Soberania digital no século XXI: considerações brasileiras a partir do novo conceito de ciberespaço

Luiz Fernando Horta
Pós-Doutorado, University of Denver (DU), Denver, Colorado, Estados Unidos.
Professor, Universidade de Brasília (UnB), Brasília, Brasil.
http://lattes.cnpq.br/0589727185579085
moonbladers@gmail.com

Andre Ricardo Nogueira
Doutorado em Ciência Política, Universidade de São Paulo (USP), São Paulo, Brasil.
Professor, Universidade Federal do Espírito Santo (UFES), Vitória, Espírito Santo, Brasil.
http://lattes.cnpq.br/0589727185579085
andrericardonogueira@gmail.com

Submetido em: 30/08/2023. Aprovado em: 04/02/2025. Publicado em: dd/mm/yyyy.

RESUMO

As transformações digitais são características já do século XXI. A velocidade das mudanças que as novas tecnologias fazem acontecer acaba deixando para trás a capacidade de transformação do próprio Estado. Criar leis, pensar sistemas de proteção à democracia, aos cidadãos e aos bens públicos é um processo mais lento do que os investimentos em ciência e tecnologia de diversas empresas. O resultado é uma tentativa de resposta rápida por parte do Estado que tem sido globalmente insuficiente tanto para assegurar direitos como para conter processos de exploração. Uma das alternativas mais utilizadas para diminuir a diferença entre as transformações e os espaços de controle do Estado tem sido a analogia entre o material e o digital. Assim, toda a legislação que por séculos foi sendo aperfeiçoada para conter os abusos de agentes econômicos sobre o tecido da sociedade se converte do mundo material para o mundo digital. Porém, esta conversão tem se mostrado errônea e insuficiente. O artigo analisa os efeitos da analogia digital do conceito de “soberania” e faz uma comparação entre as propostas norte-americanas e brasileiras em algumas áreas-chave do desenvolvimento de legislação sobre o mundo digital. A conclusão é que o Brasil está não apenas atrasado no desenvolvimento destas tecnologias, mas também na forma como o Estado tenta afirmar os direitos de seus cidadãos e proteger os bens públicos. No fundo, o digital é mais complexo do que a analogia com o material faz supor.

Palavras-chave: soberania digital; ciberespaço; transformações digitais; inteligência artificial; controle do estado.

A IDEIA DE SOBERANIA

A soberania é um conceito fundamental para a contemporaneidade. É condição essencial para a existência de um país o fato deste ter "soberania". O termo vem do latim "superanus" e refere àquele que tem o poder supremo. Exercer "soberania" sobre um território é definir seus rumos "em última instância". O conceito de soberania tem sido atacado desde o final do século XX. A geopolítica, com o surgimento de atores internacionais diversos, a consolidação de instituições internacionais e a cristalização de um rol de direitos humanos, tornaram o termo "soberania" poroso, no mínimo. Tornou-se, em essência, relativo às capacidades reais do exercício dos poderes de um Estado. Neste texto, abordarei o sentido de soberania digital e como se relaciona com o conceito de espaço digital, no século XXI. Jean Bodin (2009) define soberania como "[…] the right to impose laws generally on all subjects regardless of their consent" (Bodin, 2009, p. 33). Ele reconhece ainda que soberania não se confunde apenas com as "leis", na medida que o francês ainda pensava a partir das chaves seiscentistas de interpretação do mundo. Os homens, segundo Bodin, estão submetidos primeiramente à "lei de Deus" e é dela que emana toda existência da ideia de soberania.

Neste sentido, Bodin afirma que a soberania humana não é absoluta, mas tem fonte na religião "verdadeira", que é capaz de interpretar a vontade de Deus.

> If we insist however that absolute power means exemption from all law whatsoever, there is no prince in the world who can be regarded as sovereign, since all the princess of the earth are subject to the laws of God and of nature, and even to certain human laws common to all nations (Bodin, 2009, p. 27-28).

Enquanto para Bodin soberania é algo que emana do divino para o soberano, é Hobbes quem estabelece soberania como humana e circunscrita a um território. Território em que, segundo o autor, um contrato social opera no sentido de conferir a um poder central a possibilidade de regular o comportamento humano. Em "O Leviatã", Hobbes define soberania como "absoluta"[1] e indivisa. Ela precisa ser plena para poder sobrepujar o Estado de Natureza, e será restrita apenas pelas fronteiras do território a que está ligada.

Kant, em "A paz perpétua" segue o caminho de afrouxamento do conceito. Se com Bodin ele é pleno e divino, e com Hobbes é fruto de um contrato cuja consecução independe das vontades dos contratantes tomadas a todo tempo (funcionando como um pacto tácito), com Kant soberania dependia fundamentalmente da racionalidade dos cidadãos que compreendiam as vontades de cooperação para organização de um Estado. Os limites da ideia de soberania em Kant não estão mais apenas na delimitação geográfica (fronteira),

1 Na argumentação de Hobbes, já que não faz sentido pensar em soberania submetida a algum outro poder que lhe é entendido como superior. O poder divino, que fazia parte da conceituação de Bodin, deixa de existir. Hobbes muda a natureza e a fonte da soberania de Bodin. Ao entendê-la como humana, a fonte da soberania deveria vir do povo que buscava proteção e segurança.
"For by art is created that great Leviathan called a Commonwealth, or State (in Latin, Civitas), which is but an artificial man, though of greater stature and strength than the natural, for whose protection and defence it was intended; and in which the sovereignty is an artificial soul, as giving life and motion to the whole body; the magistrates and other officers of judicature and execution, artificial joints; reward and punishment […]" (Hobbes, 1651, p. 7).

mas também no respeito aos direitos e na promoção da autonomia da moral individual[2]. O sentido de soberania operava não mais como um pacto tácito, mas como ação conjunta condicional, que obedecia tanto à racionalidade dos sujeitos, quanto aos seus projetos morais, e seria tanto mais atraente aos pactuantes quanto mais demonstrasse respeito às limitações impostas pela cognição de cada indivíduo.

O caminho que o conceito de soberania percorre, do século XVI até hoje, reflete uma dupla adequação. Em primeiro lugar, a soberania passa de uma característica divina interpretada por um indivíduo (o soberano) para ser parte da institucionalidade do Estado. Estando à disposição do indivíduo apenas pela ligação que este tem com o Estado, e não como forma originária divina ou tácita. A formação destes Estados Modernos, nos termos de Anderson (1995), acaba impessoalizando a noção de soberania que, por volta do século XVIII, já estava completamente submetida ao conceito de Estado. Soberania não mais era exercida por alguém, mas de forma institucional, estava submersa nas capacidades e necessidades da própria ideia de Estado.

Por outro lado, a ideia de soberania precisou adequar-se à relação econômico-produtiva da contemporaneidade. Se, entre os séculos XVI e XVIII, a soberania estava restrita pelas fronteiras do Estado que a exercia, o capitalismo do século XIX e XX construiu uma noção de soberania que se desprende do espaço físico ocupado pelos Estados, circunscrita às suas fronteiras físicas. Bens, capital, pessoas, entre outros recursos econômicos, carregam um signo distintivo de sua origem que aponta sua submissão a uma autoridade estatal primordial, independente do território em que estes recursos se encontrem eventualmente. A noção de “propriedade privada” transpassa o sentido de soberania e, se não se pode dizer que a soberania é sempre plena sobre as propriedades privadas, tampouco se pode assumir que a propriedade privada está livre das disputas de soberania.

Aqui surgem leis, princípios, regras e dispositivos legais – consensuais ou não – que visam dirimir os conflitos entre soberania e propriedade privada. Soberania deixa de estar restrita às fronteiras físicas de um determinado Estado, e passa a ser reconhecida como parte integrante de um poder difuso sobre as coisas no mundo. O capital ganha o direito à “livre circulação”, por exemplo, e não mais está subordinado ao seu local original. Mercadorias ganham direitos de proteção de sua integridade material e, também, de sua privacidade.

No século XX, o termo soberania (e a sua aplicabilidade prática) se vê complexo, eis que não existe mais soberania plena ou absoluta. Por outro lado, se compartilhada, segundo Bodin e Hobbes, então parece não haver soberania possível sem alguma contradição lógica.

Para solucionar tais contradições, o Direito costuma separar a soberania em áreas de exercício. Estabelece como soberania sobre algo o conjunto de regras, costumes e

2 “As formas de um Estado (civitas) podem ser divididas ou de acordo com a distinção das pessoas que possuem o poder supremo do Estado internamente ou de acordo com o modo de governo do povo por seu chefe supremo, independentemente de quem este possa ser; a primeira se denomina propriamente a forma da soberania (forma imperii) e há apenas três maneiras possíveis, a saber, onde ou apenas um, ou alguns ligados entre si ou todos, que constituem juntos a sociedade civil, possuem o poder soberano (autocracia, aristocracia e democracia, o poder do príncipe, o poder da nobreza e o poder do povo) [...] – e, no entanto, visto que a razão, de cima do trono do supremo poder legislativo moral, condena absolutamente a guerra como via de direito e torna em contrapartida o estado de paz um dever imediato” (Kant, 2020, p. 13-18).

ações políticas emanadas por um Estado que tem por função quatro espaços de ação: (1) administrar Justiça, (2) proteger fronteiras (território, corpo ou valor), (3) organizar a produção econômica (regras, condições e interditos) e (4) cobrar impostos (de formação, de transação ou de passagem).

Contemporaneamente, admite-se soberano um Estado que esteja na condição legal (soberania de jure) e na efetiva possibilidade (soberania de facto) de realizar estas quatro tarefas sobre um espaço físico, sobre o capital, mercadoria ou pessoa a que se esteja referindo. A soberania implica, pois, no exercício monopolístico das decisões finais sobre essas quatro áreas político-econômicas, e se admite sua existência parcial, em relação ao tempo ou espaço[3].

De um sentido restrito ao território físico (a soberania em Bodin e Hobbes), termo foi adquirindo a maleabilidade necessária para atender aos interesses do capitalismo contemporâneo. Da noção encerrada no referente físico (Estado e fronteiras), o sentido se translada para uma soberania por origem, determinada pela propriedade no tempo da criação da mercadoria, do capital, ou do nascimento do indivíduo (como ato formador do pacto social) submetidos aos interesses de um Estado[4].

> Now, the contemporary crisis of the concept of sovereignty relies precisely on the progressive dissolution of its seemingly pacific relationship with borders. As a matter of fact, such a crisis is determined by factors such as the globalization of the flows of goods and information; it is actively produced by the mobility rights achieved by men and women, and yet contrasted, filtered, slowed down or accelerated by both formal and informal devices of global governance (Chignola, 2021, p. 2).

Soberania digital no século XXI

O século XXI tem como característica o surgimento de um espaço não físico em que operam os interesses humanos, de Estado e do capital em velocidades e valores crescentes (Bratton, 2016). O mundo digital surge como um paradoxo: é um espaço não-material que se constitui de não materialidades (informações, noções, ideias, sentidos), codificadas de forma binária em algum lugar, e que modifica substancialmente toda a materialidade do planeta.

3 É da leitura dos trabalhos de Carl Schmidt que surgem essas referências. Schmidt assume soberania como indiscutivelmente ligada à noção de "fronteira" e que, de forma prática, o conceito é aderente "[...] ao interesse público, ou ao interesse de Estado, à segurança pública e ordem" (Schmidt, 2005, p. 5, tradução nossa).
Original: "[...] the public interest or interest of the state, public safety and order, le salut public, and so on" (Schmidt, 2005, p. 5).
"[...] ou ao governo controlado pelo espírito do comercialismo[...]" (Schmidt, 2005, p. 10, tradução nossa).
Original: "[...] a self-governing body controlled by the spirit of commercialism [...]" (Schmidt, 2005, p. 10).

