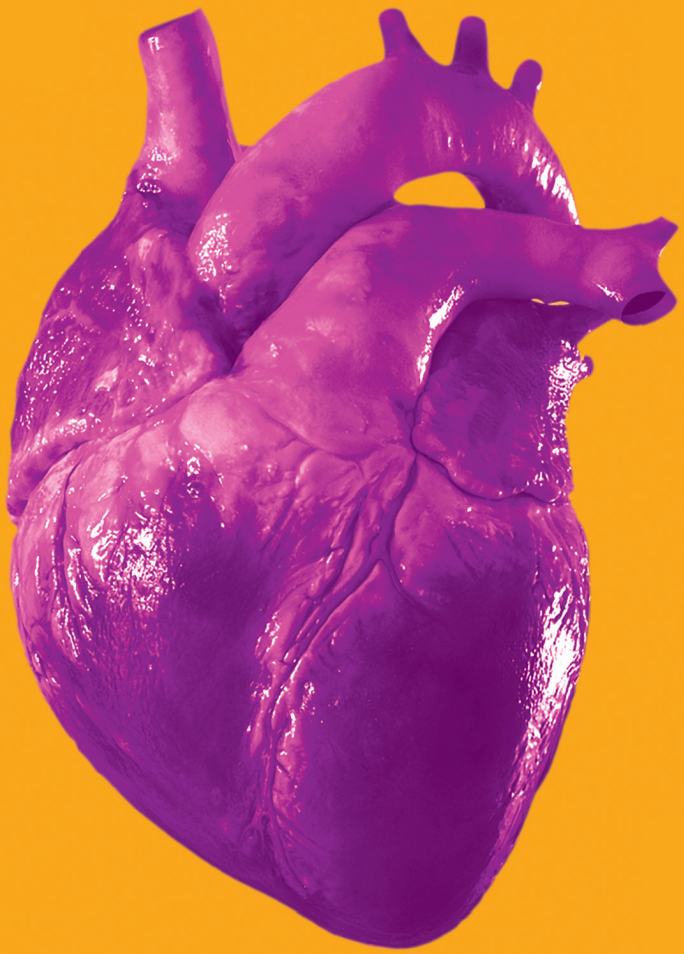
Nesta edição - Sam Lanfranco & Klaus Stoll, Bruna Santos

POLITICS

Uma publicação do Instituto Nupef Ano XII | nº31 | abr-jul 2021



Distribuição gratuita

A Declaração Universal dos Direitos Humanos na era digital primeira parte

+

Uma avaliação do Modelo de Responsabilidade de intermediários do Marco Civil para o desenvolvimento da Internet no Brasil pág. 65

POLITICS
Uma publicação do Instituto Nupef | abril-julho 2021 | https://nupef.org.br

31
ANO XIII

instituto nupef

POLI**TICS** 31 | Ano XIII | abril-julho de 2021

Todas as edições da POLITICS estão disponíveis em https://politics.org.br

Se você quiser receber gratuitamente a edição impressa da revista, envie um e-mail para politics@nupef.org.br com seu nome, endereço completo - incluindo o CEP - e a sua área de atuação.

Uma publicação do Instituto Nupef
https://nupef.org.br

ISSN: 1984-8803

Editorial

A humanidade sofreu as graves consequências de duas guerras mundiais no século 20. Com a derrota da Quádrupla Aliança pela Entente em 1918, a primeira Conferência de Paz do século em 1919 e 1920, em Paris, resultou em cinco tratados que reorganizaram o mapa da Europa e na criação, em janeiro de 1920, da Liga das Nações – a primeira organização mundial intergovernamental, que durou 26 anos. Já era parte da missão da Liga a defesa de direitos humanos, mas o objetivo era evitar que novos confrontos mundiais fossem desencadeados.

O fracasso da Liga (que chegou a ter 58 países membros) ficou evidente quando o conflito mais mortal da história humana, a Segunda Guerra Mundial, foi desatado em 1939 com a invasão da Polônia pela Alemanha. O término da guerra levou a um novo esforço de criação de uma estrutura com o objetivo de manter a paz e segurança internacional. Uma reunião em San Francisco com a participação de 50 países em abril de 1945 definiu as bases da Carta das Nações Unidas, e da estrutura intergovernamental para fazer valer os acordos de paz e os objetivos da Carta. Em outubro de 1945 a Organização das Nações Unidas começou a funcionar com 51 países membros.

Três anos depois, em dezembro de 1948, a Assembleia Geral da ONU aprovou a Declaração Universal dos Direitos Humanos (DUDH), com a adesão de 48 de seus 58 membros (oito abstenções e dois países que não votaram), pilar do desenvolvimento de uma legislação internacional de defesa de direitos humanos e referência para a Carta Internacional de Direitos Humanos – a Resolução 217-III da Assembleia Geral (1966) que integrou o Pacto Internacional dos Direitos Civis e Políticos e o Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais à DUDH. É o mais abrangente consenso intergovernamental mundial da história sobre direitos da cidadania.

O primeiro texto desta edição enfrenta um grande desafio: buscar os enlaces entre a base essencial de direitos representada pela DUDH e como esses direitos podem valer para a cidadania no espaço digital do ecossistema da Internet. Sam Lanfranco e Klaus Stoll exploram esse desafio, e aqui publicamos as primeiras seis partes de seu trabalho, analisando em detalhe os 19 primeiros artigos da DUDH no contexto da governança da Internet, resultado de uma pesquisa ainda em progresso.

Serviços de livre entrada e custo zero para os usuários, financiados por terceiros com base no acesso a preferências desses usuários no modo em que usam esses serviços – uma circularidade que ninguém imaginava tornar-se um negócio trilionário, obedecendo rigorosamente a "lei dos grandes números": um pequeno conjunto dominante desses

serviços (Facebook, Twitter, Instagram, Whatsapp, Youtube, entre outros) com centenas de milhões ou mesmo bilhões de usuários eventualmente prestando atenção em anúncios em suas telas e, em uma pequena porcentagem que significa centenas de milhões de cliques a cada segundo, eventualmente visitando a oferta de um anúncio e gerando uma porcentagem para o dito serviço gratuito.

Nesse processo eses serviços acumulam dados dos perfis de navegação dos usuários, um produto à venda para outros agentes ou para o próprio serviço – que direciona anúncios ou mensagens a cada usuário conforme seu comportamento traduzido em interesses pessoais online. Ainda mais, no trajeto entre o dispositivo do usuário e qualquer serviço da Internet, seu tráfego pode ser interceptado por provedores para acumular (e lucrar com) perfis de navegação.

As consequências da gratuidade no acesso a serviços nessas plataformas são resumidas nesse novo Termo de Serviços do Youtube: "o YouTube tem o direito de monetizar todos conteúdos na plataforma e anúncios podem aparecer em vídeos de canais que não estão no Programa de Parcerias do YouTube".[1]

Acrescente-se a esse universo de serviços os aplicativos de e-serviços (mobilidade, alimentação) que usufruem do trabalho de pessoas sem nenhum seguro ou obrigação trabalhista, criando uma legião de novos super-explorados da sociedade digitalizada.

O Marco Civil da Internet (MCI) é construido em torno de dois componentes da Internet: "provedores de conexão" e "provedores de aplicações de Internet". Este segundo componente já representava uma grande complexidade quando da sanção do MCI em 2014. Hoje isso traduz-se em empresas operadoras de serviços de rede social diversificados envolvendo uma cadeia de responsabilização setorial e transfronteiras que representa o maior desafio regulatório da governança da Internet. Como descreve Rana Dasgupta:

> *O exemplo icônico é a [empresa] Facebook, uma concentração repentina de US$700 bilhões quase totalmente isolada da população em geral: não apenas a propriedade é controlada, mas o emprego está confinado a equipes compactas de especialistas altamente pagos. Como seus pares do Vale do Silício, a Facebook disfarça o lucro e o transfere para o exterior, para que sua riqueza não se infiltre na sociedade por meio de impostos. A empresa pagou em média 10,2% em impostos na última década. As consequências negativas disso não afetam a Facebook: ela vende quase que exclusivamente para outras empresas e, portanto, não depende diretamente de consumidores abastados. E ainda assim, suas vendas e avaliação seriam zero sem os usuários, todos os quais doam a matéria-prima da empresa – seus dados pessoais – gratuitamente. Os usuários do [aplicativo] Facebook gastam bilhões de horas enviando dados, mas esse trabalho é disfarçado de consumo e não há indícios de compensação.*[2]

É essa complexidade técnica e jurídica da responsabilização de intermediários que o estudo de Bruna Martins dos Santos esmiuça com grande cuidado, atualidade e qualidade.

1. Ver *https://www.youtube.com/static?template=terms*
2. Rana Dasgupta, "The Silence Majority", Harper's Magazine, dezembro de 2020, *https://harpers.org/archive/2020/12/the-silenced-majority/*

Neste meio século não parece que os governos tenham feito pelos direitos humanos tudo aquilo a que moralmente estavam obrigados. As injustiças multiplicam-se, as desigualdades agravam-se, a ignorância cresce, a miséria alastra. A mesma esquizofrénica humanidade capaz de enviar instrumentos a um planeta para estudar a composição das suas rochas, assiste indiferente à morte de milhões de pessoas pela fome. Chega-se mais facilmente a Marte do que ao nosso próprio semelhante.

José Saramago, ao receber o Prêmio Nobel em 10 de dezembro de 1998, por ocasião do 50º aniversário da Declaração Universal dos Direitos Humanos.[1]

1. Citado por Monica de Bolle, "Esquizofrênica humanidade", em https://www.quatrocincoum.com.br/br/colunas/rupturas/esquizofrenica-humanidade

Sam Lanfranco & Klaus Stoll*

A Declaração Universal dos Direitos Humanos na Era Digital (primeira parte)

PARTE 1: FUNDAÇÕES

A governança da Internet, como toda governança, precisa de princípios orientadores a partir dos quais a formulação de políticas e o comportamento aceitável são derivados. A identificação dos princípios fundamentais para orientar a formulação de políticas do ecossistema da Internet em torno da cidadania digital e da integridade das práticas e comportamentos digitais pode e deve começar com a Declaração Universal dos Direitos Humanos (DUDH), adotada após a Segunda Guerra Mundial (1948) para proteger os direitos das pessoas no espaço literal. Estamos agora enfrentando o mesmo desafio em relação ao espaço digital.

