tomada de decisões (Lehdonvirta, 2022). Isso tem consequências diretas para os usuários dos espaços de uso comum por elas administrados e atinge, mais uma vez, questões de interesse coletivo. Ao contrário do que Lessig outrora recomendara - de que se encontrasse, na regulação da internet, o ajuste e o espírito da constituição aplicado ao ciberespaço (Lessig, 1996) -, a administração privada de espaços virtuais de interesse não presta garantias inequívocas de respeito a direitos individuais ou coletivos (qual referido no subcapítulo 2.5, a seletividade das decisões impostas pelos provedores aos seus usuários ou prestadores de serviços deflagra a inconstância nos tratamentos dispendidos casuisticamente). Além disso, o caráter transnacional dessas plataformas torna tal característica particularmente difícil de ser enfrentada pelos Estados tradicionais.

Considerando o exposto, é interessante refletir sobre o potencial do OSA de se projetar em tal cenário, sobretudo mediante a possibilidade de responsabilização objetiva de *bigtechs*. Nesse terreno, propõe-se dividir a análise em dois tópicos principais, mas que a todo tempo devem ser correlacionados. Primeiro, a enxergar a atribuição de responsabilidade a plataformas em razão de conteúdo danoso veiculado em suas redes, e em casos de inobservância dos deveres de cuidado ou deveres especiais, como reação do Estado racional coator, detentor da capacidade punitiva por excelência. Segundo, a interpretar esse movimento de retomada de influência como uma cautelosa estratégia de descentralização das políticas institucionais das *bigtechs*, buscando enfraquecer a administração de temas políticos das plataformas de internet, mas sem interferir diretamente em suas atividades financeiras.

No tocante ao primeiro ponto, dispensam-se grandes elocubrações para perceber que a decisão do legislador britânico pela possibilidade de responsabilizar plataformas representa sistematização necessária para que a autoridade estatal tenha condições de fazer valer as determinações dispostas no OSA. Tratando em termos realistas, "responsabilização é o primeiro passo necessário para efetiva intervenção" (Douek, 2022, p. 59), e é pouco provável

que outra abordagem pudesse aportar a mesma eficácia ao OSA, ao menos nas condições da conjuntura atual. É sabido que a possibilidade de responsabilização de plataformas tende a ensejar um maior arrojo dessas para remoção e supressão de conteúdos, já que, para evitar as sanções legais, provedores estarão potencialmente mais inclinados a remover materiais do estariam que sob regime de autorregulação. Outrossim, não há dúvida que esse arranjo terá o condão de interferir de forma direta sobre a liberdade de manifestação de usuários em geral. Tal dinâmica permite deduzir que a opção do governo britânico por impor penas de vultuosas multas (relembremos que estamos tratando de sanções de 18 milhões de libras esterlinas ou 10% do lucro anual obtido pela empresa, "o valor que for maior"[87]), juntamente com a possibilidade de pena privativa de liberdade a dirigentes e responsáveis, denota sua preferência por alcançar as finalidades regulatórias do OSA por meio da capacidade punitiva do Estado tradicional. É certo que muito se comenta sobre a insuficiência do modelo autorregulatório e de controle casuístico para remoção de discursos no ciberespaço, o que em uma análise breve justifica a predileção do OSA pela responsabilização de agentes intermediários. Ainda assim, em vista da disputa política existente sobre o controle dos espaços das redes - neste caso entre Estado tradicional e grandes provedores transnacionais -, é pertinente pensar o caso desde a perspectiva proposta por Lehdonvirta.

Qual comentado em mais de uma ocasião, o OSA concentra enormes poderes junto ao OFCOM. Além de ser somente por intermédio da autoridade reguladora que a responsabilização de plataformas poderá ser efetivada, ao OFCOM foi atribuída uma série de outros poderes. Apenas a título de menção, para recobrar o examinado no subcapítulo 3.4.4, a agência terá a faculdade de abrir investigações e de solicitar informações e avaliar, segundo seus critérios, a qualidade e o empenho das medidas tomadas pelas plataformas administradas no cumprimento de deveres de cuidado e deveres especiais. Mesmo a obstrução às atividades investigativas do OFCOM pode ser enquadrada como crime de responsabilidade, com penas pecuniárias e privativas de liberdade previstas. No leque de atribuições ora delegadas à autoridade reguladora, é interessante observar que a capacidade de investigar e concluir, ela própria, pela responsabilização por não cumprimento de deveres de cuidado pelas plataformas, bem como encaminhar ao Judiciário os casos que entenda necessários, consistem em ferramenta do Parlamento para trazer, para sob a égide do Estado coator e detentor do poder legítimo de violência, parte da ingerência sobre o ciberespaço.

[87] Rever nota 86.

Recorrendo a definição clássica de Estado Moderno de Max Weber, de que o

> Estado é aquela comunidade humana que, dentro de determinado território - este, o "território", faz parte da qualidade característica -, reclama para si (com êxito) o monopólio da coação física legítima, pois o específico da atualidade é que a todas as demais associações ou pessoas individuais somente se atribui o direito de exercer coação física na medida em que o Estado o permita. Este é considerado a única fonte do "direito" de exercer coação física na medida em que o Estado o permita [...] (WEBER, 2004, p. 529)

Dar ao Estado regulador a roupagem de detentor da violência legítima permite que associemos as faculdades atribuídas ao OFCOM à autoridade própria do Estado coator, encarando tal movimento como reação frente ao ganho de espaço das plataformas na conjuntura internacional de poder, ao mesmo tempo em que são observadas as limitações próprias da autoridade estatal sobre as estruturas do ciberespaço - no qual o domínio sobre o código segue concentrado junto a atores privados transnacionais. A associação proposta mostra-se particularmente interessante ao se ter em consideração o antagonismo existente entre comunidades no ciberespaço e comunidades na cidade moderna surgente, aquele mesmo observado por Sunstein (2017). Isso pois foi a proliferação das trocas na cidade medieval um dos principais fatores a permitir a consolidação do Estado burocrático racional e, nos séculos seguintes, das democracias modernas ocidentais. Em vista disso, é no mínimo curioso que, hoje em dia, a reprodução de mecanismos estatais modernos por parte das *bigtechs,* nos espaços de convívio do mundo virtual, convirjam para a concentração por afinidade ao invés das trocas de outrora. Tal singularidade do ciberespaço serve a demonstrar, juntamente com outros indicadores, os riscos à democracia provenientes da aglutinação dos sujeitos por afinidade, bem como justificar a ação ora empreendida pelo Parlamento britânico.