4 Uma parte desta problemática da discussão sobre soberania no século XXI surge das diferenças de sentido entre os termos utilizados "dominium" e "imperium". Enquanto o primeiro enseja posse e está organizado a partir dos sentidos do mundo material, o segundo estabelece autoridade, e é muito mais afeita às condições do mundo não material.
"In the years preceding its Hobbesian theoretical definition, then, the concept of sovereignty appears to be deeply influenced by global perspectives, tensions and problems. The Empire and the State constantly mirror each other on a juridical threshold that represents the trigger of the modern conceptual device. This happens precisely through a continuous exchange between the logic of 'imperium' and the logic of 'dominium' that resignifies legal practices and lexicons as well as the categories and exempla taken from ancient historiography" (Chignola, 2021, p. 9-10).

> Convinced by the demise of the Cold War and the magic of a new technology, people accepted the view that history as we once knew it was ending and that, along with the end of politics as we once knew it, there would be an end to the laws propagated by that most dismal of sciences, economics. Constraints once imposed by scarcities of resources, labor, and capital would end, or at least loosen significantly, and a new economics of cyberspace (a "network economics") would make it easier for societies to grow and, especially, to grow rich (Mosco, 2004, p. 16).

O mesmo caminho de acomodação epistemológica que o conceito de soberania trilhou (da noção dura de espaço para a noção mais sutil de tempo e propriedade) com o objetivo de ser usado como condição definidora de um Estado, pode ser percebido quando se entende o caminho histórico do conceito de "espaço digital" (ciberespaço[5]).

O termo "digital" vem como referência ao mundo construído em linguagem de máquina, cuja informação era criada, manipulada, controlada, ou modificada a partir da alteração apenas de dois dígitos (0 e 1, no sistema binário, usado como base de programação). De início incompreensível a todos e todas, o mundo digital passou a ser significado, para a maioria da população, através de uma analogia com o espaço físico.

Assim, da mesma forma que existia um espaço físico em que vivíamos e convivíamos (operado pelos sentidos do tato, olfato, audição, etc.), o mundo digital foi visto como um "espaço" não-material que existia a partir de um código ou referência digital[6]. Estabeleceu-se uma percepção inicial de que o ciberespaço só existiria por causa de um determinado conjunto de informações que necessitava uma ligação com o material (servidor armazenador).

Esta analogia operou, desde 1960, uma dupla função. Por um lado, permitiu a compreensão do que seria esse "mundo digital", de forma que os seres humanos, que são carregados pelas suas experiências sensórias e as têm como determinantes de realidade[7], puderam compreender (construir, pensar, discutir e comunicar) o mundo digital a partir da analogia com os seus referenciais e experiências físicas. Por outro lado, a definição do digital como um "espaço físico não material" deu condições para a adequação de toda reflexão historicamente construída sobre política, legislação e direitos (que havia sido criada para controlar espaços materiais) a essa nova realidade. Compreender o digital como "espaço" (territorial) permitiu que se adequassem as antigas funções de Estado ao novo domínio não material que surgia.

Nesse sentido, o pensamento liberal operou a construção de sentidos com respeito ao mundo digital, a partir da noção de soberania. Se um Estado somente é soberano se puder exercer as quatro ações (mencionadas antes nesse texto) sobre o território, então

5 O primeiro uso da palavra "ciberespaço" aparece no romance de William Gibson, "Neuromancer" de 1984: "Os japoneses já haviam esquecido mais neurocirurgia que os chineses jamais haviam aprendido. As clínicas negras de Chiba eram de ponta, escolas inteiras de conhecimento técnico suplantado mês a mês, e mesmo assim não conseguiram reparar o estrago que ele havia sofrido naquele hotel em Memphis. Um ano ali e ele ainda sonhava com o ciberespaço, a esperança morrendo um pouco a cada noite. Todo o speed que tomou, todas as voltas que deu e as esquinas de Night City por onde passou, e ainda assim ele via a matrix em seu sono, grades brilhantes de lógica se desdobrando sobre aquele vácuo sem cor [...]" (Gibson, 1984, p. 15).

6 Opto por não usar a dicotomia mundo digital vs. mundo real por entender que o digital é também real. Ao longo do artigo será usada a dicotomia mundo físico vs. mundo digital.

7 É verdade que a humanidade sempre esteve às voltas com um mundo "ideal" que operava primordialmente fora da materialidade. Contudo, a primazia da materialidade sobre a filosofia a partir do século XIX, relegou o não material a um espaço menor do que ele já ocupara na vida das pessoas nos séculos anteriores.

a soberania digital, tomada a partir da analogia com o espaço físico, afirmava que ser soberano no mundo digital é poder (1) penalizar, imputar culpa ou determinar inocência de sujeitos que operem no mundo digital, (2) criar, modificar e impor regras para o acesso, (3) determinar limites e condições à criação e/ou distribuição do valor econômico gerado pelo espaço digital e (4) cobrar impostos pela administração deste novo espaço. Por óbvio, as mesmas instituições históricas que se impuseram funcionalmente sobre o espaço material do Estado também foram as primeiras que requisitaram a legitimidade para estabelecer o mesmo tipo de relação de dominação para com o espaço digital.

O Estado se arrogou o direito de controle sobre esse "novo mundo"[8], como decorrência necessária da existência histórica prévia de seus direitos e poderes construídos e organizados para operar no mundo material. O digital, portanto, foi visto como um apêndice espelhado do mundo material, e sobre esse novo espaço deveria se aplicar, por analogia, as instituições e regras existentes já no mundo material.

Houve, assim, uma adaptação do rol de direitos e deveres existentes no mundo material para o espaço digital, seguindo, em linhas gerais, a mesma analogia original que explicava o digital como um "espaço físico não-material". A percepção liberal encroada no pensamento do século XX (*embedded liberalism*) assumiu o controle sobre o mundo digital a partir das noções de privacidade, liberdade e geração de valor econômico. Esta analogia, que, se teve o mérito histórico de permitir uma compreensão funcional do espaço digital (pelo menos até os anos 80 do século passado), provocou também uma espécie de prisão na compreensão do ciberespaço e capturou suas potencialidades e especificidades.

Dizendo de outra forma, pensar o espaço digital como analogia do físico implica em transpor as categorias sócio-históricas com que o Estado controla o espaço físico para o controle do mundo digital. E essa operação é mais complexa e menos efetiva do que o senso comum aceita ser.

Assim, na atual interpretação, um espaço digital precisa estar ancorado ao espaço geográfico (território) para que as ferramentas de controle do Estado possam operar com mínima eficácia. O direito de "ir e vir", consagrado a partir do século XVIII como um direito humano, foi – por analogia – a base da ideia de "liberdade" no mundo digital. O direito à privacidade e à intangibilidade do corpo humano operou o mesmo movimento de analogia para se tornar a "privacidade digital", e as noções de propriedade capitalista (material ou intelectual) foram a centrais para os controles fiscais e tributários estabelecidos sobre o mundo digital ao longo das décadas de 1980, 1990 e 2000.

Não é como se tivéssemos criado um conjunto normativo novo e adequado ao mundo "físico não-material" (digital). Operou-se uma transição por analogia dos conjuntos de entendimentos anteriores (sociais, políticos e econômicos) e a operacionalização dos

8 Se historicamente é possível dizer que o Estado é o produto acabado das disputas políticas entre as diversas formas de organização social tentadas ao longo do tempo, este é ainda um processo em desenvolvimento no mundo digital. Os Estados não conseguiram ainda se assenhorear e controlar o digital e normalmente só conseguem controle sobre este a partir da correlação da punição e controle sobre os supostos detentores de benefícios econômicos advindos do digital. Não se tem como controlar o digital senão pela ameaça de punição a determinados sujeitos (suas posses ou ganhos) no mundo material.

regramentos (leis) que historicamente tinham sido estabelecidos para o mundo material. E isso com uma dose de autoritarismo das nações que estavam em condição de primeiro estabelecer marcos de controle e governança sobre o mundo digital (EUA e países europeus).

A visão liberal do Estado, suas funções, ferramentas e obrigações foram, a certo modo, uma redução cognitiva para a compreensão do mundo digital. Através dessa analogia imprecisa, os direitos e garantias do cidadão no mundo físico foram transpostas para o espaço digital com pouca ou nenhuma adequação ao que realmente era a essência do novo espaço digital. O direito à privacidade, por exemplo, que toma forma a partir do século XVIII numa proteção ao indivíduo contra os abusos do Estado, se tornou, na analogia para o mundo digital, uma proteção tão somente aos "dados" daquele que opera nos espaços digitais. A analogia opera aqui com ênfase na redução do indivíduo a dados para a proteção contra o autoritarismo do Estado. Protege-se o dado imaginando (por analogia) proteger o indivíduo.

Essa relação, contudo, acaba dando mais margem a problemas de entendimento do que consegue encaminhar soluções aos questionamentos contemporâneos. Não entro aqui nas distinções legais entre "segredo" e "sigilo"[9], por exemplo, que já seria um ponto a se pensar quando se trata do mundo digital, mas, e ainda mais simples, é possível perguntar o que devemos exatamente proteger no ciberespaço?

A resposta a essa pergunta, até agora, é também obtida pelo retorno da analogia que faz entender o digital. Os dados que se pretende proteger são aqueles que permitem o usuário ser localizado, identificado ou distinguido no mundo físico. Ora, fala-se, portanto, dos endereçamentos de entrada na rede (IP – Internet Protocol) que vêm associados, na estação servidor, às informações que distinguem o usuário no mundo material. O mundo digital, nesse sentido, é percebido apenas como tendo existência/ação acessória, tributário e restrito à sua contraparte material. Recentemente, ainda sem positivação legal adequada, inseriu-se no conjunto de dados "protegidos" os históricos de passagens dos usuários nas redes[10]. Contudo, ainda há uma enorme lacuna de proteção do indivíduo[11], que, de um lado, é apropriada comercialmente pelas "*Big Tech*" e, por outro, serve de porta ataque às democracias contemporâneas.

Neste lusco-fusco sobre a compreensão do mundo digital – a partir do século XXI – várias empresas passaram a entender o indivíduo imerso no mundo digital não como uma pessoa física que atua por meio específico (digital), mas como um "cidadão digital". Há a percepção consciente de que as analogias anteriores não são mais funcionalmente válidas. Tomar o digital como um espelho do material não é mais sustentável.

9 Segredo opera uma ordem daquilo que deve estar escondido do escrutínio público por condição de si, enquanto sigilo se estabelece o mesmo sentido a partir de condições conjunturais. Enquanto segredo é condição de formação daquilo que se está protegendo, o sigilo é uma relação entre necessidade e possibilidade imposta a alguns grupos de interesses sociais, políticos e/ou econômicos.

10 Aqui são reveladores os depoimentos de Peiter Zatko sobre o *Twitter* ao Comitê Judiciário do Senado norte-americano do dia 13/09/2022 (U.S. *Senate committee on the judiciary*, 2022) e de Eugene Zarashaw sobre como e onde o Facebook trata os dados pessoais dos usuários (Biddle, 2022).

11 Aqui, cabe chamar a atenção do leitor para a diferença entre a noção do digital como espelhamento do mundo material e, aí, o indivíduo digital seria uma imagem do indivíduo material, e a noção do digital como autônomo para um indivíduo digital que existe indiferente, distante ou mesmo em oposição à existência material.