Este é um trabalho em progresso, motivado pelo 72º aniversário da DUDH, que pretende contribuir para uma discussão em todo o ecossistema da Internet em torno dos direitos digitais e do desenvolvimento de políticas do ecossistema da Internet.[2] O objetivo é contribuir para iniciativas em direção a um muito necessário Pacto Internacional sobre Direitos Civis e Políticos, Econômicos, Sociais e Culturais digitais.

*Os originais deste texto foram publicados em inglês em CircleID (http://circleid.com) a partir de dezembro de 2019. Sam Lanfranco é professor emérito e sênior, York University, Toronto. Klaus Stoll é consultor em tecnologia da informação e governança da Internet. Os autores contribuíram para este artigo apenas para fins de discussão e exclusivamente a título pessoal, e agradecem a Sarah Deutsch por suas valiosas contribuições para o texto. Esta versão em português foi traduzida e adaptada por Carlos A. Afonso, do Instituto Nupef.

2. Comentários são bem-vindos. Envie comentários com "DUDH" na linha de assunto para *klausstoll@thebro* casgroup.com. Os comentários serão usados para atualizar esta discussão sobre direitos digitais em artigos subsequentes.

Pode-se pensar que os autores da DUDH tinham a Internet em mente quando declararam no Artigo 19:

> ***Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e ideias por qualquer meio de expressão.***[3]

Todos os seres humanos têm certos direitos e não faz diferença se optam por exercê-los em uma praça ou sala de *chat* na Internet. A governança da Internet, como toda governança, precisa ser fundada e orientada pela DUDH. Esta é a primeira parte de uma série de artigos que discutem os princípios e suas aplicações reais no mundo digital. Nesta primeira parte são analisados os valores e princípios essenciais. Nas partes a seguir, examinaremos cada um dos primeiros 19 artigos da DUDH.

FUNDAÇÕES

A legitimidade de um governo pode ser medida pelo grau em que sua governança adere aos princípios contidos na DUDH.[4] A primeira frase do Preâmbulo define a agenda para a DUDH como um todo:

> ***Considerando que o reconhecimento da dignidade inerente a todos os membros da família humana e dos seus direitos iguais e inalienáveis constitui o fundamento da liberdade, da justiça e da paz no mundo...***

A DUDH evoca os valores que são de fundamental importância para o ser humano, como dignidade, igualdade, liberdade e paz. Também descreve os instrumentos pelos quais esses valores devem ser realizados, incluindo a justiça, os tribunais, a lei e as estruturas sociais em que ocorrem.

Nações e Estados podem ir e vir. Os princípios fundamentais que governam nossa humanidade comum, tal como inscritos na DUDH, permanecem inalterados. A DUDH é a referência pela qual a governança é medida para cada nação nova e antiga.

A intenção deste texto não é interpretar a DUDH novamente à luz das tecnologias digitais, mas explorar como a DUDH informa o desenvolvimento da governança, dignidade e integridade de nosso ser na era digital.

PAÍS, NAÇÃO E ESTADO

A DUDH usa os termos "país", "nação" e "Estado" repetidamente e precisamos revisar suas funções e definições antes de prosseguirmos com sua aplicação ao ciberespaço do ecossistema da Internet.

Um ***país*** é comumente entendido como um território geográfico definido e reconhecido dentro do qual as pessoas vivem de acordo com um conjunto de regras juridicamente vinculativas, que são definidas por seus próprios processos de governança. Uma ***nação*** pode existir dentro ou além das fronteiras geográficas. Pode ser definida como uma comunidade de pessoas com base em fatores políticos, econômicos, geográficos, étnicos, religiosos e outros. O termo nação nem sempre refere-se a um país. A diferença importante entre um país e uma nação é que uma nação pode não ter seu próprio poder de governo e soberania.[5] Um ***Estado*** é uma entidade política representada por um governo centralizado que tem soberania sobre uma área geográfica.[6]

3. As citações dos textos da DUDH são as originais da versão oficial em português da ONU. Notamos que o texo da DUDH não está de acordo com as noções contemporâneas de linguagem neutra em termos de gênero.
4. Conforme proclamado pela Assembleia Geral das Nações Unidas em Paris em 10 de dezembro de 1948 (resolução 217 A da Assembleia Geral). Ver *https://www.un.org/en/universal-declaration-human-rights*. A DUDH resultou em 1976 em dois importantes pactos internacionais que desenvolveram os direitos consagrados na DUDH e os tornaram vinculativos para os Estados que ratificaram a Declaração. O Pacto Internacional sobre Direitos Civis e Políticos *(https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx)* e o Pacto Internacional sobre Direitos Econômicos, Sociais e Culturais *(https://www.ohchr.org /en/professionalinterest/pages/cescr.aspx)*. Os convênios e a UHDR juntos constituem a Carta Internacional de Direitos Humanos *(https://www.ohchr.org/Documents/Publications/Compilation1.1en.pdf)*.
5. Um país pode ser uma nação, por exemplo, França, Japão e Alemanha. O Reino Unido é uma nação de países, consistindo, por enquanto, na Inglaterra, País de Gales, Escócia e Irlanda do Norte. Uma nova nação celta, consistindo de Irlanda, País de Gales e Escócia, pode ser criada como um resultado possível do Brexit.
6. Ver *https://en.wikipedia.org/wiki/Sovereign_state*. Para diferenciar o Estado (ou estado-nação) como unidade política de outros significados da palavra "estado" (inclusive do estado como unidade de uma federação ou divisão política e territorial de um país), o primeiro é apresentado neste texto com inicial maiúscula.

As descobertas intelectuais e os avanços tecnológicos são fatores impulsionadores da mudança social. Se as oportunidades de usá-los para aumentar a segurança e proteção forem percebidas como significativas o suficiente, resultarão em mudanças na estrutura social. As oportunidades são frequentemente percebidas como disruptivas e revolucionárias (como, por exemplo, a "revolução industrial"), mas dão origem ao nascimento de novas nações. A revolução pode ser violenta ou não violenta, mas nunca resulta em estase. Essas "revoluções" permitem que as pessoas alterem o antigo Estado para supostamente criar um novo Estado que projeta-se para ser mais eficaz na garantia da segurança e da prosperidade. As tecnologias digitais, com sua promessa de segurança e prosperidade exponencialmente aumentadas, causaram um grande transtorno ao introduzir técnicas que transcenderam e redefiniram muitos dos fatores característicos de um país, nação ou Estado existente.[7]

Ser membro da ONU é visto como um reconhecimento da soberania e do Estado. Embora a ONU seja uma união de nações, ela está centrada nas pessoas e vê seu papel como representante dos interesses das pessoas que estão sujeitas à governança, e não dos próprios governos. A DUDH vê o país, a nação e o Estado como o veículo apropriado para proteger a vontade de seu povo, para promover a melhor ordem social possível que sirva às necessidades e direitos das pessoas de acordo com os princípios da DUDH.

A NAÇÃO DIGITAL: O ECOSSISTEMA DA INTERNET E O CIBERESPAÇO

As tecnologias digitais estão propagando mudanças que muitas vezes desafiam diretamente os antigos valores percebidos, incluindo aqueles da DUDH . Por exemplo, a presença pessoal de alguém no ciberespaço pode usufruir de poucos ou nenhum direito aos dados pessoais, se os usuários de dados ignorarem os direitos de privacidade da DUDH com base em noções de "inovação digital não regulamentada".[8]

O alcance global em expansão do ecossistema da Internet (ciberespaço) e o acesso mais barato e mais fácil proporcionaram a bilhões de pessoas uma residência digital no ecossistema da Internet. Clique a clique, soundbite a soundbite e quadro a quadro, comunidades humanas digitais estão se formando, e a noção de uma "persona digital" separada e uma "cibernação" global multifacetada cada vez mais poderosa coexistem nesse ecossistema.

A cibernação emergente está adquirindo as propriedades de uma nação física, como uma comunidade diversa, tanto dentro dos Estados quanto em nível global. Dentro dos Estados, as cibernações podem estar sujeitas à governança do Estado, como no caso do Regulamento Geral de Proteção de Dados (GDPR) da União Europeia (UE). O GDPR também se aplica fora das fronteiras normais para cidadãos da UE que podem viver fora da UE. A ampla linguagem regulatória do GDPR não está apenas afetando os direitos de privacidade na UE, mas também tendo um efeito extraterritorial.[9] Sem um sistema global de governança eficaz, o ciberespaço ainda está em busca de sua "soberania".

É preciso agora olhar para o papel do ser humano individual na nação digital. É preciso revisar o papel da DUDH como um auxílio à navegação para incorporar os direitos digitais das pessoas à governança estatal e para desenvolver os direitos e obrigações das pessoas na governança global dos ciberespaços do ecossistema da Internet.

A PERSONA DIGITAL

Os avanços trazidos pelas tecnologias digitais criaram uma nova dimensão multifacetada para nossas personas digitais.[10] Nossa persona física é

7. O que torna as descobertas intelectuais e os avanços tecnológicos das tecnologias digitais tão extraordinários é que eles criaram um reino que é físico e virtual. Criado por meio de infraestrutura física, ele cria um mundo virtual para a existência e interação de personas digitais.
8. Práticas digitais predatórias como essas e muitas outras serão discutidas em detalhe na próxima parte deste texto.
9. Ver https://gdpr-info.eu. As tentativas dos Estados de lidar com as difíceis "regras" da Internet, seja para fins de privacidade, responsabilidade, segurança ou outros fins regulatórios, podem ter um efeito de transbordamento jurisdicional, dado que a Internet é conectada globalmente.
10. Persona digital é aqui definido como qualquer conjunto de dados de transações, comportamentais e ambientais constituidos para atribuir características à pessoa, a serem usadas para fins econômicos, políticos, sociais ou outros. A constituição dessa persona pode ser por simples agregação de dados ou usando algoritmos de inteligência artificial.

algo que nos foi dado a partir de nosso nascimento. Nossas personas digitais são criadas por tecnologias digitais.[11] Em paralelo à nossa persona física, com muito poucas exceções, as pessoas estão adquirindo simultaneamente várias personas digitais.[12] Elas consistem em construções de dados digitais (personas) que estão ligadas ao nosso ser literal único como um humano.[13] Frequentemente associados a essas personas digitais estão julgamentos de valor impostos por humanos ou máquinas que afetam a reputação de alguém no mundo real, informações pessoais, crédito, risco e outrras características que afetam o bem-estar humano básico.