De volta à análise que reflete sobre a presença do Estado coator na regulação da internet, cabe pensar essa relação desde o ponto de vista das *bigtechs*. Não obstante o comportamento institucionalizado das plataformas, e a despeito de sua inegável influência na política e organização social de quase a totalidade dos Estados nacionais, é interessante observar que lhes falta poder coator mediante uso de violência legítima (nesse caso, a autoridade legítima para cercear a liberdade de locomoção e atividades econômicas dos sujeitos, já que não se está aqui a aventar a possibilidade de disputa bélica ou que envolva vias de fato em qualquer grau). Por certo, o caráter de quase imprescindibilidade dos serviços oferecidos pelos grandes portais de internet faz com que esses gozem de enorme poder sobre recursos de primeira necessidade nos cotidianos modernos (se o Google, por motivo arbitrário, decidisse suprimir o Gmail subitamente, quase ¼ da população mundial seria diretamente

afetada[88], e há nessa faculdade poder de coação), mas isso de modo algum se confunde com a legitimidade da qual se imbui o Estado, e tampouco seu poder de diretamente intervir nas atividades econômicas das *bigtechs*. Tal relação deflagra que, apesar do poderio sem precedentes das empresas provedoras de serviços de internet, a legitimidade do Poder Público para lançar mão de mecanismos de punição segue despontando como uma das principais ferramentas de manutenção de poder. O que se salienta aqui, fazendo uso da imposição de responsabilização a plataformas e atribuição de poderes ao OFCOM, é que, no desfecho do processo legislativo para controle de conteúdo no Reino Unido, e apesar da profusão de diálogos e negociações travadas no Parlamento, foi por intermédio do poder punitivo que a autoridade estatal logrou se aproximar da ingerência sobre o ciberespaço.

É manifesto que, de momento, não há meios que permitam prever se a estratégia adotada no OSA será frutífera ou não. Ademais da lei ter deixado largas frestas de textura aberta para controle de conteúdo adulto (as quais deverão ser preenchidas pela agência do OFCOM), as variáveis em jogo são muitas e bastante recentes para que se possa ambular pela regulação das redes pisando em solo firme. Ainda assim, alguns apontamentos finais podem ser feitos no tocante à possibilidade de responsabilização de agentes intermediários por conteúdos danosos ou ilegais. Outrossim, é possível afirmar, com segurança, que a opção do Parlamento perfaz em parte as sugestões teóricas de Lehdonvirta e Douek.

O OSA se afina com Douek no sentido de que a identificação e responsabilização de agentes e empresas, por danos decorrentes de conteúdos circulantes nas redes, é uma saída constitucionalmente mais factível e politicamente mais promissora do que o controle casuístico e judicial da liberdade de expressão (Douek, 2022). Isso porque esse último está fadado à disputa ideológica e à sobrecarga do sistema judicial em razão do enorme fluxo de informação nas redes, muito superior à capacidade de vazão processual do Judiciário. A proposta também dialoga, ao menos em parte, com a proposição de Lehdonvirta, no sentido de que o OSA confere legitimidade à atuação dos provedores de serviços de internet ao atribuir caráter de *gatekeepers* a algumas plataformas (notadamente aquelas de Categoria 1A), ao mesmo tempo que imputa deveres de cuidado e responsabilidade a essas. Ao endossar ou refutar as políticas de funcionamento desenvolvidas e propostas por cada empresa, a lei acaba por direcioná-las a agirem em consonância com parâmetros e valores próprios do Estado regulador. Não obstante

[88] Levantamento da empresa divulgou que existem, em 2023, 1.8 bilhões de contas de e-mail ativas. Cerca de 22,2% da população mundial. Ver em https://www.demandsage.com/gmail-statistics/. Último acesso 12/10/2023.

o OSA não seja avançado a nível de cimentar o ciberespaço como ambiente democrático, onde as vozes dos usuários membros da comunidade têm poder de serem ouvidas – ponto no qual a obra de Lehdonvirta não encontra eco algum na nova lei britânica –, alguns mecanismos demonstram o reconhecimento do regulador acerca da importância da participação, ainda que muito tímida, dos cidadãos ordinários neste espaço. Como exemplo, têm-se os deveres de transparência e de acesso à informação por parte dos usuários, os quais representam parte do movimento que busca aportar ares de troca e de democracia ao ciberespaço. Por fim, a atribuição de responsabilidade a provedores não fere suas finalidades de lucro, as quais continuam respeitadas e passíveis de seguirem sendo exploradas no modo de produção capitalista no qual vivemos. Isso tende a demonstrar, na prática, a colocação de Lehdonvirta de que é muito mais fácil e efetivo interferir na esfera política das plataformas do que em sua estrutura econômica e de produção de lucro (Lehdonvirta, 2022, p. 232).

5. Conclusão

Antecipar o sucesso do OSA nunca poderia ter sido o objetivo deste trabalho. As previsões da lei são numerosas, o esmero do Parlamento em não repetir os resultados do DEA 2017 é notório, e as variáveis em jogo são tantas que predizer seu futuro mais perfaria o campo da adivinhação do que da ciência. Ainda que esse trabalho se pautasse amiúde pelo texto aprovado, a pendência de códigos de procedimento e conduta, os quais devem ser produzidos pelo OFCOM e aprovados pelo Parlamento para que o OSA entre em pleno vigor, não permite grandes prognósticos quanto ao desempenho do novo aparato regulatório. É somente após a entrada da autoridade reguladora em cena que serão definidos detalhes secundários. Como exemplo, aguarda-se a definição de o que deverá constar nos relatórios de avaliação de risco; quais serão os parâmetros de implementação de dispositivos de segurança e controle de conteúdo; quais serão as ferramentas de recursos e empoderamento disponibilizadas aos usuários; ou, ainda, quais serão os modelos de relatórios de transparência e dos relatórios de prestação de contas para cobrança de taxas; dentre uma infinidade de outras normatizações.

Em vista do caráter novel da OSA, este trabalho se empenhou em analisá-la como ferramenta regulatória e política, lançada pelo Poder Público em meio a um cenário de disputas sobre os usos e controle a serem feitos do ciberespaço, daqui em diante. Para alcançar tal fim, escolheu-se explorar as disposições da lei sobre deveres de cuidado, empoderamento do OFCOM, deveres de transparência e responsabilização de plataformas. Julgou-se que esses pontos compõem, juntos, suficiente panorama da proposta regulatória britânica. Não obstante o OSA reflita o caso do Reino Unido, por certo seu processo guarda paralelos com outros movimentos regulatórios da internet em outras jurisdições, no Brasil inclusive - considerando que as disputas sobre a hegemonia no ciberespaço se dão a nível internacional. Desse modo, entendemos que a análise do caso britânico contribui para ampliar os debates que refletem as adaptações do Direito e dos Estados nacionais ante a nova ordem dominante das *bigtechs.* Além disso, ela serve também para refletir sobre a crescente importância das relações humanas travadas no ciberespaço nas sociedades de modo geral.