Nesse sentido, as noções de privacidade e de liberdade também tiveram que ser atualizadas. Enquanto o Estado permanecia analógico, as empresas de tecnologia passaram a operar segundo a percepção da existência de um "ser digital". A proteção aos dados de origem do usuário (que era o centro da legislação até o final do século XX) ficou sem sentido nos modelos de negócios atuais do *Google* e *YouTube* (Zuboff, 2019) que, por exemplo, passou a reter, estudar e vender os dados da passagem do cidadão no mundo digital (escolhas, pesquisas, buscas, compras, históricos entre outras). Não era mais uma preocupação os dados de origem (aqueles que identificam o usuário no mundo físico), mas as escolhas, preferências e manifestações coletadas individual e anonimamente, e tratadas por meio estatístico, compondo um "indivíduo digital tipificado" que era apropriado por modelos digitais e psicológicos para gerar conhecimento.

O mundo digital se descolava do mundo físico. A partir da consolidação do indivíduo dentro do mundo digital pelas redes sociais (e não como mero reflexo do físico), os únicos referentes relevantes para a realização das atividades digitais passaram a ser os existentes apenas no mundo digital. Os "*e-mails*" substituíram as cartas físicas para quase a totalidade das necessidades da vida pública e privada. Com o surgimento dos e-documentos, o próprio Estado se dá por vencido e passa a usar o digital como identificadores civis, legais e sociais. Tais dados consolidam um "cidadão digital".

Neste mesmo sentido, o consumo, que poderia alegar-se ser essencialmente físico (comer, vestir, morar, aquecer-se), acaba criando todo um espaço novo de geração de valor econômico em um mundo digital, como mostram empresas como a *Uber* ou o *Ifood*. No início do século XXI, foi o mundo material que foi se tornando acessório ao mundo digital, e hoje, basicamente, a única informação que o mundo físico precisa prestar às lógicas de organização das sociedades digitais é o endereço de entrega dos itens de consumo material.

Neste novo estado de coisas, cumpre refletir sobre democracia. Em princípio, o corpo de direitos estabelecidos a partir do século XVIII tinha a razão de proteger o indivíduo limitado ao mundo material. Sua privacidade, sua liberdade de pensamento, a inviolabilidade do seu corpo físico, do espaço de sua casa (entendido como íntimo) tinham por função primordial preservar o cerne sociológico e filosófico do que é o indivíduo materialmente, conforme definidos a partir do liberalismo do século XVIII. O Estado protegia as funções biológicas de vida, sociológicas, de ação política e filosóficas da escolha dos indivíduos.

Mesmo quando nos tornamos uma "sociedade da informação"[12] (no final do século XX), essa informação era controlada e matizada por ferramentas estatais e interesses comerciais. O controle sobre os sinais de rádio e televisão, e a legislação de telecomunicações dos anos 70 e 80 são exemplos desse processo. O cidadão, naquele momento, precisava que estivessem garantidas a liberdade e a privacidade para operar dentro da democracia. Em resumo, a proteção positivada do cidadão no mundo material (desde suas funções

12 Aqui, faço uma distinção entre Sociedade da Informação e Sociedade Digital a partir do marco de consolidação do "cidadão digital". Enquanto o espelhamento entre o digital e o material garantia o digital como acessório, estávamos numa "sociedade da informação" (século XX). No século XXI o mundo digital se constitui por si mesmo e constrói uma sociedade digital (Mosco, 2017).

de privacidade até sua liberdade) são fundamentais para o exercício contemporâneo da democracia. A questão central é se tais proteções podem ser alcançadas e efetivadas pelo uso análogo do que existe de regramento no mundo material para o novo cidadão digital?

É possível estabelecer essa analogia como matriz conceitual para os regramentos no mundo digital? Basta dizermos que "o que é crime no mundo material é crime no espaço digital"? E, mais ainda, protegendo apenas pelo espelhamento do cidadão do mundo físico no mundo digital, assegura-se que no digital nós teremos uma escolha política livre e democrática? Protegendo apenas a "privacidade digital" é possível garantir a condição de pensamento autônomo e individual que se busca assegurar na democracia? O problema central para a resposta a essas perguntas passa pela forma como é conceituado o ciberespaço.

O conceito de Ciberespaço

O ponto de partida dessa conceituação foram as redes de comunicação analógica (telefone, rádio e televisão) nas décadas de 50 e 60. Assim, a noção original de ciberespaço se dava a partir de um conjunto de elementos definidores do "ponto de acesso" (I), do "nó de direcionamento" (II) e do "ponto de chegada" (III) e dos "pacotes de informação" (dados) (IV). O espaço digital era delimitado, portanto, pela relação que se estabelecia no processo da comunicação de dados (Fang, 2018, p. 28).

Aos poucos, este sentido foi consolidando a imagem de uma "rede" (network) que ligava digitalmente (e fisicamente) pontos de acesso aos locais acessados. A ligação digital entre esses pontos criava uma ilusão de um espaço imaterial, mas real, que era entendido por analogia com o espaço físico e, portanto, passível de ser coordenado/regulado pelos Estados. Encontrar responsáveis por ações no mundo digital era sempre sair deste mundo e voltar ao material para poder identificar, processar, culpar, taxar ou fazer compensar.

Em 1997, os EUA criaram números de registro e alocação digitais, entregando o manejo desses números de endereçamento (que individualizam cada acesso nas redes) a uma empresa privada chamada ICANN (*Internet Corporation for Assigned Names and Numbers*)[13]. Estava esquadrinhado o espaço digital, e as permissões ou revogações do uso deste espaço ficavam a cargo de uma empresa privada norte-americana. Isto foi apenas o começo da disputa de soberania sobre o ciberespaço (Konkas, 2023).

Até aqui, esquadrinhar o espaço digital e dar-lhe forma em números de endereçamento correspondia a ter a posse desse mesmo espaço. Neste sentido aparece no conceito de ciberespaço dado pelo *National Military Strategy for Cyberspace Operations*[14] do governo dos EUA, em 2006, como

13 No Brasil, hoje, esta é uma das funções do Comitê Gestor da Internet (CGI.br).

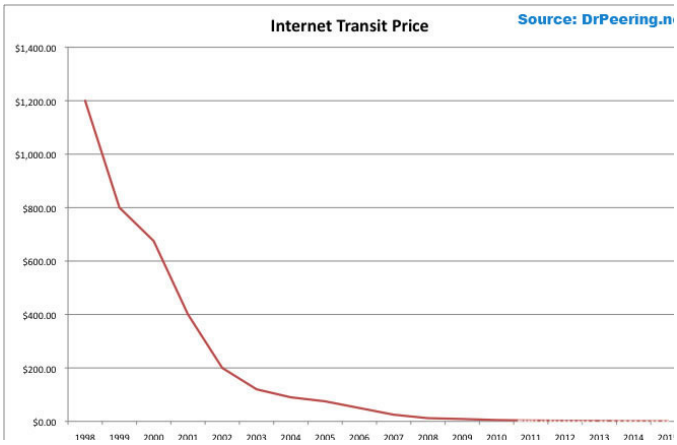
14 DEPARTAMENT OF DEFENSE WASHINGTON. **The national military strategy for cyberspace operations (U)**. Washington: Departament of defense, 2006. 54 p. Disponível em: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-023.pdf. Acessado em: 25 jul. 2025.

> […] a domain characterized by the use of eletrocnics and electromagnetic spectrum **to store, modify and exchange information** via networked systems and physical structures (Departament of Defense Washington, 2006, p. 9, grifo nosso).

Até o início do século XXI, para se proteger os cidadãos, pelo princípio da analogia do material com o digital, bastava o Estado proteger os dados de identificação do indivíduo que acessa a rede e as informações por ele armazenadas propositalmente[15]. Foi a partir do atraso no entendimento dos Estados sobre como operava o mundo digital que algumas empresas provadas vislumbraram a oportunidade de se tornarem bilionárias. Se os dados de identificação e as informações produzidas e armazenadas pelos indivíduos estavam protegidas pelo conceito de ciberespaço da época, as informações produzidas pelo **trânsito** do indivíduo (usuário) no mundo digital (tais como compras online, visitações, escolhas, "curtidas", manifestações, etc.) não estavam. Rapidamente o Google e outras empresas se organizariam no mundo digital para estimular não apenas que os indivíduos se constituíssem no mundo digital (através da criação de perfis e redes sociais) como também que navegassem e se mantivessem ativos vinte e quatro horas por dia, produzindo informações.

Por essa razão, não deve ser estranho que o custo do acesso às redes mundiais de computadores venha caindo rapidamente, se comparados aos anos 80 e 90 do século passado, e a tendência é – no mínimo – a gratuidade. Não se trata de diminuição do custo de acesso pelas "novas tecnologias", mas de um modelo de negócios que agora dependia da geração destas informações de passagem do indivíduo pelas redes[16]. Quanto mais tempo de conexão, maior o número de informações produzidas e maior o lucro das empresas que operam nesse nicho.

Imagem 1 – Internet Transit Price



Fonte: DrPering.net, c2014.

15 Cabe ressaltar entre as informações propositalmente depositadas nas redes e os dados extraídos pela ação do indivíduo dentro do mundo digital. Sobre o primeiro tipo de informação, há um consenso já relativamente estabilizado de que está protegido pelas analogias com a propriedade intelectual no mundo material. Sobre o segundo tipo de informação (as impressões de passagem e movimentação nas redes), as "*Big Techs*" asseguram o direito de serem donas de tais informações. A afirmação se baseia na ideia de que tais informações não seriam possíveis sem o trabalho de *tracking* que tais empresas fazem. Elas seriam, assim, as criadoras destes conjuntos de informação que – hoje – são imensamente mais valiosas do que as primeiras.

16 O dado agregado é média. Se estratificados, os dados mostram que em áreas periféricas e com baixo nível de consumo, os valores se mantiveram ou tiveram reduções marginais (como na América Latina) e até aumentaram, como em alguns casos no continente africano (Kazeem, 2019).

No século XXI, empresas chamadas de "*Big Tech*" incentivam que Estados tornem o direito ao acesso ao mundo digital um direito humano, e trabalhem (os Estados) para franquear a todos a possibilidade de se tornarem "cidadãos digitais". A partir daí, todo cidadão no mundo digital é criador incessante de informações de passagem[17] nas redes, e tais informações geram valor econômico. Da mesma forma que operou o surgimento da educação pública no século XIX, a lógica é que os Estados paguem os custos de inserção digital a todos para que estes ofertem matéria-prima (como cidadãos digitais) à iniciativa privada. Agora, não mais dentro de Estados apenas, mas em escala mundial.

Contudo, diferentemente das informações de distinção dos sujeitos no mundo material (seu nome, endereço, números de documentos, ou suas produções intelectuais e artísticas específicas dentro da rede), esse novo rol de informações produzidas pelos sujeitos NÃO É propriedade sua, de tal sorte que podem ser organizadas, reorganizadas, apropriadas e vendidas a partir de interesses de empresas privadas. **A mercantilização dos sujeitos digitais implica na alienação destes sujeitos sobre as informações por eles produzidas**. E aqui, convenientemente, as analogias capitalistas entre a propriedade privada do mundo material no século XX e a propriedade do mundo digital do século XXI cessaram.

A geração de valor produzida pela apropriação das informações de passagem dos diversos sujeitos pelo mundo digital foi tão grande que empresas não se preocupam mais em estabelecer ligações entre o digital e o material. Perfis falsos são criados em todas as redes sociais sem nenhuma preocupação ou controle, mostrando que as informações de distinção dos indivíduos (o foco de toda legislação e segurança do Estado no século XX) se tornaram desimportantes.