A tecnologia constrói nossas personas digitais a partir de dados reunidos de uma infinidade de fontes. Podemos nunca ser expostos ou usar tecnologias digitais. A ampla coleta e processamento de dados, todos e quaisquer dados, dão origem às nossas personas digitais. Várias versões da personalidade digital de uma pessoa podem ser construídas por outras pessoas por meio de montagem de dados e algoritmos de inteligência artificial (IA), que são contrários aos princípios da DUDH. A questão principal aqui é: quem tem direito aos dados digitais de uma pessoa e seus usos? Como os princípios da DUDH ditam os direitos e deveres digitais da pessoa e de outras pessoas? A DUDH determina que todos têm direito à liberdade e segurança em sua personalidade física. Como isso se estende às personas digitais?

Negar os direitos de alguém no ciberespaço pode significar confinamento, isolamento ou até encarceramento digital. Estruturas emergentes de governança digital devem ser empregadas para proteger os direitos de uma persona digital no ciberespaço. Deve-se ter direitos de propriedade em relação aos próprios ativos digitais no ciberespaço, incluindo as personas digitais construídas por terceiros e as interações com outras no ciberespaço. O engajamento digital deve podeer ser realizado com segurança e com proteção para a pessoa física e digital.[14]

CIDADANIA DIGITAL

Hoje, o ciberespaço confere a cada um de nós uma cidadania dupla, mas inseparável, física e digital. Mesmo que não conheçamos o ciberespaço, ou não possamos ou decidamos não usar nenhuma das tecnologias digitais, ainda somos cidadãos digitais com direitos (e correspondentes deveres). Nossas vidas, de uma forma ou de outra, são afetadas por essa cidadania.[15] Pensada a partir da DUDH, a cidadania digital vem com direitos fundamentais que toda pessoa física e digital deve desfrutar. O projeto de sistemas de governança digital para consagrar isso é uma tarefa urgente.

DIREITOS E DEVERES

Direitos não vêm sem deveres ou obrigações. A DUDH nos lembra que os direitos e liberdades que desfrutamos como seres humanos em nossa cidadania física, e agora digital, não são ilimitados. Essas funções fundamentais são referenciadas em toda a DUDH. O artigo 1 as resume e generaliza. Os seres humanos são "dotados de razão e consciência" e devem exercer ambas em relação aos outros "em espírito de fraternidade". A liberdade e igualdade, dignidade e direitos de uma pessoa são limitados pela liberdade e igualdade, dignidade e direitos do resto da humanidade.

11. Por exemplo, humanos nascidos em tribos nativas que vivem sem contato com o mundo fora de seu território tribal. Mesmo um eremita em sua caverna sem contato externo pode ter uma identidade digital criada a partir de dados de outras pessoas sobre ele.
12. Nossa persona digital poderia ter sido criada antes de nosso nascimento físico, usando dados gerados e processados conforme nossos pais anunciavam e discutiam nossa chegada iminente com familiares e amigos online.
13. Nossa persona digital é baseada em três tipos de dados:
- dados ambientais: obtidos por meio da Internet das coisas (IoT), GPS e outros dispositivos de rastreamento, dados públicos (CCTV) e dispositivos móveis, como o telefone móvel;
- dados comportamentais: obtidos de perfil de navegação, mídia social, mensagens (SMS), e-mail etc;
- dados transacionais: obtidos por meio de compras, vendas e compras online, transações financeiras etc.

14. O mundo físico está cheio de perigos que ameaçam nossa personalidade e a necessidade de segurança é uma das motivações motrizes das sociedades humanas. Da mesma forma, o ciberespaço é um lugar perigoso que pode prejudicar a personalidade física e digital. Muitos dos perigos no ciberespaço são apenas perigos que já conhecemos no mundo físico e que foram transferidos por meios digitais para o ciberespaço. Outras ameaças à nossa segurança são mais específicas do ciberespaço.
15. Para o propósito deste texto, falamos em cidadania física e digital quando nos referimos à cidadania específica para essas esferas. Hoje, todos têm cidadania em ambas. Quando falamos sobre "cidadãos", está implícito que esses cidadãos são cidadãos de ambas esferas.

INTEGRIDADE DIGITAL

A liberdade é um elemento central da dignidade humana, assim como a igualdade é um elemento central dos direitos. Liberdade e igualdade são pré-requisitos para a integridade física e digital de uma pessoa.[16] Se uma pessoa não tem a liberdade e a capacidade de controlar dados pessoais, ela pode se deparar com verdadeiros monstros de Frankenstein digitais, montadas a partir de dados como "partes do corpo" de várias fontes, frequentemente de origem duvidosa. Essas personas podem ser imprecisas, criadas sem a permissão da pessoa física e não ter integridade. Uma multidão de falsas personas digitais pode surgir e minar a integridade de uma pessoa, nenhuma delas tendo qualquer fidelidade ao seu verdadeiro eu literal e digital.

A ausência de integridade de dados pessoais compromete a dignidade física e digital, a igualdade e os direitos de uma pessoa e sua capacidade de estar sujeita à razão e à consciência no espírito de fraternidade.[17] Dados errôneos, não verificados, podem ter consequências terríveis em termos de persona virtual e vida no mundo real. Mesmo os dados corretos processados por meio de um algoritmo não transparente podem, em sua aplicação, ser prejudiciais para as pessoas nos mundos virtual e físico.[18]

SEPARADOS, MAS INSEPARÁVEIS

Liberdade e igualdade, dignidade e direitos são valores humanos fundamentais individualizados que não podem ser separados. Da mesma forma, nossas personas físicas e digitais, nossa residência em um país, nação e ciberespaço, e nossa dupla cidadania, são individualizadas mas não podem ser separadas. São interdependentes e constantemente exercem influência uma sobre a outra. A liberdade e a igualdade, a dignidade, os direitos e os instrumentos resultantes de que uma pessoa literal desfruta têm existência paralela para as personas digitais.[19] A governança em torno da existência paralela das personas digitais ainda está em evolução, e é o desafio que temos hoje.

GOVERNANÇA DA INTERNET: O CIBERESPAÇO A CAMINHO DA "SOBERANIA"

A governança, na forma de processos de formulação de políticas autorizadas, leis e regulamentações resultantes, está em sua infância no ciberespaço.[20] O vácuo existente é preenchido pelos esforços de governos para exercer uma percepção de soberania sobre a "cidadania" das pessoas no ciberespaço. Parte do argumento é que os cidadãos precisam de proteção contra danos e parte é para apoiar as estratégias de negócios digitais de terceiros. Existem pressões conflitantes aqui. Além disso, a soberania do Estado é limitada à sua autoridade sobre os cidadãos no contexto do Estado. As pessoas agora têm uma segunda forma maior de cidadania no ciberespaço global. Leis e regulamentos que não reconhecem a natureza dual da cidadania digital são, na melhor das hipóteses, um esforço incompleto para regulamentar e proteger os direitos e deveres da cidadania digital. Além da articulação de políticas domésticas de cidadania digital adequadas, não há como superestimar a necessidade e a urgência de avançar na governança do ecossistema global da Internet.

Alguns grupos de interesse, especialmente aquelas que dependem de práticas de negócios digitais que exploram o acesso a dados, se opõem ao uso da DUDH como uma referência para políticas que protegem os direitos da cidadania digital nacional.

16. Integridade digital é aqui definida como o estado em que uma pessoa detém todos os seus dados pessoais e tem controle sobre como esses dados são reunidos para personas digitais e seus usos.
17. Existem dois componentes para a integridade dos dados. O primeiro é sobre as propriedades dos dados – são relevantes para caracterizar esses dados? A segunda é sobre os usos dos dados – os usos atendem aos princípios de propriedade de dados, acesso a dados e uso de dados conforme descritos na lei e geralmente associados ao comportamento do usuário?
18. Por exemplo: uma criança diagnosticada ao nascer com um problema de saúde grave pode enfrentar custos de saúde sem os benefícios dos riscos combinados do seguro saúde. A existência desses dados e seu uso em algoritmos não transparentes disponíveis para seguradoras, governos, escolas e empregadores (ou o que a legislação permitir) afetará todos os aspectos da existência da pessoa, do nascimento à morte.
19. No restante do texto, persona refere-se à persona física e digital; cidadão significa cidadão físico e digital; e *cidadania* é definida como sujeita simultaneamente a direitos e responsabilidades físicas e digitais.
20. Por exemplo: ICANN, IGF, WEF, WSIS.

Essas partes argumentam que os regulamentos que restringem o uso de dados sufocarão a inovação digital. Alguns interesses comerciais (e políticos) no ciberespaço pressionam por inovação irrestrita nas práticas de negócios digitais. Os governos, no entanto, estão cada vez mais descartando argumentos para "inovação não regulamentada" e, em vez disso, estão respondendo com mais regulamentação, com suas consequências indesejadas.

O ciberespaço global ainda não pode reivindicar o status de um Estado soberano. Ainda falta uma estrutura de governança e uma rubrica para determinar como os cidadãos, entidades e governos participam de estruturas de governança multilaterais ou pluralistas. Os domínios do ciberespaço precisam de regras e regulamentos que governem os processos e equilibrem os direitos do indivíduo e os da comunidade.[21] Todos os cidadãos no mundo físico têm direitos sociais e, da mesma forma, os cidadãos digitais têm igual direito a alguma forma de governança global da Internet adequada e responsável. Precisamos construir estruturas de governança digital equivalentes que respondam pelo interesse de todos os setores globais, sejam eles pessoas, entidades ou Estados.