A despeito da impossibilidade de prenunciar os resultados do OSA, e em vista das reflexões aqui construídas, alguns pontos sobre a estrutura e posicionamento políticos da lei já podem ser levantados com considerável segurança. De início, é patente que a sua proposta de moderação sistêmica, *ex ante*, e pautada em políticas de *design* de plataformas, aposta na

regulabilidade da moderação de conteúdo no ciberespaço mediante ingerência indireta da autoridade estatal. Isso, tratando em termos que remetem às origens do debate sobre a regulação da internet, põe de lado antigos auspícios ciberlibertários e aposta na imposição de regras de funcionamento que busquem garantir, no ambiente do ciberespaço, a observância de valores e princípios caros ao Estado regulador estrito senso. No tocante à liberdade de expressão, possivelmente o princípio de maior relevância quando se pensa nos entraves ao controle de conteúdo e de discursos no ciberespaço, a substituição, ainda que parcial, de mecanismos de *soft law* e de autorregulação por imposições duras, com penas pecuniárias de grande monta e privativas de liberdade previstas, denota significativa mudança de paradigmas e de estratégia. Há, por um lado, o abandono da primazia da livre manifestação das ideias em prol de um controle que, embora não muito rígido, esteja voltado a garantir a saúde democrática dos debates e o controle de acesso de usuários crianças a determinados conteúdos. Algo parecido ocorre com o direito à intimidade e com questões de privacidade, porquanto o OSA chega ao ponto de prever a possibilidade de quebra de sigilo de serviços de mensageria encriptada. No tocante à "saúde democrática dos debates", é importante frisar que, sob a égide do OSA, essa deverá seguir preceitos gerais controláveis pela autoridade reguladora. Esses elementos aproximam, como nunca antes em um país de tradição liberal, a moderação de conteúdo nas redes e o Poder Público. Por fim, no tocante à proteção de usuários crianças, em que pese não tenha sido esse o enfoque do presente trabalho, é importante que seja mencionado, a título de conclusão, que se tratou do ponto que mais progrediu no projeto de lei muito em função de a proteção ao público infanto-juvenil ser tema de pouca divergência ideológica entre estadistas e privatistas. Isso ocorre porque, nesse último tópico, o cuidado com a liberdade de expressão encontra pouco eco.

O teor voltado ao resguardo do interesse público do OSA é de fácil percepção. Deveres de transparência que reservam poderes de monta ao OFCOM são exemplos disso. A atribuição de deveres de cuidado é também fruto dessa proposta. Também o são a responsabilização de plataformas por conteúdos de terceiros, o poder do OFCOM de empreender investigações e solicitar informações, bem como a possibilidade de a autoridade reguladora encaminhar casos ao Poder Judiciário quando julgar tratar-se de situação de "alto risco de dano a indivíduos no Reino Unido, dispensada a necessidade de emissão de nota provisória de contravenção ou de confirmação de decisão" (Reino Unido, 2023, p. 124). Todos os exemplos mencionados são significativos no sentido de ilustrar o quanto a nova lei se preocupa com estender garantias cidadãs ao ciberespaço no Reino Unido, sempre por

intermédio da força do Estado e a despeito da conduta até aqui priorizada pelas plataformas. Trocando em miúdos, a abordagem do OSA pode ser vista como espécie de transposição parcial do estado social para o ciberespaço.

Ainda assim, é importante notar que não há na nova legislação quaisquer menções à ingerência ou ao controle direto da Administração Pública sobre as estruturas de mídia nas quais operam as plataformas, contrariando as recomendações de pensadores como Feintuck e Morozov. Do mesmo modo que ocorreu no DEA 2017[89], o OSA não legisla de forma a explicitar como o interesse coletivo será buscado, delegando todos os pormenores à normatização secundária que deve ser produzida pela autoridade reguladora e pelas próprias *bigtechs*. Muito embora a lei permita ao OFCOM requisitar às plataformas informações detalhadas sobre sua arquitetura, estrutura algorítmica e políticas de funcionamento, não há como saber, com base no texto da lei nua, se a autoridade reguladora terá capacidade de saber quais informações requerer. A julgar pelo caráter fundamental de estruturas basilares de mídia para a democracia, bem como em decorrência das dificuldades técnicas advindas da complexidade da estrutura digital das plataformas, corre-se o risco de a Administração não gozar, sequer, de capacidade para processar tais dados sem o apoio de agentes privados. Isso, combinado com a inexistência de controle direto sobre infraestruturas básicas de comunicação, tem o potencial de significar continuidade dos riscos à democracia e ao acesso de usuários vulneráveis a conteúdos indevidos que, esperava-se, o OSA combateria.

Em conclusão ao estudo de caso empreendido e ao histórico regulatório da OSA aqui pormenorizado, e em vista do texto final da lei aprovada pelo Parlamento, é possível também reconhecer o sucesso considerável da proposta original, aquela aventada quando da publicação do *green paper* da Estratégia de Segurança na Internet (2017a) e do *Online Harms White Paper* (2019). Nesses, eram preconizadas políticas de responsabilização de plataformas por conteúdos de terceiros, implementação de sistemas de transparência *online*, soluções tecnológicas para danos produzidos por materiais no ciberespaço, criação de uma entidade regulatória independente, contenção de danos específicos a crianças e outros usuários vulneráveis, elaboração de códigos de boas práticas e fixação de regras claras para as plataformas (Reino Unido, 2017a e 2019). Todas as políticas propostas e listadas acima, qual se colhe, foram em alguma medida efetivadas no OSA. Ainda assim, conforme mencionado, a nova regulação possui inequívoca textura aberta, mesmo para quem a analisa por intermédio das lentes do

[89] Onde foi definido que a atuação do OFCOM seria pautada pelo interesse público, sem pormenorizar *no que consistiria ou o que deveria vir a ser entendido como* interesse público.

sistema de *common law.* Desse modo, é possível afirmar com bastante segurança que o sucesso do OSA para moderação de conteúdo vai depender em larga medida da atuação reguladora posterior do OFCOM, bem como da manutenção das intenções políticas do Parlamento para seguir fazendo frente a interesses de atores transnacionais do ramo das plataformas. De outra sorte, insta reconhecer que a mesma estrutura aberta que mantém viva a disputa sobre *como* a moderação de conteúdo no ciberespaço vai ser implementada, viabiliza que o OSA se consolide como lei potencialmente mais duradoura do que suas antecessoras. Tal faculdade se mostra bastante conveniente, especialmente em vista do caráter ultra veloz do desenvolvimento de novas tecnologias de comunicação digitais e da alta capacidade do fluxo de conteúdo *online* para encontrar novas formas de fluir. Justamente por permitir maiores adaptações, a depender da demanda de usuários e fluxo de dados *online*, o OSA representa evolução legislativa em comparação ao falido sistema de notificação de usuários e detentores de direitos de autoria no DEA 2010, ou ainda o sistema de verificação de idade de todos os usuários, um dia idealizado no DEA 2017[90].