As grandes empresas digitais não querem mais saber quem você é, ou onde você está. Estas informações não são mais requeridas para geração de valor no mundo digital. Elas precisam do seu perfil digital. Mapeando as escolhas, as preferências ou antipatias de sujeitos quaisquer (reais, paródias, ocultos, anônimos, etc.), ainda que não identificados ou distinguidos no mundo material, obtêm-se informações comerciais relevantes que são apropriadas pelas empresas digitais e vendidas como se propriedade delas fossem. Para a construção de perfis digitais psicográficos que possam ser usados para estratégias de marketing ou estratégias políticas, é totalmente desnecessária hoje a identificação dos cidadãos materiais no mundo digital. Dito de outra forma, o conjunto de informações que o perfil "gatinho azul" produz nas redes tem o mesmo valor do perfil que o perfil "Antônio Silva", este último plenamente identificado e singularizado no mundo material.

Embora sem conseguir um controle efetivo sobre essas informações, não passou desapercebido pelo Estado, nos últimos anos, a quantidade de valor gerada pela apropriação das informações de passagem. E, embora ainda não haja uma forma de taxação específica

17 As informações que individualizam o sujeito e permitem localizar o usuário no mundo material são protegidas, pois entende-se que o sujeito as detém. Já todo o outro rol de informações produzidas no mundo digital se entende como "não detidas" por ninguém. Todo acesso a um site de compras, páginas vistas, tempo de presença em cada site ou cada tela, "curtidas" ou outras sinalizações de aprovação, ou desaprovação gera uma brutal quantidade de informação que os modelos de negócio digitais no século XXI se apropriaram para gerar valor.

deste tipo de produção e apropriação da **criação humana no mundo digital**, o conceito de ciberespaço foi sendo paulatinamente modificado para não apenas "proteger" os usuários, mas também permitir ao Estado um maior controle (soberania) sobre o mundo digital.

Em 2003, em um documento intitulado "*The National Estrategy to secure cyberspace*", a Casa Branca definia "*cyberspace*" como

> […] composed of hundreds of thousands of interconnected computers, servers routers, switches, and fiber optic cables that allow our critical infrastructures to work (United States, 2003, p. vii)[18].

Embora fique claro que o conceito é muito pouco funcional, ele já amplia o sentido de ciberespaço se comparado com o do século XX. Antes, eram apenas os servidores e outros espaços de armazenamento de informações que compunham tal definição. As estações de contato e produção (os PC's dos usuários) não eram parte do ciberespaço, assim como também não eram os roteadores ou pontos intermediários de redirecionamento.

O conceito usado em 2022 pela NICCS (*National Initiative for Cibersecurity careers and studies*) da CISA (*Cybersecurity and Infrastructure Security Agency*) dos Estados Unidos para o entendimento do mundo digital já não é mais "*cyberespace*", mas sim "*cyber ecosystem*", e a agência o define como:

> The interconnected information infrastructure of interactions among persons, processes, data, and information and communications technologies, along with the environment and conditions that influence those interactions (NICCS, 2025, *online*).

A diferença é grande. A analogia que havia guiado as sociedades em todo o século XX, do espaço digital como um "espaço real não-material", vai se dissolvendo. O centro do conceito de 2022 não é mais qualquer noção de "espaço" em si, e sim as relações ou "sistemas" de interconexão. Em 2022, o centro da proteção que deseja atingir o Estado não são mais os dados de identificação ou os locais do seu armazenamento, mas os indivíduos digitais, duas escolhas, seu meio e suas condições de interação.

A partir deste novo entendimento do que seria o "digital", a analogia para com o espaço físico (que orientou as primeiras ações do Estado no mundo digital) começa a ser descartada e um novo esforço de conceituação se faz necessário. A proteção e controle do Estado (que caracterizam a ideia da soberania) não pode mais ser estabelecida unicamente nos pontos materiais em que o mundo digital encontra o mundo material (servidores, *switches*, cabo, etc.) é preciso também um esforço para pensar, no momento atual, em formas de proteger o "meio digital" em si, as "interações" dos usuários, e os efeitos ou consequências dessas ações na vida material.

O tecido digital se afasta da noção analógica de "espaço" e se aproxima do sentido contemporâneo de "tempo". Movimento, aliás, que é parte da transformação epistemológica

18 UNITED STATES. **The National Estrategy to secure cyberspace**. Washington: The White House, 2003. Disponível em: https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf. Acesso em: 30 ago. 2023.

característica do século XXI[19]. A ilusão do espaço digital se desfaz, e a sua transformação em um contínuo "espaço-tempo" é o que permite a gigantesca geração de valor econômico proporcionada pelo mundo digital. Essa mesma transformação, contudo, também acaba por ameaçar as democracias contemporâneas.

A PROTEÇÃO DA DEMOCRACIA

Um dos problemas contemporâneos com maior urgência a ser resolvido é a questão da influência do mundo digital sobre a democracia[20]. As transformações recentes[21] (como as experiências do *Brexit*, ou mesmo as eleições brasileiras de 2018 e 2022) se provaram um desafio muito complexo para as antigas ferramentas de controle do século XX, e até mesmo para algumas tentativas desenvolvidas no início do século XXI. Tanto o controle e apropriação das informações de passagem dos usuários quanto a formação digital dos indivíduos passaram a ser instrumentalizadas politicamente através de técnicas de micro segmentação (Eisenberg; Cepik, 2002)[22].

A profusão de novos canais e plataformas de comunicação torna praticamente impossível os controles e responsabilização cível ou penal baseados na ultrapassada analogia do mundo digital como com um "espaço" que espelha o material. Uma pacata senhora aposentada de 65 anos no mundo real pode ser uma ativa neonazista no mundo digital, operando nas redes sociais a partir de um celular vinte e quatro horas por dia. Se nem as informações de passagem produzidas pelos usuários no mundo digital são propriedades destes usuários (pois estas são as fontes de geração de valor pelas *Big Tech*), então crimes cometidos no mundo digital (como as "*fake news*") parecem deter uma condição ontológica de não terem autoria, ficando mais além das capacidades de controle (soberania) do Estado[23].

---

19 Entre todas as novidades que estão em estudo ou já de alguma forma assentadas, a epistemologia do século XXI passou a não assumir o objetivo e o subjetivo como separados, emulando a impossibilidade de separar o tempo do espaço predito pela Teoria da Relatividade (Wendt, 2015).

20 "A revolução digital, em particular o forte desenvolvimento das redes sociais, alterou radicalmente o funcionamento da nossa democracia. Oferece inúmeras novas possibilidades de comunicação e de acesso a uma quantidade infinita de informações. Mas a Internet também deteriorou a qualidade que tradicionalmente estava assegurada na informação, reduziu o nível dos debates e inundou o espaço público de slogans simplistas, notícias falsas e polarização. Substituiu as comunidades reais, que uniam pessoas reais, solidárias entre si, por bolhas virtuais, que não proporcionam aos seus membros ligações genuínas" (Council of Europe, 2022, p. 3, tradução nossa).
Original: "The digital revolution, in particular the strong development of social media, has radically changed the functioning of our democracy. It offers a myriad of new possibilities to communicate with each other and to access infinite information. But the internet has also undermined the traditional quality assurance of information, lowered the standard of debate and filled the public space with a deluge of simplistic slogans, fake news and polarisation. It has replaced the real communities that bound real people together, caring for each other, with virtual bubbles that do not give their members a rooting in anything real" (Council of Europe, 2022, p. 3).

21 "Cyberspace is not just the space in which myths are enacted; it also contributes to mythic thinking today, because it embodies the sense of betwixt and between (or, more formally, what cultural theorists call liminality). Myths are fed by the sense that we are leaving one era, the Industrial Age, and entering a new one, with a host of names, most of which, like "Information Age" and "Digital Age," have to do with computers. The "then" and "now" markers change depending on whether one accentuates the technological, the economic, the political, the social, or the cultural (e.g., are we moving from the factory to the office? From modernism to postmodernism?). They also change depending on how one feels about (e.g.) the difference between the Information Age and the Surveillance Society" (Mosco, 2004, p. 32).

22 Forma ou processo de uso de grandes bases de dados sobre as redes digitais para mapear padrões de comunicação e endereçar estilos de comunicação exclusivos para determinados grupos com o objetivo de aumentar a aderência, confiabilidade e legitimidade da mensagem passada, indiferente – muitas vezes – ao conteúdo ser ou não verdadeiro.

23 Até o fechamento deste artigo, eu esperei o texto final do PL 2630 proposto pelo governo brasileiro para regular as *Big Tech* e "acabar com as *fake news*". Pelos mesmos problemas apontados aqui neste artigo a tentativa brasileira também é inútil. Padece de problemas de desenho da lei, falta de capacidade técnica do Estado e um profundo desconhecimento da escala de produção de informações que hoje existe no mundo digital. Mesmo o DSA (*Digital Services Act*), a regulação proposta pela EU entrará em vigor apenas em 2024 e, na prática, ainda estamos sem exemplos efetivos de proteção estatal.

Entender o digital como um espelhado “espaço físico” para poder aplicar a ele, por analogia, as ferramentas de controle historicamente desenvolvidas para o Estado Moderno têm se provado insuficientes para a proteção da própria democracia. A computação na nuvem, por exemplo, tornou quase impossível sustentar tal analogia, já que os “servidores” não conseguem mais ser usados como únicos e individuais pontos físicos de entrada, passíveis de punição e controle com relação à informação que fazem circular. Nesta brecha, muitas ameaças têm se mantido ativas. Tanto as companhias passam a vender informações para partidos ou grupos políticos, quanto esses grupos passam a atuar de forma criminosa e agressiva contra instituições democráticas, sem uma oposição que seja minimamente funcional por parte dos poderes de Estado.

No mundo físico, desenvolveram-se polícia, fronteiras, vigilância por câmeras, denunciação anônima e uma série de outras ferramentas de Estado para controlar o espaço e fazer valer a soberania do Estado. Isso se deve, em grande medida, ao fato de que no mundo físico a matéria não se reproduz (ou desaparece) numa velocidade maior do que os meios de controle e prova podem se apropriar (ou tomar ciência) da existência dela. Se pegarmos, por exemplo, as formas pelas quais o Estado controla atividades como a propagação do nazismo, ou como taxação de mercadorias produzidas, veremos a importância da materialidade física. A condição de existência física da matéria é a base de toda construção institucional que o Estado fez para exercitar sua soberania. Isso deixou de existir nos últimos vinte anos no mundo digital[24].

Todas as tentativas de controle físico do mundo digital têm sido infrutíferas. Códigos rastreáveis, programas de espelhamento e manutenção digital de dados, e toda a sorte de singularização das informações têm sido tentadas. A tecnologia da NFT[25] é exatamente isso. Esforços desesperados para manter a analogia do mundo digital com o físico e reproduzir no digital a escassez característica do mundo material. A arma de um crime que se quer punir, ou o produto do trabalho humano que se quer taxar, não se multiplicam (ou somem) no mundo material como é capaz de se fazer no mundo digital[26]. Tal característica do mundo digital vem se provando um desafio complexo para que o Estado possa exercer efetivamente sua soberania sobre o mundo digital.

Parte significativa desse problema reside na analogia do digital como um “espaço” que requer uma materialidade singular (ou ao menos uma construída por dados) para poder se fazer entender na cabeça dos seres humanos. De onde (base física) partem os ataques cibernéticos a um país? Onde está o ponto de acesso do usuário que atenta contra a democracia? O referente da localização espacial de tais perguntas é essencial para que

24 No mundo real, dois corpos não podem ocupar o mesmo espaço ao mesmo tempo, e não há replicação da matéria sem um enorme uso de energia e tempo. No mundo digital, ao contrário, tudo é replicável, consumível e some sem deixar quase nenhum rastro.