Fazer da DUDH a base da governança da Internet é o primeiro passo para garantir os direitos e obrigações digitais em um ecossistema global da Internet com integridade. Os esforços para criar estruturas de governança da Internet justas e autorizadas podem começar examinando a DUDH como uma ferramenta de referência universal e confiável para sinalizar direitos e deveres digitais e destacar áreas e questões onde o ciberespaço da Internet apresenta desafios. Precisaremos de um diálogo multilateral e pluralista contínuo para dar corpo à definição de vários direitos e deveres digitais e à construção de estruturas de governança da Internet.

É chegado o momento da comunidade da Internet explorar a aplicação potencial da DUDH para abordar as principais proteções para a cidadania e para a governança do ecossistema global da Internet.

PARTE 2: ARTIGOS 1-5

A governança digital, como toda governança, precisa ser fundamentada em princípios orientadores dos quais toda formulação de políticas deriva. Não há princípios mais fundamentais para orientar nossa formulação de políticas do que a DUDH. O texto anterior explora os fundamentos da Declaração. Esta parte discute os Artigos 1-5 que enfocam a liberdade humana, igualdade, dignidade e direitos.

NASCIMENTO

Artigo 1: Todos os seres humanos nascem livres e iguais em dignidade e em direitos. Dotados de razão e de consciência, devem agir uns para com os outros em espírito de fraternidade.

Nós nascemos nesta Terra. Não participamos da decisão que nos tornou seres humanos, cidadãos e cidadãs do planeta. Hoje já nascemos com uma identidade digital e com o início das personas digitais multifacetadas que estão associadas a ela. Nossa presença digital pode ter começado antes do nosso nascimento físico, quando nossos pais anunciaram e discutiram online nossa chegada iminente com a família e amigos. Configuradas a partir de uma miríade de fontes, nossas personas digitais consistem nos dados digitais que estão associados a nós, cada persona construída por outros, para seus próprios fins.

Mesmo para uma pessoa que nunca usa tecnologias digitais, existe uma identidade digital e personas, com base em dados que foram coletados por meios que não requerem a intervenção da pessoa. Dentro da nuvem de dados da Internet residem mais do que apenas nossas ações digitais deliberadas (atividade de compra, banco etc). Nossas personas digitais são construídas com uma mistura de dados comportamentais observados e dados ambientais que não controlamos.

A nuvem de dados que cerca um ser humano e a persona digital, gerada por algoritmos a partir desses dados, são separadas, mas inseparáveis.[22]

21. O artigo 28 da DUDH apoia esta noção: "Todos têm direito a uma ordem social e internacional na qual os direitos e liberdades estabelecidos nesta Declaração possam ser plenamente realizados".

22. Dados incorretos podem ter consequências terríveis em termos de persona virtual de alguém, mas mesmo dados corretos podem ser problemáticos no sentido literal. Por exemplo: uma criança diagnosticada ao nascer com um problema de saúde grave pode enfrentar custos de saúde sem os benefícios dos constantes do contrato do seguro-saúde. A existência desses dados e seu uso em algoritmos não transparentes disponíveis para seguradoras, governos, escolas e empregadores (ou o que os regulamentos permitirem) afetarão todos os aspectos da existência da pessoa, do nascimento à morte e possivelmente além.

LIBERDADE E IGUALDADE

Existem dois valores fundamentais que são inseparáveis de nossa personalidade física e digital:

1. Somos livres: ninguém tem o direito de escravizar-nos no mundo real. Ninguém deve ser escravizado no ciberespaço como consequência de terceiros reivindicarem nossos dados pessoais e usá-los para construir nossas personas como sua propriedade.

2. Além disso, todas as personas digitais são iguais e devem ser tratadas igualmente.

A igualdade de tratamento como cidadãos digitais significa que devemos garantir a igualdade de acesso ao ciberespaço para todos.[23] Isso significa a criação de uma infraestrutura digital que não favoreça os ricos ou privilegiados, um espaço ao qual ninguém é impedido de acessar por motivo de condições sociais ou econômicas . O acesso digital precisa ser visto como um bem público, e sua oferta como um serviço público.[24]

A igualdade vai além do acesso técnico. Devemos garantir que as tecnologias não sejam tendenciosas e não favoreçam um usuário em detrimento de outro devido ao status socioeconômico, idade, gênero, etnia ou outras características culturais. Isso requer acesso equitativo aos níveis de alfabetização digital e o tratamento não discriminatório dos fluxos de dados nas redes. Por exemplo, sobre a neutralidade da rede, o tratamento não discriminatório dos fluxos de dados tem sido defendido como um direito humano básico de todo cidadão digital e essencial para manter a Internet como um espaço uniforme para inovadores, provedores de serviços e usuários de serviços.[25]

DIGNIDADE

Nossa dignidade é uma consequência direta de nossa liberdade e igualdade. A dignidade de uma persona digital é violada quando se perde o controle sobre os dados que compõem a persona digital, personas que se vinculam à identidade digital de alguém. Esse dano resultante à dignidade digital de uma pessoa ocorre quando algoritmos opacos de processos de negócios digitais são usados para produzir personas digitais independentes dos desejos da pessoa. Com parâmetros internos opacos que podem refletir preconceitos dentro do algoritmo, as múltiplas versões da personalidade digital de alguém podem resultar em abuso. Esse abuso pode ser minimizado, se não totalmente evitado, se uma pessoa tiver controle total sobre seus dados pessoais e esses dados estiverem sendo usados.

DIREITOS

Outra consequência de nossa liberdade e igualdade é que nossos direitos são inseparáveis de nosso ser como pessoa. A forma como esses direitos são interpretados e se manifestam pode variar de acordo com o contexto e pode evoluir ao longo do tempo, mas os valores fundamentais expressos na DUDH e que orientam esse processo são imutáveis.

Com os direitos vêm as obrigações.[26] Nossa dignidade pessoal como cidadão digital depende de como exercemos nossos direitos e obrigações. Nossas obrigações digitais são baseadas em nossos direitos digitais e são (ou deveriam ser) estabelecidas por meio de processos adequados de formulação de políticas. Sob nenhuma circunstância a formulação de políticas, ou resultados, deve negar ou violar nossos direitos humanos fundamentais expressos na DUDH.

A falta de processos legítimos e eficazes de formulação de políticas em torno dos direitos digitais deixa-nos com controle limitado sobre nossa identidade digital e personas digitais. A perda da integridade digital restringe o exercício de nossos

23. Isso será considerado na análise do artigo 3, a seguir.
24. Este é um campo para formulação de políticas. A teoria da utilidade pública supõe infraestrutura em grande escala a preços regulados para obter economias de escala sem concentrar o poder de monopólio. A teoria dos bens públicos pressupõe usuários adicionais a um custo marginal próximo de zero, uma situação que pode ser representada pelo avanço do armazenamento em nuvem e da tecnologia 5G.
25. Neutralidade da rede – a ideia que os provedores de serviços de Internet (ISPs) devem tratar todos os dados que trafegam por suas redes de forma isonômica, sem discriminação indevida em favor de aplicativos, sites ou serviços específicos – é um princípio que deve ser mantido para proteger o futuro da Internet como uma rede aberta. É um princípio que enfrentou muitas ameaças ao longo dos anos, com ISPs forjando pacotes para adulterar certos tipos de tráfego, ou desacelerando ou até mesmo bloqueando completamente protocolos ou aplicativos. Ver Electronic Frontier Foundation: *https://www.eff.org/issues/net-neutrality*
26. Neste texto, obrigações digitais e deveres digitais são sinônimos.

direitos e deveres digitais. Com as tecnologias de vigilância, a Internet das Coisas (IoT) e algoritmos de IA, nossos dados digitais crescem e as personas proliferam. Essas personas digitais criadas por terceiros não estão sujeitas a permissões nem validação. Não ter a posse de nossos dados pessoais viola o mais fundamental dos direitos humanos.

RAZÃO E CONSCIÊNCIA

O Artigo 1 diz que os seres humanos, "[d]otados de razão e de consciência, devem agir uns para com os outros em espírito de fraternidade". Expressa o que nos torna, como usuários de tecnologias digitais, diferentes da própria tecnologia digital.

As tecnologias digitais, e especialmente a IA[27] podem aprender, o que significa uma capacidade de processar *big data* rapidamente e agregar dados para diversos usos. Esse aprendizado tem várias dimensões, mas grande parte é baseada no reconhecimento de padrões, inferência ou dedução. Por mais poderoso que seja para processar *big data*, ainda está longe da capacidade de raciocinar ou de ter consciência. As afirmações promissoras dos entusiastas da IA, não importa quão inteligentes sejam as máquinas que criam, nunca chegam a competir com a verdadeira razão e consciência humanas. A elas faltarão integridade e dignidade, empatia e respeito pelos outros.

Os sistemas de decisão automatizados e de IA são adotados por razões de eficiência e frequentemente elogiados por sua capacidade de "fazer o bem". Mas, como qualquer tecnologia multifuncional, há uma desvantagem real e perigosa.[28] Sistemas de decisão automatizados e algoritmos de IA são criados de maneiras não transparentes e não consensuadas. O principal interessado, a pessoa cuja identidade digital está sendo transformada em persona, não é consultado. Algoritmos opacos, com tendências não identificadas, tomam decisões que afetam profundamente as vidas humanas.[29]

É essencial que haja transparência e responsabilidade pelo uso dos dados e pelas determinações pessoais. Sem supervisão real, onde está a verificação preventiva para testar se as decisões automatizadas são erradas, discriminatórias ou tendenciosas? Como esses erros são corrigidos antes que as vidas dos cidadãos sejam afetadas negativamente? Tais sistemas de decisão, sem total consentimento e informação, podem e têm prejudicado as pessoas.[30] As tentativas de apropriação de dados pessoais digitais, na ausência de transparência de uso e consentimento da pessoa, devem ser fortemente combatidas.

Iniciativas para testar, validar e auditar sistemas de decisão automatizados geram preocupações sobre propriedade intelectual. O sigilo em torno dos algoritmos digitais, valiosos para práticas de negócios digitais cada vez mais questionáveis, tem dificultado o escrutínio dos aplicativos de prática de negócios. A alegação de segredo comercial tem sido usada para evitar o diagnóstico e a correção de sistemas defeituosos e resultados de decisões.