Apesar da manutenção das linhas gerais outrora sugeridas no ISSGP e no OHWP, a textura aberta da qual se revestiu o OSA é também sintomática das dificuldades de conciliar os inúmeros interesses políticos e ideológicos quando se trabalha moderação de conteúdo no ciberespaço. Vale lembrar aqui que, quando da publicação do primeiro esboço do projeto de lei, o *Draft Online Safety Bill (*DOSB), foi proposta a criação de dever de cuidado com relação a conteúdos legais, porém nocivos. Como estudiosos e internautas, é fácil para o leitor perceber que o significado de conteúdo nocivo *apesar de legal* serve a enquadrar quase qualquer tipo de material - e o que parece nocivo para um por vezes não parece para o outro. Na ocasião, a ideia gerou verdadeiro alvoroço, tanto entre a sociedade civil quanto entre as plataformas alvo do projeto regulatório. Os primeiros reclamavam que a medida colocaria nas mãos de empresas estrangeiras o controle dos discursos no Reino Unido, os últimos contestavam a factibilidade técnica e riscos de negócio potencialmente aportados pela proposta, de forma que, posteriormente, a cláusula acabou por ser substituída pelo triplo escudo[91]. Críticas à factibilidade ou ao caráter intrusivo da proposta à parte, é certo que foi a partir desse ponto que o OSA deixou de ser um projeto de proteção ferrenha contra conteúdos nocivos para todos os grupos e se voltou a zelar com mais vigor por usuários crianças ou em condição de

[90] O sistema de verificação de identidade ora previsto na OSA é muito mais aberto que seu antecessor, e delega às plataformas o desenvolvimento do mecanismo de checagem.
[91] Para maiores detalhes sobre o triplo escudo, ver *A Guide to the Online Safety Bill*, disponível em https://www.gov.uk/guidance/a-guide-to-the-online-safety-bill. Acesso em 20 de dezembro de 2023.

vulnerabilidade – o controle de conteúdo adulto é bastante menos rígido do que as demais matérias reguladas.

A dificuldade de moderar conteúdos adultos não expressamente vetados por lei tem no OSA exemplo prático de o quanto a liberdade de expressão é, ao fim e ao cabo, uma norma condicionadora dos comportamentos não facilmente modificável pela lei. Isso ocorre justamente em razão do caráter iminentemente cultural do direito de livre manifestação das ideias, aquele mesmo descrito por Balkin (2009). Ao pensar as quatro modalidades condicionadoras do comportamento de Lessig (1996), é interessante observar que, no ciberespaço, muito embora seja possível influenciar o código indiretamente por intermédio da lei, o mesmo não ocorre com as normas sociais – dentre elas a percepção coletiva do que é a liberdade de expressão. O código é a lei, mas isso não é suficiente para tocar corações e mentes daqueles que circulam entre o ciberespaço e o Estado nacional tradicional. Apesar das particularidades de estrutura do ciberespaço em comparação ao mundo real, e não obstante a literatura acadêmica insista em dizer que em razão das características do mundo virtual a liberdade de expressão lá deve ser tratada de modo diverso, a noção coletiva de liberdade de expressão segue, no ciberespaço, bastante próxima do que é no mundo real. É pouco provável que a regulação tenha o condão de modificar isso. Apesar de tal entrave, em meio às moções internas e externas pela implementação de sistema de moderação de conteúdo *online* no Reino Unido (lembrando aqui da governança ágil do FEM e da OCDE, mencionada no Capítulo 3, e da proposta das Nações Unidas de criar quadro regulatório geral para controle de conteúdo a ser aderido por países membros) (Fjeld, 2023), o Parlamento chegou a um resultado surpreendentemente voltado à defesa dos interesses do Estado. Isso especialmente ao se ter em conta a tradição liberal britânica e o Partido Conservador encabeçando Westminster no momento de produção do OSA. Além disso, a alteração de enfoque da nova lei (de conteúdos nocivos em geral para conteúdos nocivos a usuários vulneráveis, em especial) representa outro forte indicativo do potencial de sucesso do OSA neste ponto. Isso pois o controle mais rígido de matérias pontuais tende a ser menos polêmico do que seria tratar de forma rígida uma gama muito extensa de temas. Como consequência, menos entraves à consecução da lei devem ser criados.

Em vários momentos este trabalho recorreu à metáfora que contrasta o isolamento em bolhas de conteúdo, no ciberespaço, às trocas entre sujeitos de posicionamentos diversos na cidade democrática. À alegoria das cidades, somou-se a proposta teórica de Lehdonvirta (2022), a qual aponta no comportamento institucional das *bigtechs* a reprodução de

mecanismos próprios do Estado tradicional, em movimento por meio do qual plataformas se empoderam e se afastam da ingerência da Administração Pública. O encontro das duas ideias se mostrou particularmente sugestivo por seus atributos históricos e de antagonismo, presentes a todo tempo quando se pensa a atuação das grandes plataformas de serviços digitais na atualidade. Para que fique claro o cabimento dessa última afirmação, entende-se que recorrido histórico muito enxuto é aqui necessário.

A gênese dos centros urbanos modernos tem seu gérmen no ressurgimento das cidades comerciais medievais, ocorrida na Europa entre os séculos XI e XV (Pirenne, 1973). É o crescimento dos centros comerciais urbanos, onde "o ar da cidade liberta", que acaba por conduzir, pouco a pouco, à concentração das atividades administrativas junto a um governo uno, esvaziando a ingerência até então pulverizada dos feudos sobre seus territórios (Anderson, 1989). Esse movimento histórico consistiu em passo elementar para a constituição do que, hoje, entendemos por Estado moderno nacional, uma vez que foi a esse tempo que os processos de controle de exércitos, produção legislativa, territorialização, soberania, burocratização e nacionalismo foram paulatinamente se acumulando sob a égide de um único governo, já no período Moderno. A conformação dos Estados nacionais europeus, fruto dessa dinâmica histórica, representa evento cujas consequências são, até hoje, elementares para a organização das sociedades democráticas ocidentais. É somente após a consolidação do Estado nacional (ou do Estado burocrático racional, em termos weberianos) que se consolida o Estado social e democrático (Hobsbawm, 2004), e é nesse último que as trocas entre citadinos de orientações ideológicas diversas, aquelas aventadas por Sunstein ao se referir à cidade democrática, ocorrem. Isso posto, não é estranha a afirmação do autor de que a democracia, para se manter pulsante, demanda que seus cidadãos compartilhem experiências em comum e sejam defrontados por conteúdos que, se fosse depender de sua própria vontade, prefeririam não enfrentar (Sunstein, 2017). Isso pois valores em comum são elementos essenciais para a boa amarração de um grupo de indivíduos sob uma coalizão nacional propriamente dita. São justamente esses aspectos, elementares à sociedade democrática, que se depauperam no ciberespaço com a concentração dos sujeitos em bolhas de conteúdo, promovida pela ação de algoritmos.