25 NFT quer dizer textualmente “*non fungible token*” ou peça não consumível, no sentido que não desaparecerá ou será replicada em sua essência. É uma tentativa do mundo digital de recriar a escassez do mundo material e conferir “valor” a certos objetos digitais. Uma obra de arte produzida no mundo digital pode ser infinitamente copiada e não há nenhuma possibilidade de escassez. Na percepção econômica tradicional, seu valor seria sempre o mesmo e tendente a zero. Com a criação das “NFT’s” o capitalismo digital tenta romper com essa característica do mundo digital e, assim, aplicar as lógicas de valor pela escassez bem conhecidas do mundo.

26 Uma das tentativas mais bem-sucedidas para evitar o apagamento e mudança de dados é a tecnologia de “*blockchain*” que está permitindo a consolidação de moedas digitais, conforme a professora Gláucia Campregher (2022).

as ferramentas atuais do Estado possam operar no controle ou contenção exatamente por analogia. A existência digital sem a referência material é ainda difícil de ser compreendida, especialmente para sociedades historicamente analógicas.

A experiência norte-americana

A velocidade da transformação digital é ainda algo com o qual os países e as sociedades do mundo não se adaptaram. Se é verdade que os EUA foram o país que controlou o mundo digital em todo o século XX, criando empresas para indexar, controlar e explorar o mundo digital, também é verdade que mesmo assim os EUA parecem não estar prontos para as transformações mais recentes tanto da economia que lida com o digital, quanto das transformações sociais derivadas.

O sociólogo Vincent Mosco (Mosco, 2004) argumenta que existia um mundo digital antes das *Big Techs*[27] e outro, completamente diferente, após as transformações que estas empresas geraram no mundo digital. O século XXI tem acompanhado mudanças cada vez mais rápidas e profundas na forma como as sociedades vivem através do mundo digital. Se todo o processo de criação da rede mundial de computadores foi controlado pelos EUA durante o século XX[28], a partir da escala de produção de informação praticada no século XXI o Estado norte-americano não foi capaz de manter o domínio e escrutínio da rede.

As repercussões desta transformação foram muitas, desde a percepção da perda de controle do Estado, redundando em investigações sobre as falhas de segurança que acabaram por permitir os atentados ao WTC em 2001, até em investigações sobre crimes sexuais e contrabando de armas químicas. A sociedade norte-americana passou a exigir um controle sobre o mundo digital que os EUA, enquanto Estado, não conseguiria mais impor.

Neste cenário, as "*Big Tech*" se impõem. Não apenas houve uma modificação na forma de extrair valor do mundo digital. A criação das chamadas "redes sociais" (como *Facebook*, *Twitter* e *YouTube*) fez surgir, efetivamente, indivíduos digitais. Antes delas, havia uma presença efêmera dos seres nas redes. A internet era usada como meio de comunicação, depósito de dados ou plataforma de troca. **As redes sociais geram vida (existência) digital**. Ao construir um "perfil" o usuário se constitui no mundo digital. Seus gostos, interesses, posições políticas, preferências sociais, e até a forma como constrói seus discursos passaram a ser apropriadas (exploradas) pelas plataformas que mercantilizaram estas "informações de passagem". Não interessava mais o nome real do usuário, seu endereço ou qualquer destas informações que o mundo material exige e impõe "sigilo". As redes lucram mais com perfis falsos (já que com eles também diminuem os custos legais

27 *Big Tech* é o termo utilizado para se referir ao conjunto de companhias que controlam e operam no mundo digital. O *Google* é criado em setembro de 1998, o *Facebook* em fevereiro de 2004 e a *Uber*, por exemplo, em março de 2009. Cada um desses serviços tem uma empresa por trás, como, por exemplo, a *Alphabet Inc*. controladora do *Google*, *YouTube,* etc.

28 Da década de 60 até 1997, era o "Departamento de Comércio" norte-americano que controlava todas as permissões e até mesmo as indexações de endereçamento na rede. Em 1997, o governo dos EUA passou esta atribuição (e o monopólio de atribuir nomes e números de registro) para a empresa ICANN (*Internet Corporation for Assigned Names and Numbers*), que mantém ainda hoje suas atribuições (ICANN, 2021).

de manutenção dos perfis) e não precisam para isso sequer saber quem efetivamente está por trás do perfil, onde ou com que objetivo. Todo o arcabouço de governança digital criado no século XX ficou completamente obsoleto.

Constituídos como indivíduos digitais, os seres humanos passaram a viver nas redes. Consumir, aprender, colaborar, explorar, trabalhar, roubar, ameaçar, sequestrar e praticamente todos os verbos de ação que são feitos no mundo material, passaram a ser realizados no mundo digital. As redes sociais hoje dispensam nomes em troca de informações sobre comportamento político, social e comercial construídas, de preferência, vinte e quatro horas por dia. Toda a luta dos marcos de governança do século XX sobre não entregar "informações sigilosas" dos indivíduos ficou anacrônica. O modelo de extração de valor hoje, dispensa qualquer informação que relacione o real e o digital. Com exceção do endereçamento para entregar as mercadorias compradas, nada mais é necessário que as plataformas mantenham.

A partir da passagem desses seres digitais pelas redes, eles vão imprimindo padrões de comunicação, de conduta política, de preferência comercial e de comportamento[29]. No século XXI, o mundo digital extrai valor exatamente destas informações que, no século XX, eram tidas como desimportantes (*garbage* no termo em inglês). Se tais informações serão produzidas usando um perfil social com nome e fotos verdadeiros, ou se vai ser um perfil falso com uma foto de bichinho de pelúcia e um nome completamente estranho, para as plataformas, não faz hoje a menor diferença. O bichinho de pelúcia no perfil vai consumir, compartilhar, produzir, etc. da mesma forma que o perfil "verdadeiro", e para o mundo digital sua individualização não precisa mais espelhar o mundo material. Daí surge a pergunta: então, o que o Estado tem efetivamente que proteger?

No século XX eram os endereços reais, números de documentos e toda sorte de informações que – por analogia com o mundo material – o Estado pensava serem importantes. A mudança nessa importância não foi bem compreendida ainda hoje pelos Estados, nem mesmo o norte-americano. Trilhões de dólares foram produzidos a partir dos rejeitos informativos digitais (informações que no século XX ninguém queria) e os controles estatais foram inócuos[30]. Tanto para proteger a sociedade, quanto para taxação e cobrança de impostos. Na prática, as *Big Techs* viveram os últimos 10 ou 12 anos de um paraíso capitalista sem lei. Empresas digitais de apostas, de jogos, de venda do que quer que se imagine (bens e serviços legais e ilegais) se amontoaram nas redes, tornando-se bilionárias e deixando o Estado, cada vez mais impotente, a partir da analogia primordial de compreensão que citamos neste artigo. Relacionar o digital com o material não mais permitia a compreensão do digital como um dia se tentou.

O momento em que o Estado se deu conta de que precisava voltar a compreender o mundo digital e, agora a partir de novas balizas, foi o surgimento da *Cambridge Analytica*

29 Todas essas informações eu chamo aqui de "informações de passagem" porque são produzidas a partir do tempo de uso (conexão) dos cidadãos no ciberespaço.

30 O exemplo mais preocupante foi o da *Cambridge Analytica*, que comprou do *Facebook* bilhões de informações (ao preço de 2 ou 3 dólares por perfil) que naquela época não estavam protegidas porque eram "desidentificadas". O *Facebook* (*Meta*) foi alterando os termos de privacidade para obrigar-se a proteger apenas as informações de individualização no mundo material e não os dados de passagem. Estes foram vendidos para a *Cambridge Analytica* (Mccallum, 2022).

e a manipulação que o mundo digital passou a fazer dos sentidos políticos dentro de uma sociedade. O referendo de 23 de junho de 2016, no qual a Inglaterra decide sair da União Europeia, descortinou esse novo mundo digital para o qual todas as ferramentas de controle anteriores (que já eram quase inúteis) se tornaram obsoletas.

EUA, Europa e praticamente o mundo todo percebera que o que deveria ser protegido não eram as informações estacionárias num servidor qualquer, a respeito da origem e caracterização material de algum usuário. **O que deveria ser protegido era a condição humana de tomada de decisão individual, bem-informada e crítica**. O mundo digital capturava a essência dos nossos construtos políticos e a unidade básica das nossas democracias: **as condições para formar juízos a respeito do mundo**.

A comercialização deste novo "produto", sequestrado pelas *Big Tech*, nos trouxe de volta o fascismo. A extrema-direita, fortemente apoiada por bilionários, conseguiu sobrepassar características singulares de alguns políticos de massa, como capacidade de comunicação, carisma, empatia, representatividade, com mecanismos e ferramentas de comunicação digital. Hoje, na política digital, pode-se criar Martin Luther King's e Mandela's do nada, com estratégia de comunicação digital. Isso deu à extrema-direita todo o sucesso eleitoral de que precisava para atacar a própria ideia de democracia.

Ainda mais interessante sobre isso, é que as *Big Tech* comercializam essas informações, extraem valor financeiro e político sobre tudo o que ocorre nas redes, mas, ao mesmo tempo, declaram-se neutras e inimputáveis pelo que quer que seja produzido através de suas ferramentas no mundo digital. Esse comportamento dual de uma presença para reivindicar lucros e propriedades e, ao mesmo tempo, uma ausência para assumir responsabilidades é a questão central hoje em todos os estudos sobre governança digital[31].

Nesse sentido, a Suprema Corte Norte-Americana passa, em abril de 2022, a analisar a questão, a partir do caso "Reynaldo Gonzalez *et al*. vs. *Google*"[32]. Basicamente, os proponentes da ação argumentam que a indexação e oferecimento da informação não podem ser considerados uma atitude neutra:

> Mere posting on bulletin boards and in chat rooms was the prevalent practice when section 230[33] was originally enacted. But over the last two decades, many interactive computer services have in a variety of ways sought to recommend to users that they view particular other-party materials, such as written matter or videos. Those recommendations are implemented through automated algorithms, which select the specific material to be recommended to a particular user based on information about

31 Basta acessar os relatórios de pesquisa produzidos pela União Europeia em 2021 e 2022 para se ter uma ideia de como este problema está sendo central para a política do Velho Continente. Por um lado, há uma dificuldade de taxar e regular, por outro, há também dificuldade de responsabilizar e mesmo de proteger os cidadãos digitais. (ver, por exemplo, o "Relatório do grupo de alto nível para a democracia europeia" de 31 de janeiro de 2022).

32 UNITED STATES. Court of appeals for the Ninth Circuit. Petition for a writ of certiorari filed. **No. 21-1333**. Julgado em: 22/06/2021. Disponível em: https://www.supremecourt.gov/docket/docketfiles/html/public/21-1333.html. Acesso em: 25 jul. 2025.

33 A "seção 230" do título 47 do "Telecommunications Act", de 1996, diz que "No provider or user of an interactive computer service shall be treated as the publisher of or speaker of information provided by another information content provider" (One hundred fourth congress of the United States of america, 1996, p. 101). Esse dispositivo é a base da blindagem que as *Big Techs* se atribuem quando responsabilidades civis ou criminais recaem sobre elas.

> that user that is known to the interactive computer service. The public has only recently begun to understand the enormous prevalence and increasing sophistication of these algorithm-based recommendation practices (United States, 2021, *online*).