Podemos conceder autoridade às tecnologias digitais e podemos conceder-lhes direitos de tomada de decisão, mas isso sempre será um exercício da intenção humana. Sempre teremos que reconhecer que é nossa capacidade de raciocinar e nossa

27. Este texto diferencia Inteligência Artificial Estreita (IAE) , que consiste basicamente de algoritmos sofisticados que emitem decisões com base na entrada de dados que recebem, e Inteligência Artificial Geral (IAG), onde as máquinas são basicamente e supostamente mais inteligentes do que nós. Hoje a inteligência artificial na prática é IAE, e a IAG permanece como um sonho (ou pesadelo) sobre o futuro.

28. "Sem a participação democrática, não temos como garantir que a inteligência artificial não agrave a desigualdade e obstrua a agência humana – possivelmente, sem que nunca saibamos". Ver *https://www.aclu.org/issues/privacy-technology/will-artificial-intelligence-make-us-less-free*

29. Ver, por exemplo, Cathy O'Neil, Weapons of Math Destruction, Nova York: Crown Books, 2016.

30. Massachusetts aprendeu que "*big data*" nem sempre é confiável em 2013, quando voluntários usaram o aplicativo "Street Bump" de Boston para relatar a ocorrência de buracos. Os dados indicaram mais buracos nas áreas mais ricas do que nas mais pobres. A razão para esse resultado falso foi que os residentes mais ricos eram mais propensos a possuir um smartphone e usar o aplicativo. Ver *http://ritaallen.org/blog/confronting-the-data-dilemma*. O exemplo dos buracos de Boston é uma advertência. Os sistemas de dados automatizados em outras partes do país já prejudicaram os cidadãos em áreas críticas como bem-estar infantil, educação e habitação. Em 2015, Indiana concedeu um contrato lucrativo à IBM para automatizar os requisitos de elegibilidade do bem-estar do Estado, o que acabou expulsando erroneamente os deficientes do Medicaid. Em 2016, o Arkansas começou a usar um sistema de decisão automatizado que prejudicou centenas de residentes com necessidades especiais ao restringir indevidamente seu acesso a serviços de saúde domiciliar. A Assistência Judiciária processou o Estado e o tribunal considerou esse sistema inconstitucional e falho. Ainda hoje, o governo federal dos EUA está promovendo regras que são contrárias aos objetivos de proteção do HR 2701 ("Youth Access to Sexual Health Services Act" de 2019). O HUD ("Housing and Urban Development Department") está considerando a adoção de novas regras que isolariam proprietários, bancos e seguradoras da responsabilidade pelo uso de modelos algorítmicos, independentemente das consequências discriminatórias. Ver *https://www.eff.org/deeplinks/2019/09/dangerous-hud-proposal-would-effectively-insulate-parties-who-use-algorithms*

consciência as responsáveis pelas decisões que as máquinas tomam. As tecnologias digitais não podem ser usadas de maneiras que escapem à nossa razão e consciência. Situações em que as tecnologias digitais recebem direitos sobre outros humanos são uma abdicação de nossas responsabilidades e isso é profundamente fraudulento e arriscado.

ESPÍRITO DA HUMANIDADE

Razão e consciência nos dizem que apesar de todas as diferenças aparentes, compartilhamos uma humanidade conjunta. Aprendemos desde cedo que vivemos melhor quando aprendemos a viver juntos e a cuidar do outro. Liberdade, igualdade, dignidade e direitos são os elementos que constituem o espírito da humanidade. O desafio que temos pela frente é entender como os espaços digitais da Internet global podem ser usados para o bem. Ao mesmo tempo em que protegemos nossos direitos, devemos aprender que o ciberespaço deve ter integridade digital para que nós, como humanos, tenhamos integridade pessoal e coletiva.

> ***Artigo 2: Todos os seres humanos podem invocar os direitos e as liberdades proclamados na presente Declaração, sem distinção alguma, nomeadamente de raça, de cor, de sexo, de língua, de religião, de opinião política ou outra, de origem nacional ou social, de fortuna, de nascimento ou de qualquer outra situação. Além disso, não será feita nenhuma distinção fundada no estatuto político, jurídico ou internacional do país ou do território da naturalidade da pessoa, seja esse país ou território independente, sob tutela, autônomo ou sujeito a alguma limitação de soberania.***

O Artigo 2 reforça o Artigo 1, declarando que todos têm todos os direitos e liberdades da DUDH. Nenhuma distinção pode ser feita entre as pessoas com base em fatores biológicos (raça, sexo, cor), na cultura (idioma, religião, opinião política ou outra), ou nas circunstâncias de nosso nascimento (nacionalidade, riqueza, status social, classe). O Artigo 2 afirma ainda que a igualdade também não é afetada pelo país ou território ao qual uma pessoa pertence.

Com base no princípio de separado, mas inseparável, isso é igualmente válido para a identidade digital de uma pessoa, persona digital e capacidade de exercer sua cidadania digital. Nenhum indivíduo ou grupo de partes interessadas deve ser capaz de negar os direitos de outros cidadãos digitais no que diz respeito à privacidade e propriedade de dados pessoais e basear essa negação em distinções feitas por razões biológicas, culturais, de origem, riqueza ou afiliação de país/território.

VIDA

> ***Artigo 3: Todo o indivíduo tem direito à vida, à liberdade e à segurança pessoal.***

No contexto das tecnologias digitais, a vida literal e digital são interdependentes. Vida digital, liberdade e segurança significam acesso e o direito de controlar os dados pessoais e seu uso. Isso, por sua vez, impacta a vida literal de uma pessoa.

O direito à vida no contexto das tecnologias digitais consiste no direito de livre acesso e nos nossos direitos de cidadania digital em relação à segurança, privacidade e integridade do nosso ser digital e sobre nossos direitos como personas digitais construídas por aqueles com quem interagimos.

LIBERDADE

No contexto da liberdade no ciberespaço, precisamos começar com uma discussão sobre o acesso, um termo ao qual teremos que retornar frequentemente.

O acesso ao ciberespaço é um direito fundamental de cada pessoa. É essencial para o exercício da cidadania digital. O acesso gratuito ou acessível à Internet (bibliotecas,[31] telecentros, telefones celulares) é a base essencial para o envolvimento de um cidadão digital na proteção de seus direitos literais e digitais. O acesso requer um ambiente de política que favoreça o acesso acessível.

As políticas que restringem o acesso de um cidadão à Internet (como a rescisão de "infratores

31. Ver *https://www.ifla.org/digital-plans*

reincidentes" de direitos autorais; políticas de três ataques) podem violar os direitos digitais dos cidadãos à vida, à liberdade e à segurança pessoal. O acesso a produtos e serviços digitais tornou-se parte integrante da vida diária e pode ser uma questão de vida ou morte. Por exemplo, quando medicamentos vitais só são acessíveis para um paciente por meio de farmácias online, existem várias políticas e áreas de políticas regulatórias que requerem atenção para que o direito de viver da pessoa seja respeitado.[32] Segredos comerciais ou com cláusulas confidenciais em contratos de licença de terceiros para sistemas de decisão automatizados ou software relacionado representam problemas de política. Essas disposições impedem a capacidade de acessar e testar métodos operacionais subjacentes que determinam como as decisões sobre personas e outros usos de dados são feitos. O público permanece desinformado sobre como seus dados privados estão sendo usados. Quaisquer dados subjacentes derivados de pessoas (que contenham ou não informações identificáveis) só devem ser acessíveis a terceiros com a permissão da pessoa e quando a pessoa estiver totalmente informada dos usos pretendidos.

Ninguém deve ser forçado a abrir mão de seus direitos fundamentais de igualdade e liberdade em troca de bens e serviços, ou pela capacidade de receber os direitos de cidadania e residência (por exemplo, assistência social e emergencial).[33] Os impactos das decisões do processo digital para o indivíduo e a comunidade precisam ser compreendidos e atendidos agora, para evitar mais estratificação social e a criação de mais residentes em situação de pobreza digital.[34]

SEGURANÇA

Aqui devemos perguntar: segurança e proteção de quê? Para que nossa persona digital opere como uma pessoa digital funcional e competente é preciso, além do acesso seguro e confiável, a segurança em relação a tudo que corrompa ou controle esses dados pessoais. Ataques que ameaçam nossa integridade digital resultam em sérios danos ao nosso corpo físico e à vida literal.

ESCRAVIDÃO DIGITAL

Artigo 4: Ninguém será mantido em escravatura ou em servidão; a escravatura e o trato dos escravos, sob todas as formas, são proibidos.

Embora a escravidão física e a servidão possam parecer dissociadas de nossa presença digital no ciberespaço, as técnicas digitais estão sendo usadas para violar direitos humanos literais (tráfico sexual, pornografia infantil etc) e resultar em escravidão humana. A escravidão digital está em outro nível e a cidadania digital precisa ser protegida da escravidão digital.[35]

A escravidão digital ocorre quando, sem permissão, os dados digitais de uma pessoa são apropriados e as personas digitais são construídas com o propósito específico de influenciar ou manipular o comportamento dessa pessoa. A persona digital de uma pessoa está a serviço de outros e sem permissão ou compensação. A exploração de dados pessoais, incluindo vigilância e mineração de dados, são práticas digitais nas quais está baseada a economia escravista digital. Cada vez mais, um modelo escravista digital de um eleitor manipulado e complacente está corroendo as estruturas da democracia representativa. O desenvolvimento incipiente em curso das regras de governança digital deve ser baseado na DUDH e respeitar esses direitos no ecossistema digital.

São muitas as características conjuntas da escravidão e da exploração digital. Ambas veem

32. Por exemplo, os "Princípios de Bruxelas sobre a venda de medicamentos pela Internet", *https://www.brusselsprinciples.org*

33. Isso é relevante no contexto da IA. Ver nota 8 acima.

34. Como diz o ditado, quem não aprende com a história está condenado a repeti-la. A rica história de projetos de bem-estar social bem intencionados em Massachusetts pode ser uma lição instrutiva sobre como lidar com os riscos da IA e dos sistemas de decisão automatizados. Por exemplo, Boston estabeleceu o primeiro abrigo para pobres nos EUA em 1662. Nos duzentos anos seguintes, abrigos surgiram em todo o país como uma forma de "administrar" a pobreza. Os cidadãos assinaram um "juramento de indigente" renunciando aos seus direitos fundamentais, incluindo o direito de voto. Embora bem intencionados, os abrigos tornaram-se conhecidos por suas condições miseráveis e desumanas. As famílias foram reduzidas a "casos" a serem gerenciados. Os riscos apresentados por sistemas de decisão digital automatizados e IA precisam ser compreendidos e tratados agora, para reduzir a perda de poder digital e literal e para evitar a criação de versões digitais dos abrigos.