É nesse ponto que o antagonismo da situação exsurge, e a metáfora que atravessa este trabalho desponta. A emulação de ferramentas de controle estatal pelas plataformas (a exemplo da determinação de condições para frequentar comunidades, o estabelecimento de regras para mercados de serviços, ou a fixação de mecanismos de identificação de usuários, listadas por

Lehdonvirta) não apenas serve para que essas tomem para si espaços de poder no mundo virtual, como também o faz através do estremecimento da ordem existente no mundo real. Em outros termos, é curioso como o agigantamento de poder de *bigtechs* no ciberespaço, mediante a imitação dos mesmos comportamentos institucionais estatais que possibilitaram a ascensão da cidade moderna, tem efeitos perniciosos sobre a mesma ordem democrática e citadina que parece inspirar a organização interna das plataformas. Os efeitos das ações de uma seara na outra (ou seja, os efeitos das ações no ciberespaço sobre o mundo real) estão no cerne da disputa política e por influência que hoje se opera entre os mais diversos agentes, notadamente Estados nacionais e grandes provedores de serviços de internet. Tem-se, aí, o grande pano de fundo deste trabalho e de quase qualquer outro que discuta regulação de plataformas na internet.

Como comentado ao fio desta dissertação, o OSA é consequência de tal fenômeno, e representa uma das mais vigorosas respostas de um Estado nacional para moderação de conteúdo ante o empoderamento de *bigtechs* até o momento – em ação de envergadura comparável, no Ocidente, ao Lei dos Mercados Digitais do bloco europeu[92] (Kira e Schertel Mendes, 2023) (The Cyberlaw Podcast, 2023). A morosidade e o cuidado com que se conduziu o processo legislativo se esforçou por observar, na medida do possível, a rapidez do fluxo de conteúdo *online* ao atribuir papel *quase* legislador ao OFCOM. Com isso, o Parlamento reconhece a demora natural da atividade legiferante por excelência e tende a facilitar os rearranjos regulatórios que vierem a se fazer necessários com a lei em funcionamento (em movimento regulador que observa, ao menos em alguma medida, a teoria do comunitarismo de rede de Andrew Murray[93]). Dita capacidade de adaptação do OSA o reveste de potencial promissor para, no decorrer dos anos - e caso o OFCOM tenha vigor de efetivamente implementar as previsões da nova lei -, colocar a autoridade estatal em paridade de forças para acomodar seus interesses com os interesses das empresas reguladas. Em vista do formato assumido pelo texto legal, e a despeito das reformas operadas no projeto original, é possível concluir que a lei, em boa medida, se aproxima das recomendações da literatura acadêmica que respalda este trabalho. À parte das dificuldades que devem advir com a produção legislativa secundária pelo OFCOM, o OSA tem o condão de atenuar os efeitos da tomada de espaço de Estados tradicionais por empresas de tecnologia.

[92] Para maiores detalhes, ver comentários em *The Cyberlaw Podcast.* Disponível em https://www.steptoe.com/podcasts/TheCyberlawPodcast-473.mp3. Último acesso 23/11/2023.
[93] O Professor Andrew Murray foi consultado pelo Parlamento durante a feitura da OSB, quando falou sobre fluxo de conteúdos e legitimidade regulatória. A transcrição da audiência pode ser lida através do link https://committees.parliament.uk/oralevidence/3032/pdf/. Último acesso em 23/10/2023.

A pesquisa e reflexões aqui empreendidas não necessariamente se encerram com este trabalho, e têm potencial para seguir diferentes rumos. O *Online Safety Act* representa marco significativo no processo de retomada de soberania no Reino Unido, consolidando desejos e estratégias outrora manifestados por intermédio da votação do Brexit (2016) e do *Global Britain in a Competitive Age* (Reino Unido, 2021). Em vista disso, analisar seu sucesso e processo de implementação junto ao OFCOM deve render valiosos insumos para a análise da relação política entre governos e a internet no Século XXI. É sabido que, no atual momento, países e blocos econômicos ao redor do mundo se esforçam por construir relações com as *bigtechs* e com as redes, de forma a manter sua soberania e valores nacionais também na era do ciberespaço. Essas ações, é também sabido, se dão especialmente mediante mecanismos de regulação. Nesse movimento, e não sem surpresa, cada Estado se volta a moldar a internet em seu território de modo condizente com suas orientações políticas e institucionais internas. A fim de ilustrar essa última afirmação, basta comparar as regulações de controle parcial propostas pelo Bloco Europeu com as rígidas regulações da internet impostas pela China. Ou, ainda, dentro de uma mesma unidade nacional, observar o quanto a internet proposta pelo Vale do Silício é livre e voltada às empresas, ao passo que a internet proposta por Washington DC é voltada à burocracia estatal. Em razão desse momento e da abordagem proposta pelo OSA, seria deveras interessante analisar, ao fio dos anos, o grau de sucesso do Reino Unido para construir, de fato, a sua própria internet: soberana, separada do bloco europeu, em consonância com os valores daquele Estado, e, quem sabe, "o lugar mais seguro do mundo para estar *online*".

Para além do cenário britânico, o trabalho aqui desenvolvido tem potencial de contribuir para análise comparada de diferentes processos regulatórios de moderação de conteúdo, em especial o caso brasileiro. De fato, o leque de possibilidades comparativas é amplo e não se restringe ao mero contraponto entre OSA, Marco Civil da internet (Brasil, 2014), e o PL 2630/2020 (Brasil, 2020). Mais do que o contraste entre os projetos regulatórios, chamam a atenção os paralelos traçáveis entre as relações entre os governos e as *bigtechs*. Em termos mais precisos, entre as determinações do Parlamento, por meio do OSA, e a atuação do Poder Público brasileiro no combate à circulação de materiais danosos por meios digitais. Se Estados mundo afora se esforçam por se adaptar e regular a vida em rede, a exemplo do caso britânico, qual é a atuação do Brasil frente a esse desafio global?

Bibliografia

1) Artigos, Livros, Periódicos e Reportagens:

ANDERSON, Perry. **Linhagens do Estado Absolutista**. 2a ed. São Paulo: Brasiliense, 1989.

BALKIN, Jack M. ***The future of free expression in a digital age***. Pepperdine Law Rev., v. 36, p. 427, 2009. Disponível: http://digitalcommons.law.yale.edu/fss_papers/223/. Último acesso em 23/03/2023.

BARLOW, John Perry: A ***Declaration of the Independence of Cyberspace***, February 1996. Disponível em https://www.eff.org/cyberspace-independence. Último acesso em 12/05/2023.