O caso em tela discute exatamente a pergunta: "O que se deve proteger, com respeito ao mundo digital?". O argumento dos peticionantes é exatamente que a indexação e oferecimento de qualquer conteúdo não se dá por meio de um algoritmo "neutro" e, se permite lucro a partir da compra de espaços publicitários e preferências de indexação, também precisa responder pelos danos que as informações ali dispostas possam produzir.

> That financial structure has given rise to the now widespread practice of recommending (for want of any agreed upon better term) material to website users, in the hope of inducing them to look at yet more material and thus to remain ever longer on that website. Many of those recommendations are based on algorithms, which review all the information an interactive service provider has about each particular user, and selects for recommendation the material in which that user is most likely to be interested. "[A]lgorithms [are] devised by these companies to keep eyes focused on their websites.... '[T]hey have been designed to keep you online [...] (United States, 2021, *online*).

Até o fechamento deste artigo, a Suprema Corte ainda não havia se pronunciado, mas a questão é clara e recomenda uma mudança completa de paradigma. O que se deve proteger, via legislação de Estado, não é mais o "espaço" digital, tomado em analogia com o material através das informações que permitem reconhecimento e individualização de cidadãos reais. Tampouco as informações estacionárias, dentro de um ou mais servidores, precisam exatamente da proteção do Estado no mundo digital do século XXI. Está se pleiteando a proteção do Estado ao "tempo" que o indivíduo fica aderido ao mundo digital. Mudar o conceito de Ciberespaço para uma interpretação de tempo dentro das redes permite proteger a própria capacidade de compreensão do mundo tomada individualmente por cada cidadão, a partir da responsabilização das indexações e apresentações de informação ao cidadão digital.

Não é claro se esta mudança de paradigma será suficiente para proteger os cidadãos (e por conseguinte a política e a democracia) no mundo digital. Contudo, é visível que o caminho tomado pelos EUA parece mais fértil para resolver o problema do que as iniciativas brasileiras, por exemplo. Iniciativas essas que passamos a analisar.

O caminho do Brasil

A relação de analogia entre o digital e o material já surge no Brasil a partir da LGPD (Lei Geral de Proteção de Dados) de 2018[34]. Há uma enorme dificuldade em referenciar a abrangência da Lei exatamente pela questão da analogia. No artigo 3º, por exemplo, a lei afirma que

34 BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Brasília: Presidência da República, 2018.

> [...] aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados (Brasil, 2018, *online*)

seguido de 3 incisos que tentam dar mais acuidade geográfica ao disposto enfatizando o elemento "território nacional". Por óbvio, aqui entra a aplicação da noção de soberania e, portanto, legislar somente sobre coisa "nacional", mas também se recorre à malfadada noção analógica de "território" que, como mostramos, tem sido abandonada pelo mundo todo no que tange à governança digital[35].

No artigo 5º da mesma lei, ela tenta definir sobre o que, efetivamente, a lei versa, elencando um total de 19 incisos para tentar dar conta da definição dos quatro elementos que compõem o mundo digital, a saber: emissor, receptor, meio e mensagem[36]. A tentativa de precisar os termos da lei e substanciar o melhor possível os elementos sobre os quais se legisla, falha exatamente por conta da manutenção da analogia com o mundo material (Nemer, 2022). Falha essa que abre brechas enormes para que a lei seja contornada em sua capacidade regulatória central: a proteção do cidadão e do Estado brasileiro.

Em nenhum momento, em toda a redação da lei, se lê qualquer referência às palavras "ciberespaço", "ecossistema digital" ou quaisquer outras que estejam sendo utilizadas nos documentos de governança digital. Em apenas um local (no início do primeiro artigo) usa-se o termo "meios digitais" e, EM MAIS LUGAR NENHUM o termo aparece. A preocupação da lei é, assim, com "dados" estacionários e seu referencial material geográfico (nacionais) tão somente. Estando já completamente ultrapassada e sem capacidade sequer de definir — conforme usabilidade contemporânea — os próprios termos a que se destina, a lei de 2018 falha fragorosamente.

A governança digital brasileira opera em cima de duas leis (14129 de 29/03/2021 e Lei complementar 182 de 01/06/2021[37]), 8 decretos (10996, 10782, 10332, 10278, 9756, 9854, 9637, 9319, lançados entre 2018 e 2022 apenas), contando com mais cinco portarias e uma resolução para o triênio de 2013–2015. No documento principal, a lei 14129, não aparece nenhum termo semelhante aos mencionados acima, afirmando no inciso XI do artigo 4º que usará todos os conceitos da LGPD de 2018[38]. Incorre-se daí num erro teórico e epistemológico continuado ao não se adequar aos sentidos do digital em compasso com o que se produz no mundo todo.

O curioso, nessa lei, é que, apesar de utilizar-se de um arcabouço teórico insuficiente e falho para definir o digital, ela se propõe a ser contemporânea no que tange à construção

35 O DSA (*Digital Services Act*) europeu e o DMA (*Digital Markets Act*) já tratam de não se restringir ao território europeu como sede de "servidores" que guardam informações estacionárias e pretendem soberania sobre tudo o que for acessado por cidadãos europeus: "A fim de assegurar a eficácia das regras estabelecidas no presente regulamento e condições de concorrência equitativas no mercado interno, essas regras deverão aplicar-se aos prestadores de serviços intermediários, independentemente do seu local de estabelecimento ou da sua localização, desde que ofereçam serviços na União, tal como comprovado por uma ligação substancial à União" (União Europeia, 2022, *online*).

36 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). (Redação dada pela Lei nº 13.853, de 2019). Brasília: Presidência da República, 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 25 jul. 2025.

37 Apenas aqui mencionada por regular "startups" que comumente são formas de inovação digital no século XXI.

38 Até o fechamento deste artigo, o conteúdo da PL 2630 ainda não tinha sido votado na Câmara Federal.

de um “cidadão digital” estabelecendo uma ruptura com a cultura do espelhamento entre o digital e o material e no seu capítulo V, artigo 42 afirma que “os órgãos e as entidades referidos no art. 2º desta Lei, mediante opção do usuário, poderão realizar todas as comunicações, as notificações e as intimações por meio eletrônico”. O perigo desta abordagem é que sem um arcabouço sólido de entendimento e definição do que seja o espaço digital no século XXI, a lei pula um passo adiante de tornar desnecessários processos históricos no mundo material (intimação e notificação, por exemplo) substituindo-os por analogias no mundo digital. Desnecessário argumentar novamente pela incongruência desta analogia, mas é preciso perceber que o caminho atribulado da “modernização” da legislação, ao tentar “pular” etapas importantes de regulação, compreensão e teorização, acaba criando espaços de “não-legislação” no mundo digital que podem ser utilizados em desfavor das melhores práticas jurídicas[39]. As iniciativas do governo Bolsonaro se tornam ainda mais preocupantes quando se lê no decreto 10332 de 2020, em seu anexo, o objetivo de “transformar cem por cento dos serviços públicos digitalizáveis até 2023”. Sem resolver a questão central do que é e como se conceitua funcionalmente o ciberespaço, parece que estamos construindo uma casa sobre o nada.

O “Plano Nacional da Internet das Coisas” (Decreto 9.854 de 25 de julho de 2019) é ainda mais falho e inócuo para realizar a proteção do cidadão e do Estado brasileiro no campo digital no século XXI. Define, por exemplo, IoT (*Internet of Things*) como

> [...] a infraestrutura que integra a prestação de serviços de valor adicionado com capacidades de conexão física ou virtual de coisas com dispositivos baseados em tecnologias da informação [...] (artigo 2º, inciso I) (Brasil, 2019, *online*).

Ou seja, novamente, nenhuma referência ao substrato conceitual-epistemológico necessário que é a representação do digital em nosso tempo e sociedade. Trabalha com uma analogia paralela que ajuda na incapacidade regulatória, estabelecendo a IoT como “prestação de serviços” numa tentativa preguiçosa de criar conexão com os marcos regulatórios já existentes e operantes para o mundo material (Pani; Pandey, 2022).

A última referência brasileira a questões como “segurança cibernética”, “defesa cibernética” é de 2018, com o decreto 9.637 de dezembro de 2018, ainda assinado por Michel Temer. Aqui, preocupa a redação do artigo 12 (modificada pelo decreto 10641 de 2021) que dá ao GSI (Gabinete de Segurança Institucional da Presidência da República) a competência sobre os temas de “segurança da informação”, alijando outros órgãos e instâncias dos processos decisórios sobre o tema. Apenas a título de ênfase, o artigo 13 da mesma lei afirma que o Ministério da Defesa (instância civil maior) precisa “APOIAR” o GSI no que se

39 As dificuldades de citação para início de processos jurídicos são comum no Brasil, sendo que o próprio STF tem recorrido ao fechamento completo dos serviços como forma de forçar os donos dos aplicativos a comparecerem frente às autoridades jurídicas brasileiras (Sant’Ana; Falcão; Vivas, 2022).
Este tipo de ação é inconsistente, eis que há várias formas de se burlar a proibição, desde os populares VPNs (*Virtual Private Network*), até extensões em browsers que não podem ser rastreados, como o *Thor*, que opera a partir da *deep web*.

refere à segurança cibernética (Puyvelde; Brasntly, 2019). É desnecessária a argumentação pela inversão dos sentidos de participação política nestas decisões, sendo que o governo Bolsonaro optou sempre pela diminuição e nunca pelo incremento participativo.

Se insuficientes e falhos são os atuais marcos de governança digital em vigor no Brasil, e temerárias as "adequações" estabelecidas ainda durante o quadriênio 2018–2022 no governo Bolsonaro, as tentativas de avanço sobre questões ainda mais contemporâneas beiram o completo desastre. No tema "inteligência artificial", por exemplo, temos as iniciativas de projetos de lei 5051/2019, 21/2020 e 872/2021[40]. Esses projetos, que sequer foram votados, em nada adentram nas questões centrais sobre inteligência artificial estudadas na contemporaneidade[41]. O projeto 5051/2019 volta a exigir "garantia da privacidade e dos dados pessoais" (SIC) e pugna pela submissão decisória da Inteligência Artificial à "supervisão humana". É descabida essa posição na medida que se torna de impossível execução. Os microprocessos gerenciados pelas inteligências artificiais são por demais numerosos para que se possa sequer pensar em qualquer submissão em *stricto sensu* e a legislação é inócua mesmo no *lato sensu*, já que não consegue sequer conceituar o que seria uma Inteligência Artificial.

O projeto 21/2020, embora algo mais elaborado, pretende definir Inteligência Artificial como artigo 2º

> [...] o sistema baseado em processo computacional que, a partir de um conjunto de objetivos definidos por humanos, pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo predições, recomendações, classificações ou decisões [...][42] (Brasil, 2020, *online*).

Nesta definição, enquadra-se até programação terminal nas antigas calculadoras científicas ou rotinas em aplicativos populares como o *Excel,* que já tem condições de reconhecer padrões externos e "prever" e "recomendar" ações. Já em 1950, Alan Turing oferecia uma reflexão mais acurada do problema central a respeito das Inteligências Artificiais que é sua relação (e não submissão) com o componente humano A PARTIR das suas concepções históricas, políticas e sociais perguntando se tais regras de mediação poderiam ser pensadas como "invariáveis no tempo" e, portanto, inumanas:

40 Projetos de iniciativa do senador Styvenson Valentim (PODEMOS/RN), deputado federal Eduardo Bismarck (PDT/CE) e senador Vital do Rêgo (MDB/PB), respectivamente.