35. É importante notar aqui que os autores não estão tentando igualar o incomparável e colocar a escravidão em pé de igualdade com a exploração digital. Apesar de todos os sofrimentos da exploração digital, eles nunca podem ser equivalentes, nem comparáveis. No entanto, podemos tomar a história como um aviso e inspiração e usar as lições aprendidas como auxiliares de navegação e interpretação.

os seres humanos como mercadorias e ignoram os direitos humanos básicos. Ambas formam a base de um ecossistema econômico para justificar a exploração. Lembra a situação nos Estados Unidos antes e durante a Guerra Civil Americana. O Sul, colhendo os ganhos econômicos, tolerou a exploração e escravização de humanos, enquanto grande parte do Norte proibiu a prática. Da mesma forma, hoje temos partes interessadas corporativas e governamentais que buscam a exploração digital, argumentando que é necessário para a inovação e prosperidade digital, enquanto outras partes interessadas argumentam que tais práticas são exploradoras e devem ser proibidas.

Muito da governança digital atual baseia-se quase caso a caso em mecanismos apropriados por grupos de interesses especiais. Esses mecanismos precisam empoderar aqueles cujos direitos digitais são apropriados e cuja cidadania digital está comprometida.

Os esforços para a emancipação da escravidão digital exigirão vigilância. Os grandes desafios exigem consciência, liderança inspirada e construção de capacidades para uma boa governança digital, integridade nas práticas de negócios digitais e comportamento digital respeitoso. Hoje, os defensores dos direitos e integridade digitais contam com a força adicional da Declaração Universal dos Direitos Humanos (DUDH) como base para a promoção dos direitos digitais e da cidadania digital.

O direito à privacidade é um direito inalienável de todo cidadão digital. O controle deve permanecer com a pessoa literal. As práticas que buscam o acesso e o uso de dados digitais pessoais (como em acordos de usuário) exigem termos de acordo explícitos e claros para impedir que tornem-se instrumentos de um comércio de escravos digitais, resultando em escravidão ou servidão literal ou digital.

Um estado de servidão digital (quase escravidão) também é alcançado quando o status de quase monopólio de um aplicativo digital significa que, para comunicar-se, interagir ou conduzir negócios no ecossistema da Internet, o cidadão digital é forçado a aceitar permissões de escravidão digital como condição para usar esse aplicativo digital específico. Uma situação similar também ocorre quando serviços de governo só podem ser utilizados por meio digital e exigem que a pessoa forneça dados pessoais não relevantes para o serviço procurado.

TORTURA DIGITAL

Artigo 5: Ninguém será submetido a tortura ou a penas ou tratamentos cruéis, desumanos ou degradantes.

Pode parecer exagero abordar o tópico da tortura digital, mas um breve exame aqui é instrutivo. Pense na tortura digital como atos deliberados para enfatizar a identidade digital e a presença digital de alguém. Um estado de tortura digital pode existir quando, por exemplo:

- uma pessoa é impedida de acessar a totalidade ou partes do ciberespaço;
- não há acesso digital para controlar os dados ou, se desejado, para excluí-los;
- as tecnologias de dados digitais influenciam ou prejudicam a pessoa física (um risco crescente com a Internet das Coisas);[36]
- os dados pessoais são alterados , excluídos ou usados para criar deliberadamente personas enganosas que causam danos à pessoa;
- *ransomware* (sequestro digital de dados) é usado para fazer reféns de dados, com restauração disponível apenas por extorsão.

As tecnologias digitais, por sua própria natureza, permitem comportamentos maliciosos que submetem os cidadãos digitais a muitas formas de tratamento online cruel, desumano ou degradante. A capacidade de comunicação online em massa, geralmente anônima, é usada para espalhar desinformação com o objetivo de assediar e processar outras pessoas. O desenvolvimento de

36. Isso relaciona-se a situações difíceis de notícias falsas, negadores de vacina e assim por diante.

estruturas de governança digital deverá colocar em prática instrumentos e medidas que evitem tais comportamentos.

Nesta breve revisão e reflexão sobre os primeiros cinco artigos da DUDH, as principais questões relacionadas aos direitos e obrigações pessoais digitais foram identificadas. Em cada caso, a orientação para uma boa política e boa governança aponta de volta para a DUDH como uma pedra angular para a definição e elaboração dos direitos e deveres digitais da residência digital (cidadania digital) no ecossistema da Internet. Sugerimos as propriedades inclusivas de uma abordagem multissetorial para o desenvolvimento de políticas aqui.

PARTE 3: ARTIGOS 6-12

A governança da Internet, como toda governança, deve ser fundamentada em princípios orientadores que são a base da formulação de políticas. Não há melhores princípios fundamentais para orientar nossa formulação de políticas do que a DUDH. Nesta Parte 3 discutimos os artigos 6 a 12 da DUDH e abordamos tópicos como valores digitais fundamentais, lei cibernética, formulação de políticas e o papel dos tribunais na governança digital.[37]

Os artigos 6 e 7 estão intimamente relacionados e estão discutidos em conjunto.

Artigo 6: Todos os indivíduos têm direito ao reconhecimento, em todos os lugares, da sua personalidade jurídica.

Artigo 7: Todos são iguais perante a lei e, sem distinção, têm direito a igual proteção da lei. Todos têm direito a proteção igual contra qualquer discriminação que viole a presente Declaração e contra qualquer incitamento a tal discriminação.

O Artigo 6 estabelece a base para os direitos pessoais com o "reconhecimento de uma pessoa como tal perante a lei". Ele "reconhece a existência do indivíduo como um ser humano com necessidades, interesses e opiniões distintas".[38] Este é "um pré-requisito para todos os outros direitos do indivíduo".[39]

TODOS, EM TODOS OS LUGARES, IGUALMENTE

Os artigos 5 e 6 enfatizam a universalidade dos direitos pessoais e não fazem distinções com base em raça, religião, cultura ou orientação de gênero. Personalidade é um conceito amplo sob a DUDH, e a tarefa urgente agora é reconhecer formalmente a personalidade digital,[40] dados pessoais e "personas construídas" formalmente sob sua proteção.

Universalidade e inclusão sem limitações geográficas são características fundamentais do ciberespaço e os pilares de sustentação da cidadania digital.[41] Os direitos de todos, em todos os lugares, igualmente (os "3E" do inglês "everyone, everywhere, equally") são "separados, mas inseparáveis" como princípios fundamentais da DUDH e devem ser a base da cidadania digital. Nenhum cidadão deve ter o acesso e a proteção da lei negados ou ser forçado a desistir desses direitos fundamentais em relação aos seus dados digitais e personas digitais no ecossistema da Internet.[42]

37. Esta série de artigos apresenta-se um pouco como a preparação da fundação de uma casa – aqui a casa é a "casa dos regulamentos e direitos" na era digital. Uma compreensão dos direitos digitais desejados e das armadilhas da política e regulamentação é necessária para construir uma plataforma robusta e relevante de direitos digitais.
38. Margaret Edith Brett, The Right to Recognition as a Person before the Law and the Capacity to Act under International Human Rights, página 9, LLM em Legislação Internacional de Direitos Humanos, Irish Centre for Human Rights, National University of Ireland, Galway, agosto de 2012, *https://www.chiark.greenend.org.uk/~chrisj/Right_to_Recognition.pdf*
39. Geraldine Van Bueren, *The International Law on the Rights of the Child* (Martinus Nijhoff: 1995), 40; Manfred Nowak, *U.N. Covenant on Civil and Political Rights: CCPR Commentary* (2ª ed. revisada, N.P. Engel: 2005), 369.
40. Discutimos nossa persona digital na Parte 1.
41. Esta área é mais crítica em face do maior uso de desligamentos digitais/Internet para lidar com questões internas.
42. Já discutimos isso na Parte 1 sob o título "Liberdade".

Nas palavras de Wolfgang Kleinwächter:

O conceito de "compartilhamento" está no DNA de toda a Internet. Isso leva a uma "situação ganha-ganha" e não conhece perdedores. Se o conceito de compartilhamento for ignorado ou substituído por um "jogo de soma zero" do século 20 com vencedores e perdedores, o risco é alto de que, em um mundo interconectado, no final do dia todos sejam perdedores. Esta é uma lição fundamental dos 50 anos de história da Internet, que não deve ser esquecida na década de 2020.[43]

VALORES DO DNS

Os 3E também se aplicam, em sentido técnico, à operação do sistema de nomes de domínio da Internet (DNS).[44] Quando o DNS responde a consultas de endereços digitais, ele não faz distinções e atende a todos, em qualquer lugar, igualmente. O DNS reflete e defende o princípio mais importante quando se trata da aplicação da lei: não discrimine.[45] O DNS é mais do que uma inovação técnica – sua operação incorpora inerentemente o respeito pelos direitos no ciberespaço e exibe integridade na comunicação humana em um sistema de confiança. As tentativas de enfraquecer a universalidade do DNS por meio de raízes alternativas, segmentos nacionais e espaços fechados diminuem nossos direitos como pessoas e reduzem o papel do ecossistema da Internet como um local para construir nossa humanidade conjunta digital e humana.

RECONHECIMENTO

O reconhecimento perante a lei significa não só o reconhecimento do ser humano como pessoa e cidadão, mas também o reconhecimento das circunstâncias específicas em que reside, aqui como personas digitais e cidadãos digitais. As leis, regulamentos e comportamento relativos à existência digital devem respeitar a residência (global) sem fronteiras de nossos seres digitais e tratar nossos dados e personas digitais como parte de nosso ser.