BARROS, J. D. "Cidade" e "Cultura" – considerações sobre uma relação complexa. Revista de História Regional, [S. l.], v. 16, n. 1, 2011. Disponível em: https://revistas.uepg.br/index.php/rhr/article/view/2399. Último acesso em 20/05/2023.

BERMAN, Paul Schiff. ***Cyberspace and the state action debate: the cultural value of applying constitutional norms to private regulation.*** University of Colorado Law Review, v. 71, p. 1263, 2000. Disponível: https://scholarship.law.gwu.edu/cgi/viewcontent.cgi?article=1083&context=faculty_publications

CATLEY, Henrietta. ***"The Online Safety Bill: a failure to regulate false information online"***. In Communications Law. : Bloomsbury Professional. Edição Peter Coe. Vol. 28 (1). Fevereiro de 2023. Disponível em https://www.bloomsburyprofessionalonline.com/view/journal_communications_law/CL-28_1.xml Último acesso 18/09/2023.

COE, Peter. ***The Draft Online Safety Bill and the regulation of hate speech: have we opened Pandora's box?*** Journal of Media Law, v. 14, número 1, p. 50-75. Junho de 2022. Disponível em http://pure-oai.bham.ac.uk/ws/portalfiles/portal/176875818/The_Draft_Online_Safety_Bill_and_the_regulation_of_hate_speech_have_we_opened_Pandora_s_box.pdf. Último acesso 03/07/2023.

COULTER, Chris; NEGISHI, Masayuki; FOSKETT, Elizabeth. ***UK Steps Toward "Digital Britain" with the Introduction of the Digital Economy Act 2010***. 2013. The Computer and Internet Lawyer. 27(9), p. 25-31.

Digital Economy Act 2010: summary of main provisions. Reino Unido. Thomson Reuters Practical Law. 2010. Disponível em https://uk.practicallaw.thomsonreuters.com/9-502-0116?transitionType=Default&contextData=(sc.Default)&firstPage=true#co_anchor_a1037147. Acesso em 21 de dezembro de 2023.

DELOUYA, Samantha. ***Montana governor bans TikTok***. CNN, maio. 2023. Disponível em https://edition.cnn.com/2023/05/17/tech/montana-governor-tiktok/index.html. Acesso em 20 de dezembro de 2023.

DOUEK, Evelyn. ***Content moderation as systems thinking***. Harvard Law Review, v. 136, p. 528, dezembro, 2022. Disponível em https://harvardlawreview.org/2022/12/content-moderation-as-systems-thinking/. Último acesso em 23/03/2023.

FARREL, Henry; LEVI, Margareth; O'REILLY, Tim. Mark Zuckerberg runs a nation-state, and he's the king. Vox Media. 10 de abril de 2018. Disponível em https://www.vox.com/the-big-idea/2018/4/9/17214752/zuckerberg-facebook-power-regulation-data-privacy-control-political-theory-data-breach-king. Acesso em 20 de dezembro de 2023.

FEINTUCK, Mike. ***3. Regulatory Rationales Beyond the Economic: In Search of the Public Interest***. In: *The Oxford Handbook of Regulation*. Edição por Robert Baldwin, Martin Cave, and Martin Lodge. Oxford: Oxford University Press, 2010. ISBN: 9780199560219

FEINTUCK, Mike; VARNEY, Mike. 4 ***The Regulatory Framework Before and After the Communications Act 2003***. In: *Media Regulation, Public Interest and the Law*, 126-168. Edinburgh: Edinburgh University Press, 2006.

FEINTUCK, Mike; VARNEY, Mike. 7 ***Conclusions: Protecting democratic values***. In: Media Regulation, Public Interest and the Law, 244-279. Edinburgh: Edinburgh University Press, 2006.

FILBY, M., ***The Digital Economy Act 2010: Is the DEA DOA***?. European Journal of Law and Technology, Vol. 2, No.2, 201. Disponível em https://ejlt.org/index.php/ejlt/article/view/58/153. Último acesso 07/06/2023.

FJELD, Jessica; BENSADON, Sol. ***One Law to Rule Them All: We're Skeptical of UN-sponsored Guidance for Content Regulation***. Medium Berkman Klein. Cambridge, Estados Unidos. 10 de abril de 2023. Disponível em https://medium.com/berkman-klein-center/one-law-to-rule-them-all-705e8c776e38. Último acesso 20/10/2023.

FOWLER-MASON, Esme. ***The Online Safety Bill needs more algorithmic accountability to make social media safe***. Medi@LSE Blog. 8 de fevereiro de 2023. Disponível em https://blogs.lse.ac.uk/medialse/2023/02/08/the-online-safety-bill-needs-more-algorithmic-accountability-to-make-social-media-safe/. Acesso em: 20 de dezembro de 2023.

GARSTKA, Krzysztof. T***he Amended Digital Economy Act 2010 as an Unsuccessful Attempt to Solve the Stand-Alone Complex of Online Piracy***. IIC International Review of Intellectual Property and Competition Law 43.2 (2012): 158–174. ISSN: 0018-9855

HARCUP, Tony. ***A Dictionary of Journalism.*** Oxford University Press, 2014. Disponível em https://www-oxfordreference-com.ezproxy-prd.bodleian.ox.ac.uk/view/10.1093/acref/9780199646241.001.0001/acref-9780199646241-e-968.

HOBSBAWM, Eric. **Nações e nacionalismo desde 1780: programa, mito e realidade**. Trad. Maria Celia PAOLI e Anna Maria QUIRINO. 4a ed. Rio de Janeiro: Nova Fronteira, 2004.

HUTCHINSON, Allan C. ***Some "What If" Thoughts: Notes on Donoghue v Stevenson***. York University. Osgoode Hall law journal (1960), 2014, Vol.51 (2), p.701-712. ISSN: 2817-5069

Internet Matters Organization: Resposta À Consulta Pública Dosb. Reino Unido. 2021. Disponivel em https://www.internetmatters.org/wp-content/uploads/2021/09/Internet-Matters-Response-to-Online-Safety-Bill-Sept-2021.pdf. Acesso em 21 de dezembro de 2023.

JENNINGS, Rafe. ***The Online Safety Bill Part 2: Do these proposals go too far, leading to overzealous policing?*** UK Human Rights Blog. 11 de setembro de 2021. Disponível em https://ukhumanrightsblog.com/2021/09/11/the-online-safety-bill-part-2-do-these-proposals-go-too-far-leading-to-overzealous-policing/. Acesso em 21 de dezembro de 2023.

KAFKA, Peter. ***Mark Zuckerberg wants you — and your government — to help him run Facebook.*** Media Vox. 31 de março de 2019. Disponível em https://www.vox.com/2019/3/31/18289375/mark-zuckerberg-facebook-regulation-washington-post-op-ed. Acesso em 20 de dezembro de 2023.