41 As três grandes discussões aqui são sobre a autonomia, a opacidade e a responsabilidade no que tange às Inteligências artificiais (Chesterman, 2021).

42 A definição é uma cópia quase literal do artigo 3 de um documento da União Europeia (*Proposal for a Regulation of the European Parliament and of the council Laying down Harmonised Rules on Artificial Intelligence and amending certain Union legislative acts*) necessitando-se compreender o fato de que este documento é o resultado de 38 páginas de discussão anterior e que remete a um Anexo (como recurso de definição) que se refere objetivamente a "*Machine Learning*", "*Deep Learning*", "sistemas dedutivos e indutivos de máquinas" e "abordagens estatísticas". O autor do projeto desconsiderou parte essencial do documento e fez uma "cópia" cujo resultado é a impossibilidade de qualquer avanço no sentido da boa regulação.

> The idea of a learning machine may appear paradoxical to some readers. How can the rules of operation of the machine change? They should describe completely how the machine will react whatever its history might be, whatever changes it might undergo. The rules are thus quite time-invariant (Turing, 1950, p. 21).

Questionamentos contemporâneos como IA's fortes vs. IA's fracas, a aplicabilidade destas entidades e a discussão dos limites e diferenças entre *Deep Learning* e *Machine Learning* sequer parecem ter sido aventadas, e questões completamente impossíveis como a "busca pela neutralidade" (Art. 5º, inciso 4º) estão ali descritas como "princípios" operativos.

Um resumo da desconexão entre o que se discute em termos internacionais (e que representa, de alguma forma, uma melhor aderência ao atual estado da técnica na discussão) e o que o Brasil ainda está em vias de discutir legislativamente pode ser claramente visto a partir da comparação entre o que pretende disciplinar o Projeto de Lei 872 de 2021 (também sobre inteligência artificial) e a iniciativa na União Europeia sobre o mesmo assunto. No Brasil, a redação do artigo 2º do referido projeto de lei é (Brasil, 2021, *online*):

> A disciplina do uso da Inteligência Artificial tem como fundamento:
>
> i. O respeito à ética, aos direitos humanos, aos valores democráticos e à diversidade;
> ii. A proteção da privacidade e dos dados pessoais;
> iii. A transparência, a confiabilidade e a segurança dos sistemas;
> iv. A garantia da intervenção humana, sempre que necessária.

O documento produzido pela União Europeia[43] tem mais de 108 páginas e se refere ainda a outros anexos como forma de representar o pensamento legislativo do momento e afirma que o objetivo da regulação é:

> (a) harmonised rules for the placing on the market, the putting into service and the use of artificial intelligence systems ('AI systems') in the Union;
>
> (a) prohibitions of certain artificial intelligence practices;
>
> (b) specific requirements for high-risk AI systems and obligations for operators of such systems;
>
> (c) harmonised transparency rules for AI systems intended to interact with natural persons, emotion recognition systems and biometric categorisation systems, and AI systems used to generate or manipulate image, audio or video content;
> (d) rules on market monitoring and surveillance (European Commission, 2021, p. 38)

Enquanto o comparativo legislativo brasileiro ainda se preocupa com "dados" e elenca valores que, embora essenciais, estão postos de forma vaga e inoperante (como

43 EUROPEAN COMMISSION. **2021/0106 (COD)**. Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence act) and amending certain union legislative acts. Brussels: European Commission, 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Acesso em: 28 jul. 2025.

“ética”, “direitos humanos” e “diversidade”), a contraparte europeia já trabalha num rol taxativo de proibições no uso de sistemas de IA, obrigações para os operadores e regras de transparência com requerimentos específicos para a avaliação de risco na utilização de tais tecnologias. Pode parecer incorreta a comparação aqui feita a partir da ideia de que a União Europeia funciona com a burocracia de uma organização supranacional composta, em grande medida, pelos resultados das burocracias de 27 países, enquanto o esforço brasileiro se restringe a um só país. Porém, o argumento aqui não é a comparação dos recursos financeiros ou mesmo do contingente numérico de pessoas envolvidas na concepção dos projetos, mas sim as concepções em si. É visível o distanciamento da discussão brasileira tanto dos conhecimentos já assentados, como das premissas para a discussão do tema, e também quanto aos sentidos de necessidade de proteção regulatória.

O projeto brasileiro desconhece os avanços atuais sobre o tema e não parte de qualquer conceituação minimamente operacional, além de propor regular pontos ou impossíveis (como a “garantia da intervenção humana”) ou desimportantes (como a “proteção aos dados pessoais”). Ao mesmo tempo, o projeto que — frise-se — ainda sequer foi votado no Parlamento já nasce insuficiente e incapaz de responder aos anseios sociais atuais quanto ao mundo digital (Silva, 2021).

CONCLUSÃO

Soberania digital é um termo completamente diferente de “soberania” como entendido no século XX, a partir do processo de ressignificação histórica desde Jean Bodin. Enquanto o antigo conceito de soberania tinha como referentes vigiar, controlar, punir, taxar, e se referia à capacidade de controlar, em última instância, os destinos dos corpos e mercadorias dentro de determinadas fronteiras, soberania digital não permite que tais referenciais estejam presentes.

Se a analogia com o “espaço” material, que, mostrei, guiou a compreensão humana a respeito do “digital” não é suficiente para a compreensão das funcionalidades, limites e possibilidades com respeito ao mundo digital, é preciso que busquemos uma nova forma de compreensão e geração de sentido, capaz de nos ordenar os sentidos para podermos compreender e construir as sociedades a partir das transformações do século XXI.

Este artigo propõe a mudança de significação de compreensão do mundo digital da antiga analogia com um “espaço” agora digital, para uma analogia com o “tempo”. As tentativas recentes de mudança da conceituação do mundo digital, colhidas pelo mundo, mostram não somente o desconforto com a analogia do digital com o “espaço” físico, mas também os esforços epistemológicos de transformação desse entendimento. O consenso hoje é o termo “ecossistema digital”. O sentido de ecossistema introjeta a ideia de movimento, bem como de correlações e sinergias que não são unicamente compreendidas pelo seu sentido utilitário. Num ecossistema, toda existência é causa e consequência das existências com quem partilha o tempo e o espaço.

Entender o mundo digital a partir do referente tempo significa repensar as formas de soberania. Implica em pensar em novos objetos alvos de proteção do Estado. Esse caminho foi trilhado já pelas chamadas “*Big Tech*”. Enquanto os Estados seguem legislando (guiados por analogias disfuncionais) buscando proteger, por exemplo, a privacidade dos usuários e a propriedade intelectual dos grandes construtos digitais, os modelos de negócios digitais atuais pouco ou nada se importam com esses marcos. Em realidade, nem a *Meta*, a *Alphabet* ou mesmo a controladora do *Twitter*, hoje, não tem interesse algum em saber (reter, manter ou divulgar) os dados que singularizam o usuário no mundo material (nome, números de documentos, etc.). Tais informações são desimportantes ao modelo atual. O foco da lucratividade e, portanto, o objetivo da apropriação que as *Big Tech* hoje realizam é com os dados “de passagem”. Desidentificada, a brutal quantidade de dados que pode ser coletada em 24 horas dentro do território brasileiro é o verdadeiro sentido de acumulação capitalista dos negócios do mundo digital hoje. Esses dados tanto permitem produzir poderosos modelos estatísticos de comportamento e consumo, como servirão para compreender os padrões de aprendizado humano, os sentidos de tomada de decisão política, os conjuntos de referentes linguísticos a serem utilizados sobre determinado tema e — na ponta — tudo isso acaba sendo matéria-prima para o desenvolvimento de algoritmos e Inteligência Artificial.

O que pode ser visto a partir do artigo é que nenhuma dessas funções está sendo alvo da proteção do Estado. Nem do ponto de vista educacional e social (como forma de proteção

da sociedade sobre as transformações digitai) e nem mesmo de forma mercadológica, eis que ainda se toma esses dados como se fossem “produzidos por ninguém” e se entrega ao coletador (as plataformas) a propriedade deles sem nenhuma contrapartida ao Estado ou sociedade.

Na passagem do século XX para o XXI, os Estados, incapazes de compreender em profundidade o mundo digital (em grande parte pelo uso da malfadada analogia com o material), não conseguiram perceber o surgimento das “*Big Tech*”. Empresas capitalistas que dominam, exploram, controlam e manipulam o mundo digital, exercendo poder político e econômico de fato. Os efeitos do exercício destes poderes se derramam não apenas sobre o tecido digital, mas afetam o mundo material que — ao longo do século XXI — tem se tornado cada vez mais um acessório do mundo digital. Esta novidade deixou os Estados em situação indefesa ante as mudanças e transformações em operação. Notadamente no que tange ao exercício das instituições políticas e jurídicas.

Pensar a soberania digital se torna, portanto, uma das maiores necessidades no século XXI. Pensar o mundo digital a partir de conceitos e funcionalidades próprias é, hoje, a maior necessidade de um Estado. No entanto, poucos são os Estados que estão já em condições de realizar estas ações. Este artigo analisou algumas das tentativas de EUA e Brasil e nem mesmo os norte-americanos, que foram referência social, política e econômica em todo o século XX, estão hoje na vanguarda do processo de compreensão e domínio do mundo digital.

A análise dos caminhos legislativos do Brasil e dos EUA traz muitas preocupações na medida em que ambos operam ainda com base na analogia digital-material que já se mostrou insuficiente. Contudo, se nos EUA ao menos já se enxerga uma transformação conceitual nos marcos de entendimento e legislação do mundo digital, no Brasil estamos muito aquém do que se tem hoje como “estado da técnica” para conhecer, operar e regular o mundo digital. A análise dos projetos de lei em tramitação no Congresso Nacional torna essa preocupação evidente.

A conclusão da análise sugere que se comece a pensar na alteração da analogia-base de entendimento do mundo digital. Não mais um “espaço” digital em que se precisa defender os pontos de contato deste com o mundo físico (informações de individualização de usuários, documentos, endereços, etc.), mas que passemos a entender o digital como um TEMPO. O tempo que o indivíduo fica conectado à rede digital precisa ser alvo de proteção social, política e econômica. Cada vez mais os indivíduos estão conectados ao mundo digital e cada vez por mais tempo, gerando mais valor sem nada receber em troca.

Pensar em mudar a analogia significa repensar todos os marcos legais de proteção, tributação, ação e interdição. A União Europeia, por exemplo, ensaia criar uma taxação anual

a ser paga pelas empresas que operam o mundo digital pela utilização do "tempo" social da população em que está submetida à sua proteção[44]. Como se fez com os espectros e bandas eletromagnéticas, o tempo dos cidadãos digitais é agora espaço de tributação.

Da mesma forma, as proteções que o Estado precisa oferecer precisam migrar do referente espaço para o referente tempo. Não cabe mais perguntar onde está situada esta ou aquela empresa que opera o mundo digital. Deve-se atentar ao tempo que ela opera na vida dos cidadãos. Desde que o mundo digital saiu da condição de uma rede externa e passou a ser parte efetiva das nossas vidas (através do uso incessante dos PC's, *tablets*, celulares, etc.), é impossível hoje manter-se ainda preso às analogias do século XXI.

Como o referente tempo é intangível se comparado ao referente "espaço", os Estados ficam enclausurados no problema da definição do mundo digital e em como serem funcionais para proteger os direitos que historicamente lhe são obrigações de proteger. O avanço das tecnologias é tão rápido e efetivo na transformação das relações sociais e econômicas que o próprio tempo do Estado democrático para lidar com questões propostas já o torna inerte para a solução dos problemas.