LEI CIBERNÉTICA[46]

Lei cibernética é qualquer lei aplicável no ciberespaço. O tratamento perante a lei baseia-se na lei codificada e na jurisprudência. Jurisprudência sob governança digital está em sua infância e se desenvolverá com o tempo. O mesmo acontecerá com a jurisprudência e os processos jurídicos relativos a questões como propriedade intelectual, violação de marca registrada, disputas de nomes de domínio, pirataria cibernética e práticas de comércio eletrônico. O desenvolvimento legislativo sobre crimes cibernéticos e o desenvolvimento de políticas para práticas e comportamentos aceitáveis nas esferas política, econômica e cultural digital, estão em sua infância.[47]

É essencial que o trabalho nessas áreas tenha um firme entendimento e embasamento nos princípios embutidos na DUDH conforme se aplicam a pessoas, dados pessoais e personas nos ciberespaços do ecossistema da Internet. As leis e regulamentos devem ter o cuidado de abordar os problemas da forma mais restrita possível e evitar consequências indesejadas no fluxo livre de informações na Internet.

Atualmente, existe um consenso geral de que as atuais leis e tratados internacionais aplicam-se ao ciberespaço. A discussão concentra-se mais em "como eles se aplicam" do que em "se eles se aplicam".[48] Alguns governos consideram os tratados existentes e as leis nacionais como adequados. Outros veem a necessidade de criar novas leis específicas

43. Wolfgang Kleinwächter, "Internet Governance Outlook 2020: The Next Generation of Players and Problems Is Coming", CircleID, *http://www.circleid.com/posts/20200107_internet_governance_outlook_2020_next_generation_of_players*
44. Para obter mais informações sobre o DNS, ver: *https://en.wikipedia.org/wiki/Domain_Name_System e https://www.icann.org*
45. Esta é uma das principais distinções entre a busca no DNS e o uso de mecanismos de busca onde os algoritmos sempre contêm elementos de parcialidade, discrição e ambiguidade humana.
46. O tema da lei cibernética e seu desenvolvimento futuro é recente, amplo e importante. Ele merece atenção cuidadosa para que não codifique regulamentos que impactam negativamente os direitos digitais das pessoas.
47. Para obter mais informações sobre o contexto internacional de tratados e iniciativas de crimes cibernéticos, consulte a nota de rodapé 25, abaixo.
48. Por exemplo, uma das principais questões entre os Estados é a aplicação do direito internacional à guerra cibernética. Ver *Tallinn Manual on the International Law Applicable to Cyberwarfare (https://en.wikipedia.org/wiki/Tallinn_Manual)*

para o ciberespaço.[49] Dada a natureza global do ecossistema da Internet, as leis nacionais e regionais do ciberespaço muitas vezes têm uma relevância que vai além dos limites da soberania territorial.[50]

Embora os Estados possam concordar que a legislação cibernética está sempre sujeita a (ou guiada por) leis nacionais e acordos internacionais, estamos nos estágios iniciais na concepção de leis cibernéticas nacionais, bem como em algum grau de harmonia global entre as políticas digitais. A natureza global do ecossistema da Internet provavelmente envolverá discussões intensivas em torno dos acordos internacionais relativos aos direitos digitais e ao significado da cidadania digital global. Há também o risco no ambiente online global de que o primeiro país a regulamentar possa, em virtude de ser o "primeiro", essencialmente impor regras legais e responsabilidades potenciais ao resto do mundo.[51]

GOVERNANÇA DIGITAL E FORMULAÇÃO DE POLÍTICAS

Com o crescimento explosivo da Internet, observamos esforços crescentes por parte de alguns Estados para questionar a aplicabilidade do direito internacional existente no ciberespaço. Em 2004, as Nações Unidas conferiram mandato ao "Grupo de Especialistas Governamentais sobre Promover o Comportamento Responsável do Estado no Ciberespaço no Contexto da Segurança Internacional" (GGE).[52] O mandato do GGE era "considerar as ameaças existentes e potenciais na esfera da segurança da informação e possíveis medidas cooperativas para abordá-las'. Seis reuniões do GGE não conseguiram produzir um relatório de consenso em 2017 mas apenas delinear uma agenda digital global e o princípio geral de que o direito internacional se aplica ao ciberespaço.

As diferenças fundamentais em como os Estados veem o papel da lei no ciberespaço tornaram-se óbvias em 2018, quando a ONU adotou duas novas resoluções que determinavam outro GGE como uma continuação do anterior e cujo mandato incluía "levar em consideração as avaliações e recomendações do grupo anterior",[53] e em paralelo um "Grupo de Trabalho Aberto sobre Desenvolvimentos no Campo das TICs no Contexto da Segurança Internacional" (OEWG). Havia agendas, métodos de trabalho e atribuições sobrepostos e às vezes contraditórios.[54] Os dois grupos da ONU são uma manifestação da grande diferença conceitual entre os Estados-membros quando se trata de lei cibernética e governança digital. Um grupo de Estados prioriza sua própria soberania e proteção contra ameaças cibernéticas percebidas e influências externas indesejadas em seus assuntos internos. Outro grupo de Estados prioriza a segurança das informações pessoais sobre a segurança cibernética e coloca a integridade do ecossistema da Internet e como as informações digitais são processadas no topo de sua agenda. Essas tendências conflitantes tornam muito difícil

49. *O British Computer Misuse Act 1990* é um dos primeiros exemplos. Para mais informações, ver: *https://en.wikipedia.org/wiki/Computer_Misuse_Act_1990*. Um exemplo recente é o Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Para mais informações, ver: *https://ec.europa.eu/info/law/law-topic/data-protection_en*

50. Por exemplo, consulte o artigo da *Forbes Magazine*, "15 Unexpected Consequences of GDPR", 15-8-2018, *https://www.forbes.com/sites/forbestechcouncil/2018/08/15/15-unexpected-consequences-of-gdpr/ # 7b3a9e0894ad*

51. O GDPR da União Europeia pode ser visto como um excelente exemplo.

52. Para mais informações, consulte: *https://www.un.org/disarmament/ict-security*

53. Ver *https://digitallibrary.un.org/record/799853* – "Em sua resolução, a Assembleia Geral solicitou que um grupo de especialistas governamentais fosse constituído em 2014, com base em distribuição geográfica equitativa, para continuar os estudos, com vistas a promover entendimentos comuns, ameaças existentes e potenciais na esfera da segurança da informação e possíveis medidas cooperativas para enfrentá-las, incluindo normas, regras ou princípios de comportamento responsável dos Estados e medidas de fortalecimento da confiança, as questões do uso de tecnologias de informação e comunicação nos conflitos e como o direito internacional se aplica ao uso das tecnologias de informação e comunicação pelos Estados, bem como os conceitos voltados para o fortalecimento da segurança dos sistemas globais de informação e telecomunicações. O Grupo também foi convidado a levar em consideração as avaliações e recomendações de um Grupo anterior (ver *http://undocs.org/A/68/98*). O Secretário-Geral foi solicitado a apresentar um relatório sobre os resultados do e estudo para a Assembleia em sua septuagésima sessão".

54. Os especialistas do GGE se reuniram em um formato a portas fechadas, sem observadores permitidos. O trabalho do GGE é ainda limitado pelo mandato da Assembleia Geral "determina o trabalho dos GGEs diretamente no domínio da segurança internacional e do desarmamento e, portanto, não como um exercício técnico". O GGE também "decidiu que as questões que não estão sob a alçada do Primeiro Comitê - como espionagem, governança da Internet, desenvolvimento e privacidade digital - não são o foco do trabalho do Grupo". O Grupo de Trabalho Aberto começou em junho de 2019 e está aberto a todos os Estados membros da ONU. O OEWG realiza reuniões consultivas com outras partes interessadas do setor privado, sociedade civil e academia, que também podem se inscrever para participar das reuniões. O OEWG aborda seis questões substantivas: 1. Ameaças existentes e potenciais; 2. Direito internacional; 3. Regras, normas e princípios; 4. Diálogo institucional regular; 5. Medidas de construção de confiança; e 6. Capacitação. O objetivo do OEWG é desenvolver relatórios em uma base de consenso.

e improvável a formação de um consenso sobre políticas e práticas internacionais ou globais.

Outro processo foi criado recentemente no âmbito da ONU durante a 74ª Assembleia Geral. Uma resolução iniciada pela Rússia foi adotada para estabelecer um comitê intergovernamental ad hoc aberto de especialistas para "elaborar uma convenção internacional abrangente sobre o combate ao uso para fins criminosos de tecnologias de informação e comunicação".[55] Embora sua suposta intenção fosse abordar cibersegurança, isso deve ser visto como outra tentativa de sequestrar processos de governança da Internet sob o pretexto de segurança.

Wolfgang Kleinwächter resumiu os esforços em torno da formulação de políticas digitais até agora:

> ***"Na década de 2000, havia uma batalha mais ou menos ideológica entre 'ismos' – multissetorialismo x multilateralismo – que produziu mais polêmica do que progresso. Na década de 2010, foi amplamente reconhecido que ambos os conceitos poderiam coexistir [..] Mas como o Painel da ONU delineou, para a década de 2020, isso não será suficiente. A próxima geração de governança da Internet precisará de processos muito mais inclusivos, onde o multilateralismo e o multissetorialismo devem ser tratados como dois lados da mesma moeda".[56]***

GOVERNANDO OS ROBÔS ASSASSINOS

O ciberespaço é visto como outro teatro de guerra. Os governos identificaram rapidamente o potencial das tecnologias digitais para uso militar na defesa de seus países. Um grupo de especialistas governamentais está negociando desde 2014 um tratado sobre "Sistemas de Armas Letais Autônomas" (LAWS), no âmbito da Convenção sobre Certas Armas Convencionais (CCW).[57] Suas recomendações têm potencialmente uma grande influência na formulação de políticas para o ciberespaço. A avaliação da legalidade dos robôs assassinos baseados em IA difere amplamente entre os Estados. Alguns querem bani-los tal como as armas químicas, outros apoiam o uso dessas inovações digitais assassinas, mas nenhum está subestimando o impacto das tecnologias digitais na guerra. Dada sua importância e a expansão explosiva do uso de drones militares, é surpreendente quão pouco a discussão sobre robôs assassinos está ocorrendo no debate global geral.