KIRA, Beatriz; SCHERTEL MENDES, Laura: ***A Primer on the UK Online Safety Act: Key aspects of the new law and its road to implementation****, VerfBlog,* 2023/11/13, https://verfassungsblog.de/a-primer-on-the-uk-online-safety-act/, DOI: 10.59704/2120f79b5f59e60b. Último acesso 12 de dezembro de 2023.

LEHDONVIRTA, Vili. ***Cloud Empires: How Digital Platforms Are Overtaking the State and How We Can Regain Control***. MIT Press. 2022. ISBN 9780262047227

LEISER, Mark; MURRAY, Andrew. ***The Role of Non-State Actors and Institutions in the Governance of New and Emerging Digital Technologies***', in Roger Brownsword, Eloise Scotford, and Karen Yeung (editores), The Oxford Handbook of Law, Regulation and Technology, Oxford Handbooks, 2017. Disponível em https://doi.org/10.1093/oxfordhb/9780199680832.013.28. Último acesso 19/05/2023.

LESSIG, Lawrence. ***The constitution of code: limitations on choice-based critiques of cyberspace regulation***. CommLaw Conspectus, v. 5, p. 181, 1997.

LESSIG, Lawrence. ***The law of the horse: What cyberlaw might teach***. Harvard Law Review, v. 113, n. 2, p. 501-549, 1999.

LESSIG, Lawrence. ***Reading the constitution in cyberspace***. Emory Law Journal, v. 45, p. 869, 1996.

LESSIG, Lawrence. ***Code: version 2.0***. New York: Basic Books, 2006.

LOMAS, Natasha. ***Germany accuses Twitter of failing to remove illegal hate speech***. TechCrunch. Boston, Estados Unidos. Abril, 2023. Disponível em https://techcrunch.com/2023/04/04/twitter-netzdg-germany/?guccounter=1. Acesso em 20 de dezembro de 2023.

MARQUES, José. ***Moraes autoriza inquérito para investigar dirigentes de Google e Telegram***. Folha de São Paulo. São Paulo, Brasil. 12 de maio de 2023. Disponível em https://www1.folha.uol.com.br/poder/2023/05/moraes-autoriza-inquerito-da-pgr-sobre-dirigentes-de-google-e-telegram.shtml. Acesso em 20 de dezembro de 2023.

MARTINS HARTMANN, I. A.; SARLET, I. W. Direitos fundamentais e direito privado: a proteção da liberdade de expressão nas mídias sociais. **Direito Público**, *[S. l.]*, v. 16, n. 90, 2019. Disponível em: https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/3755. Último acesso 05/10/2023.

MELLO, Patrícia Campos. **"Não basta regular, é preciso ter infraestrutura digital pública"**. Entrevista com Evgeny Morozov. Folha de São Paulo. Agosto de 2023. Disponível em https://www1.folha.uol.com.br/tec/2023/08/nao-basta-regular-e-preciso-ter-infraestrutura-digital-publica-diz-especialista.shtml. Acesso em 20 de dezembro de 2023.

MENDIS, Dinusha. ***Digital Economy Act 2010: fighting a losing battle? Why the 'three strikes' law is not the answer to copyright law's latest challenge***. International Review of Law, Computers & Technology, 2013. Vol. 27, Nos. 1–2, 60–84, http://dx.doi.org/10.1080/13600869.2013.764137.

MORGANELLI, Marie. ***What is Systems Thinking?*** Southern New Hampshire University. 18 de março de 2020. Disponível em https://www.snhu.edu/about-us/newsroom/business/what-is-systems-thinking. Acesso em 20 de dezembro de 2023.

MURRAY, Andrew D. ***Nodes and gravity in virtual space***. Legisprudence: International Journal for the Study of Legislation, Hart Pub., v. 5, n. 2, out./2015, p. 195-221.

NAUGHTON, John. ***Who needs a government when you've got Amazon to keep things running?*** The Guardian. 28 de março de 2020. Disponível em https://www.theguardian.com/commentisfree/2020/mar/28/who-needs-crisis-government-when-youve-got-amazon-coronavirus. Acesso em 20 de dezembro de 2023.

NEUDERT, Lisa Maria. ***Regulatory capacity capture: The United Kingdom's online safety regime***. Internet Policy Review, 12(4). 2023. Disponível em https://doi.org/10.14763/2023.4.1730. Acesso em 20 de dezembro de 2023.

ONLINE SAFETY BILL EXPLANATORY NOTES. London: [Dandy Booksellers Ltd], 2022. Print.

OXFORD DICTIONARY OF LAW. 8a Edição. Oxford, Reino Unido. Oxford University Press, 2015.

PIRENNE, Henri. **As Cidades na Idade Média**. Tradução de Carlos Montenegro Miguel. Lisboa: Publicações Europa- América 1973.

REIDENBERG, Joel R. ***Lex informatica: The formulation of information policy rules through technology***. Texas Law Review, v. 76, p. 553, 1997.

ROWBOTTOM, Jacob. ***Democracy Distorted: Wealth, Influence and Democratic Politics.*** Cambridge United Kingdom: Cambridge Press, 2010. DOI 10.1017/CBO9780511844805.

SCHLESINGER, Philip. ***The neo-regulation of internet platforms in the United Kingdom***. Policy & Internet, 14, 47– 62, 2022. Disponível em https://doi.org/10.1002/poi3.288 . Último acesso 24/05/2023.

SIQUEIRA, Carol***. Lira defende responsabilização das 'bigtechs' por ofensiva contra o PL das Fake News***. Agência Câmara de Notícias. 2 de maio de 2023. Disponível em https://www.camara.leg.br/noticias/957860-lira-defende-responsabilizacao-das-big-techs-por-ofensiva-contra-o-pl-das-fake-news/. Acesso em 20 de dezembro de 2023.

SUNSTEIN, Cass R. ***#Republic: Divided Democracy in the Age of Social Media***. Princeton, NJ: Princeton University Press, 2017. ISBN 9781400884711 1400884713

SUZOR, Nicolas. ***Digital Constitutionalism: Using the Rule of Law to Evaluate the Legitimacy of Governance by Platforms***. Social Media + Society, 4(3). Sage Journals. Julho de 2018. Disponível em https://doi.org/10.1177/2056305118787812. Acesso em 20 de dezembro de 2023.

THE REDMOND DOCTRINE: Lessons from Microsoft's corporate foreign policy. The Economist. 2019. https://www.economist.com/business/2019/09/12/the-redmond-doctrine. Acesso em 20 de dezembro de 2023.