A partir desse problema, vários países estão passando das tentativas de criação de leis para regulações chamadas "*soft*" com a formação de conselhos e comitês gestores, ao mesmo tempo que buscam treinar e educar sua população para o novo mundo digital (letramento digital). Qualquer tentativa do Estado hoje de operar no mundo digital que não esteja centrada essencialmente no conceito de tempo, na ideia da existência de cidadãos digitais e em um largo esforço de educação digital se torna já obsoleta pela própria velocidade de desenvolvimento da tecnologia.

É preciso que, em vez de endereços, nomes e documentos, nós protejamos todo o tempo em que o cidadão está conectado ao mundo digital. Como isso se torna impossível sem o comprometimento das próprias empresas operadoras do mundo digital, é mais viável trabalharmos na outra ponta: a educação do cidadão digital. Esta mudança é tão drástica que se pode dizer que "soberania digital" hoje se alcança com educação, pesquisa e tecnologia e não com legislação, controle e punição. E como as transformações digitais estão operando muitos prejuízos ao mundo material (violência urbana, terrorismo digital, violência sexual, fascismo, destruição das democracias) além de criarem uma nova forma de colonialismo, é preciso que o Estado encontre uma forma de fazer os lucros destas empresas financiarem todo um trabalho de reeducação e habilitação das populações analógicas a mundo digital.

O fato que causa apreensão é que o Brasil está muito atrasado nesta mudança e mesmo na compreensão do que seja o mundo digital. E isso implica em perceber que estamos nos inserindo no século XXI como nação submetida e não soberana. Como cidadãos a descoberto dos perigos do mundo digital e que não consegue nem desfrutar e nem transformar o mundo que se está transformando no século XXI. Dado que estas

44 Ver o considerando número 101 do DSA da União Europeia (*Digital Services Act*). Em princípio, serão cobradas taxas (chamadas de "taxa de supervisão") para subsidiar os custos dos Estados para manter as estruturas de fiscalização e reparação de danos a partir das ações de exploração do mundo digital europeu. Há, porém, já estudo no sentido de tornar essa uma forma nova de tributação (ver considerando 112).

transformações não são passíveis de serem bloqueadas ou atrasadas, urge um esforço de "*catching up*" para que não fiquemos em posição medieval quando o mundo todo já está na alta industrialização. Apenas aqui, para usar uma analogia que talvez possa ser explicativa do cenário atual no Brasil.

REFERÊNCIAS

ANDERSON, P. **Linhagens do estado absolutista**. 3. ed. São Paulo: Brasiliense, 1995.

BIDDLE, S. The Intercept. **Facebook engineers**: we have no idea where we keep all your personal data. 7 Sept. 2022. Disponível em: https://theintercept.com/2022/09/07/facebook-personal-data-no-accountability/. Acessado em: 24 jul. 2025.

BODIN, J. **Six books of the commonwealth**. Oxford: Liberty Library of Constittional classics, 2009.

BRASIL. **Decreto nº 10.332, de 28 de abril de 2020**. Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências. Brasília: Presidência da República, 2020.

BRASIL. **Decreto nº 10.641, de 2 de março de 2021**. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o, que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília: Presidência da República, 2021.

BRASIL. **Decreto nº 9.637, de 26 de dezembro de 2018**. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília: Presidência da República, 2018.

BRASIL. **Decreto nº 9.854, de 25 de junho de 2019**. Institui o Plano Nacional de Internet das Coisas e dispõe sobre a Câmara de Gestão e Acompanhamento do Desenvolvimento de Sistemas de Comunicação Máquina a Máquina e Internet das Coisas. Brasília: Presidência da República, 2019.

BRASIL. **Lei complementar nº 182, de 1º de junho de 2021**. Institui o marco legal das startups e do empreendedorismo inovador; e altera a Lei nº 6.404, de 15 de dezembro de 1976, e a Lei Complementar nº 123, de 14 de dezembro de 2006. Brasília: Congresso Nacional, 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acessado em: 24 jul. 2025.

BRASIL. **Lei nº 14.129, de 29 de março de 2021.** Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília: Presidência da República, 2021.

BRASIL. **Projeto de Lei n° 21, de 2020.** Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Câmara dos Deputados, 2020.

BRASIL. **Projeto de lei n° 2630, de 2020**. Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet. Brasília: Congresso Nacional, 2020.

BRASIL. **Projeto de lei nº 5051/2019**. Estabelece os princípios para o uso da Inteligência Artificial no Brasil. Brasília: Senado Federal, 2019.

BRASIL. **Projeto de lei nº 872/2021**. Dispõe sobre o uso da Inteligência Artificial. Brasília: Senado Federal, 2021.

BRATTON, B. H. **The stack**: on software and sovereignty. Londres: MIT Press, 2016.

CAMPREGHER, G. A terra é redonda: eppur si muove. **Moedas digitais** – que dinheiro é esse? 30 jun. 2025. Disponível em: https://aterraeredonda.com.br/moedas-digitais-que-dinheiro-e-esse/. Acessado em: 25 jul. 2025.

CHESTERMAN, S. **We, the robots?** regulating artificial intelligence and the limits of the law. Cambridge: Cambridge University Press, 2021.

CHIGNOLA, S. Homo homini trigris: Thomas Hobbes and the global images of sovereignty. **Philosophy and Social Criticism**, [*s. l.*], v. 48, n. 5, p. 726-754, 2021.

COMITE DAS REGIÕES EUROPEU. **Relatório do grupo de alto nível para a democracia europeia**. Bruxelas: União Europeia, 2022. Disponível em: https://cor.europa.eu/en/news/Pages/Report-of-the-High-Level-Group-on-European-Democracy.aspx. Acessado em: 17 ago. 2025.

EISENBERG, J.; CEPIK, M. (org.). **Internet e política:** teoria e prática da democracia eletrônica. Belo Horizonte: Editora UFMG, 2002.

EUROPEAN COMMISSION. **2021/0106 (COD)**. Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on Artificial Intelligence (Artificial Intelligence act) and amending certain union legislative acts. Brussels: European Commission, 2021. Disponível em: https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence. Acessado em: 28 jul. 2025.

EUROPEAN UNION. **EUR-Lex**. 27 Oct. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014. Acessado em: 24 jul. 2025.

FANG, B. **Cyberespace sovereignty:** reflections on building a community of common future in cyberspace. Pequim: Springer, 2018.

GIBSON, W. **Neuromancer**. São Paulo: Aleph, 1984.

HOBBES, T. **Leviathan**. London: Green Dragon, 1651.

INTERNET CORPORATION FOR ASSIGNED NAMES AND NUMBERS. ICANN. **Policy development**: how domain name system policy is developed, and how you can get invoved. [*S. l.*]: ICANN, 2021. Disponível em: https://www.icann.org/en/system/files/files/icann-policy-development-report-16jun21-en.pdf. Acessado em: 24 jul. 2025.

KANT, I. À paz perpétua: um projeto filosófico. 2. ed. Petrópolis: Vozes, 2020.

KAZEEM, Y. **The cost of internet access dropped everywhere in the world last year**—except in Africa. 21 Mar. 2019. Disponível em: https://finance.yahoo.com/news/cost-internet-access-dropped-everywhere-112424571.html. Acessado em: 24 jul. 2025.

KOKAS, A. **Trafficking data:** how China is winning the battler for digital sovereignty. Nova Iorque: Oxford University Press, 2023.

MCCALLUM, S. Meta settles Cambridge Analytica scandal case for $725m. **BBC**. 23 Dec. 2022. Disponível em: https://www.bbc.com/news/technology-64075067. Acessado em: 24 jul. 2025.

MOSCO, V. **Becoming digital**: toward a post-internet society. Londres: Emerald Publishing Limited, 2017.

MOSCO, V. **Digital sublime**: myth, power and cyberspace. Londres: MIT Press, 2004.

NATIONAL INITIATIVE FOR CYBERSECURITY CAREERS AND STUDIES. NICCS. Cybersecurity and career resources. **Vocabulary**. c2025. Disponível em: https://niccs.cisa.gov/cybersecurity-career-resources/glossary#C. Acessado em: 24 jul. 2025.

NEMER, D. **Tecnologia do oprimido:** desigualdade o mundano digital nas favelas do Brasil. Vitória: Editora Milfontes, 2022.

NORTON, W. B. DrPeering international. **Internet transit prices** - historical and projected. c2014. Disponível em: https://drpeering.net/white-papers/Internet-Transit-Pricing-Historical-And-Projected.php. Acessado em: 25 jul. 2025.

ONE HUNDRED FOURTH CONGRESS OF THE UNITED STATES OF AMERICA. **Telecommunication services**. Begun and held at the City of Washington on Wednesday, the third day of January, one thousand nine hundred and ninety-six An Act To promote competition and reduce regulation in order to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies. Washington: Congress, 1996. Disponível em: https://transition.fcc.gov/Reports/tcom1996.pdf. Acessado em: 25 jul. 2025.

PANI, S. K.; PANDEY, M. (ed.). **Internet of things:** enabling technologias, security and social implications. Singapura: Springer, 2022.

PUYVELDE, D.; BRANTLY, A. **Cybersecurity:** politics, governance and conflict in cyberspace. Medford: Polity Press, 2019.

SANT'ANA, J.; FALCÃO, M.; VIVAS, F. **G1**. **Politíca**. Moraes determina bloqueio do aplicativo de mensagens Telegram em todo o Brasil. 18 mar. 2022. Disponível em: https://g1.globo.com/politica/noticia/2022/03/18/moraes-determina-bloqueio-do-aplicativo-de-mensagens-telegram-em-todo-o-brasil.ghtml. Acessado em: 24 jul. 2025.

SCHMIDT, C. **Political theology:** four chapters on the concept of sovereignty. Chicago: Chicago University Press, 2005.

SILVA, T. **Racismo algoritmico:** inteligência artificial e discriminação nas redes digitais. São Paulo: Edições SESC, 2021.

TURING, A. Computing machinery and intelligence. **Mind**, [*s. l.*], v. 49, n. 236, p. 433-460, 1950.

U. S. SENATE COMMITTEE ON THE JUDICIARY. **Senate judiciary committee releases testimony of twitter whistleblower peiter "Mudge" Zatko**. 13 Sept. 2002. Disponível em: https://www.judiciary.senate.gov/press/dem/releases/senate-judiciary-committee-releases-testimony-of-twitter-whistleblower-peiter-mudge-zatko. Acessado em: 24 jul. 2025.

UNIÃO EUROPEIA. Parlamento Europeu. Conselho da União Europeia. **Regulamento (UE) 2022/2065**, de 19 de outubro de 2022. Relativo a um mercado único para os serviços digitais e que altera a Diretiva 2000/31/CE (Regulamento dos Serviços Digitais). ***Jornal Oficial da União Europeia***, L 277, p. 1–102, 27 out. 2022. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32022R2065. Acessado em: 24 jul. 2025.

UNITED STATES. Court of appeals for the Ninth Circuit. Petition for a writ of certiorari filed. **No. 21-1333**. Julgado em: 22/06/2021. Disponível em: https://www.supremecourt.gov/docket/docketfiles/html/public/21-1333.html. Acessado em: 25 jul. 2025.

UNITED STATES. **The National Estrategy to secure cyberspace**. Washington: The White House, 2003. Disponível em: https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf. Acessado em: 24 jul. 2025.

WENDT, A. **Quantum mind and social science:** unifying physical and social ontology. Cambridge: Cambridge University Press, 2015.

ZUBOFF, S. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Nova Iorque: Perseus Books, 2019.