THURMAN, Neil.; OBSTER, Fabian. ***The regulation of internet pornography: What a survey of under-18s tells us about the necessity for and potential efficacy of emerging legislative approaches***. Policy Internet, 13, 2021, pags. 415– 432. https://doi.org/10.1002/poi3.250

VIKHORNOVA, Anastasia. ***What we can learn from the history of Systems Thinking***. Medium Journal. 17 de Agosto de 2018. Disponível em https://medium.com/systems-thinking-for-non-systems-thinkers/what-we-can-learn-from-the-history-of-systems-thinking-79852d8955c4. Acesso em 20 de dezembro de 2023.

WEBER, Max. **Economia e Sociedade: Fundamentos da sociologia compreensiva. 2. Vol**. Trad. Regis Barbosa e Karen Elsabe Barbosa São Paulo: Editora UnB, Imprensa Oficial, 2004.

WOODS, Lorna. ***The Duty of Care in the Online Harms White Paper***. The Journal of Media Law 11, pags. 6-17, 2019.

WOODS, Lorna. ***The Carnegie Statutory Duty of Care and Fundamental Freedoms***. Carnegie UK Trust. Dezembro de 2019. Disponível em https://d1ssu070pg2v9i.cloudfront.net/pex/pex_carnegie2021/2019/12/05125454/The-Carnegie-Statutory-Duty-of-Care-and-Fundamental-Freedoms.pdf . Último acesso 19/09/2023.

WOODS, Lorna; BAYER, Judit; HOLZNAGEL, Bernd; KORPISAARI, Päivi. ***Perspectives on Platform Regulation Concepts and Models of Social Media Governance Across the Globe.*** Judit Bayer, Bernd Holznagel, Päivi Korpisaari, Lorna Woods (eds.) 601 pp. 1. ed. Baden Baden: Nomos Verlagsgesellschaft mbH & Co. KG, 2021. v. 1. P. 77-97. ISBN 978-3-7489-2978-9.

2) <u>Podcasts</u>

THE CYBERLAWPODCAST. ***Episode 473: The UK adopts na Online Safety Bill that allows regulation of Ecrypted Messaging. Podcast***. 25 de setembro de 2023. Disponível em: https://www.steptoe.com/podcasts/TheCyberlawPodcast-473.mp3. Último acesso 11 de dezembro de 2023.

3) <u>Documentos Oficiais</u>

BRASIL. Câmara dos Deputados. **Projeto de Lei n. 2630/20**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. 2020. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1909983 . Acesso em 21 de dezembro de 2023.

BRASIL. **Lei 12.965**, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 21 de dezembro de 2023.

BRASIL. **Ministério Público Federal**. Procuradoria da República do Estado de São Paulo. Procuradoria Regional dos Direitos dos Cidadãos. Inquérito Civil Público nº 1.34.001.009969/2021-35. Yuri Correa da Luz. 01 de maio de 2023. Disponível em https://internetlab.org.br/wp-content/uploads/2023/05/mpf-manda-google-meta-explicarem.pdf. Acesso em 20 de dezembro de 2023.

BRASIL. **Supremo Tribunal Federal**. Decisão sob sigilo no Inquérito 4781/DF. Ministro Alexandre de Morais. 2 de maio de 2023. Disponível em https://internetlab.org.br/wp-content/uploads/2023/05/Decisao.pdf. Acesso em 20 de dezembro de 2023.

REINO UNIDO. *Act of Parliament.* ***Communications Act 2003***. 2003. Disponível em https://www.ofcom.org.uk/__data/assets/pdf_file/0022/229045/Annex-4-Communications-Act-2003-c-21-downloaded-April-2021.pdf. Último acesso 05/06/2023.

REINO UNIDO. *Act of Parliament.* ***Digital Economy Act 2010***. 2010. Disponível em https://www.legislation.gov.uk/ukpga/2010/24/contents. Último acesso 07/06/2023.

REINO UNIDO. *Act of Parliament*. **Digital Economy Act 2017**. 2017. Disponível em https://www.legislation.gov.uk/ukpga/2017/30/contents/enacted. Último acesso 26/06/2023.

REINO UNIDO. *Cabinet Office (CO).* ***Global Britain in a competitive age: The integrated review of security, defence, development and foreign policy***. Março 2021. Disponível em https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy. Último acesso 29/06/2023.

REINO UNIDO. *Department for Digital, Culture, Media and Sport (DCMS)*. ***Internet Safety Strategy Green Paper.*** Outubro, 2017a. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf. Último acesso 26/06/2023.

REINO UNIDO. *Department for Digital, Culture, Media and Sport (DCMS)*. ***Government Response to the Internet Safety Strategy Green Paper.*** Maio, 2018. Disponível em

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/708873/Government_Response_to_the_Internet_Safety_Strategy_Green_Paper_-_Final.pdf. Último acesso 26/06/2023.

REINO UNIDO. *Department for Digital, Culture, Media and Sport (DCMS)*. ***Disinformation and 'Fake News': Interim Report.*** Julho, 2018a. Disponível em https://web.archive.org/web/20181126165156/https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/363/363.pdf. Último acesso 23/06/2023.

REINO UNIDO. *Department for Digital, Culture, Media and Sport (DCMS)*. ***Online Harms White Paper***. Abril, 2019. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf. Último acesso 26/06/2023.

REINO UNIDO. *Department for Digital, Culture, Media and Sport (DCMS)*. ***Online Harms White Paper: Full Government Response to the consultation***. Dezembro, 2020. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf. Último acesso 07/07/2023.

REINO UNIDO. *Department for Digital, Culture, Media and Sport (DCMS)*. ***Draft Online Safety Bill***. Maio, 2021a. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf. Último acesso 07/07/2023.

REINO UNIDO. *Department for Digital, Culture, Media and Sport (DCMS)*. ***Online Safety Bill Explanatory Notes***. Maio, 2021b. Disponível em https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985031/Explanatory_Notes_Accessible.pdf. Último acesso 07/07/2023.

REINO UNIDO. *Health and Safety at Work etc Act 1974*. Londres, 1974. Disponível em https://www.hse.gov.uk/legislation/hswa.htm. Acesso em 20 de dezembro de 2023.

REINO UNIDO. HM Government. ***Agile nations charter***. 25 de novembro de 2020. Disponível em: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/942312/Agile_Nations_Charter.pdf. Acesso em 21 de dezembro de 2023.

REINO UNIDO. *House of Lords (HL)*. ***Communications and Digital Committee. Corrected oral evidence with Andrew Murray***. Novembro 2021c. Disponível em https://committees.parliament.uk/oralevidence/3032/pdf/. Último acesso em 23/10/2023.

REINO UNIDO. *House of Lords (HL)*. ***Online Safety Bill***. *Bill 164*. Julho de 2023. Disponível em https://bills.parliament.uk/publications/52368/documents/3841. Último acesso 15/08/2023.

REINO UNIDO. ***The Online Pornography (Commercial Basis) Regulations***. 2019a. Disponível em https://www.legislation.gov.uk/uksi/2019/23/contents/made. Acesso em 21 de dezembro de 2023.