MECANISMOS DE ELABORAÇÃO DE POLÍTICAS DIGITAIS

Ao longo dos anos, tem havido um número crescente e cada vez mais confuso de iniciativas para estabelecer mecanismos de formulação de políticas para o ciberespaço.[58] Algumas são baseadas na ONU.[59] Algumas são baseadas em esforços nacionais.[60] Algumas foram iniciadas por outras partes interessadas.[61] O número de iniciativas é confuso e parece ser limitado apenas pelo número de interesses especiais representados na governança digital. Sua característica comum é que são criadas como instrumentos para garantir que os interesses específicos de um grupo prevaleçam sobre os dos outros: o lucro sobre a privacidade; interesses nacionais sobre fraternidade global; ganhos políticos de curto prazo sobre o bem comum de longo prazo, a lista é longa enquanto houver

55. Ver *https://digitallibrary.un.org/record/3831879*
56. Wolfgang Kleinwächter, "Internet Governance Outlook 2020: The Next Generation of Players and Problems Is Coming", CircleID: *http://www.circleid.com/posts/20200107_internet_governance_outlook_2020_next_generation_of_players*
57. Para mais informações: *https://www.unog.ch/80256EE600585943/(httpPages)/8FA3C2562A60FF81C1257CE600393DF6*
58. Por exemplo, a Comissão Global sobre a Estabilidade do Ciberespaço (GCSC), *https://cyberstability.org*; a Plataforma de Internet de Genebra, *https://www.giplatform.org*
59. Por exemplo, a Cúpula Mundial sobre a Sociedade da Informação (CMSI/WSIS), *https://www.itu.int/net/wsis;* ou o Forum de Governança da Internet (IGF), *https://www.intgovforum.org/multilingual*
60. Por exemplo, o Fórum da Paz de Paris, *https://parispeaceforum.org;* ou o Diálogo de Genebra, https://genevadialogue.ch. Uma das iniciativas mais iluminadas e promissoras é a Rede de Políticas de Internet e Jurisdição, *https://www.internetjurisdiction.net*
61. Por exemplo, a Internet Corporation for Assigned Names and Numbers (ICANN), *https://www.icann.org* (nomes de domínio); Fórum Econômico Mundial (WEF), *https: //www.weforum.org* (capitalismo neo-liberal); "Contrato para a Web" de Tim Berners-Lee, *https://contractfortheweb.org*; Cybersecurity Tech Accord, *https://cybertechaccord.org*; Cyber Peace Institute, (CPI), *https://cyberpeaceinstitute.org*; Global Forum on Cyberexpertise (GFCE), *https://www.thegfce.com*

interesses especiais buscando proteção.

Outra característica que essas iniciativas compartilham é a pretensão de serem inclusivas e abertas a todas as partes interessadas, afirmando que o bem comum está em primeiro lugar em suas mentes. Isso lembra fortemente a proclamação dos porcos que controlam o governo no romance Animal Farm de George Orwell: "Todos os animais são iguais, mas alguns animais são mais iguais do que outros!"[62] Essa pretensão expôs a hipocrisia dos autoproclamados e autoempoderados grupos internacionais de formulação de políticas, órgãos que proclamam a igualdade absoluta de todos os cidadãos digitais, mas na prática preservam o poder e mantêm os privilégios de uma pequena elite.

MECANISMOS E TRIBUNAIS DE FORMULAÇÃO DE POLÍTICAS DIGITAIS

Não existe um órgão judiciário específico para o ciberespaço. Os Estados tentam preencher o vazio e estender sua soberania ao ciberespaço, sujeitando as atividades de seus cidadãos no ciberespaço a leis nacionais, algumas com elementos de extraterritorialidade. Esses esforços só podem resultar em aplicações inadequadas da lei e expressões de justiça. Eles não consideram as características especiais do ciberespaço e transpõem conceitos de direito e justiça baseados no território para o reino digital de atividades e comportamentos sem fronteiras, universais e inclusivos. Há uma necessidade urgente de definir a lei cibernética, estabelecer mecanismos de aplicação e criar tribunais de resolução de disputas, todos desenvolvidos por meio de processos legítimos de formulação de políticas. Para estabelecer leis cibernéticas legítimas e criar tribunais competentes, os cidadãos digitais devem estar capacitados e envolvidos nos processos de formulação de políticas.

HABILITANDO O RECONHECIMENTO

Algumas das razões pelas quais a governança digital eficaz até agora não foi estabelecida estão contidas na redação do Artigo 6. O reconhecimento perante a lei agora exige o reconhecimento igual dos direitos de todos, em qualquer lugar, no contexto de suas vidas nos reinos literais e digitais inseparáveis.[63]

São necessários modelos de governança digital que reconheçam e permitam a participação igual de todos, de todos os lugares, nos processos abertos de formulação de políticas. O modelo de participação múltipla é o que mais se aproxima desse ideal, mas pode ser corrompido por meio de barreiras artificiais de acesso, como financiamento entre outras. Como as partes interessadas da sociedade civil podem ser eficazes e independentes quando muitas vezes são as únicas que atuam como voluntárias e dependem do financiamento de outras partes interessadas para permitir sua participação?[64] Como as associações comerciais podem ser representantes de todos os seus membros quando sua formulação de políticas é ditada pelos interesses de seus principais membros corporativos?

Para explorar e eliminar as influências da corrupção institucional "[...] precisamos pensar sobre as maneiras pelas quais os sistemas de incentivos, ou economias de influência, podem promover ou impedir um objetivo coletivo".[65] A função da governança digital não é apenas política – fazer, mas também criar as condições para isso, por meio de esforços sem precedentes de conscientização, engajamento e capacitação com o objetivo de estabelecer os "3E". Como qualquer bom juiz, os processos de engajamento devem ser neutros e imparciais com todas as partes interessadas.

62. Ver *https://en.wikipedia.org/wiki/Animal_Farm*

63. Um bom exemplo da distinção, mas inseparabilidade do físico e digital, são as mudanças climáticas. As infraestruturas do mundo digital requerem grandes quantidades de energia, resultando em gases de efeito estufa. Tecnologias digitais como IA, blockchain e nuvem requerem grandes quantidades de energia e contribuem para a poluição. Potencialmente, essas mesmas tecnologias podem se tornar fatores importantes para superar os problemas que causam. A realização dos Objetivos de Desenvolvimento Sustentável da ONU depende em grande medida da implantação estratégica de tecnologias digitais, as mesmas tecnologias digitais que usadas indevidamente agravarão os problemas subjacentes.

64. Já discutimos essa problemática no artigo "Quo Vadis ICANN", ver *http://www.circleid.com/posts/20181211_quo_vadis_icann*

65. Lawrence Lessig: "Foreword: 'Institutional Corruption' Defined", *https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2295067.* A corrupção institucional é um campo que requer exploração urgente no contexto do ciberespaço e da governança da Internet e os trabalhos de Lessig fornecem um bom ponto de partida.

SEM DISCRIMINAÇÃO

O Artigo 7 dá muita ênfase à proteção dos cidadãos contra a discriminação que decorre de violações de seus direitos humanos básicos. Vai ainda mais longe ao condenar não apenas a discriminação ativa, mas também o "incitamento a essa discriminação". Muitos modelos de negócios digitais exploradores discriminam e, conforme discutido na Parte 2 desta série, reduzem o engajamento digital de alguém a pouco mais do que escravidão digital. Eles permitem e promovem a exploração de dados pessoais, incluindo vigilância, mineração de dados e personas digitais construídas, e contribuem para o resultado final da discriminação.

Enquanto o ciberespaço não tiver mecanismos de governança justos e eficazes, cabe ao Estado proteger os direitos de seus cidadãos, incluindo seus direitos como cidadãos digitais.[66] Isso não dá aos Estados o direito de presumir que podem discriminar os direitos dos cidadãos digitais por meio da aprovação de leis que estão em desacordo com as noções de direitos estabelecidas na DUDH, nem de buscar políticas de interesse especial às custas do bem público. A natureza global do ciberespaço impõe certos limites às ações efetivas dos Estados sobre os direitos e obrigações dos cidadãos digitais que são digitalmente ou literalmente residentes dentro dos limites do Estado e digitalmente residentes globalmente ao mesmo tempo.

TRIBUNAIS COMPETENTES

Artigo 8: Toda a pessoa tem direito a recurso efetivo para as jurisdições nacionais competentes contra os atos que violem os direitos fundamentais reconhecidos pela Constituição ou pela lei.

O Artigo 8 presume a existência de tribunais nacionais competentes e os direitos dos cidadãos baseados na lei. Até o momento, não existem tribunais competentes para o ciberespaço, seja nacionalmente ou para o ecossistema global da Internet. O ciberespaço carece de tribunais apropriados onde um cidadão digital possa buscar uma solução eficaz para questões de direitos digitais. Existem tentativas de estabelecer tribunais cibernéticos, incluindo tribunais que operam em nível global, mas eles tendem a se concentrar em questões de interesses especiais, muitas vezes comerciais, como propriedade intelectual e disputas de nomes de domínio.[67] Eles carecem de mecanismos de devido processo para usuários finais e lutar para alcançar os níveis de legitimidade que defendam os princípios gerais necessários para servir a uma base constituinte de múltiplas partes interessadas.[68]

O Artigo 8 também afirma que os tribunais devem ser competentes. De acordo com o artigo 14 do "Pacto Internacional sobre Direitos Civis e Políticos" (CCPR), para um tribunal ser competente é preciso ter independência e imparcialidade. Independência significa uma separação clara dos poderes do Estado, especialização dos oficiais de justiça envolvidos e a independência dos membros do tribunal em relação ao apoio de terceiros, como financiamento.[69] O surgimento de pseudo-tribunais, tribunais de "remoção" acelerados e outros processos rápidos pode frequentemente atropelar os direitos do usuário e diminuir o papel dos tribunais judiciais tradicionais.

Nenhum dos mecanismos de governança digital anteriores, atuais ou propostos e tribunais relacionados qualificam-se como "competentes".[70] Eles não estão claramente separados das instituições que eles "julgam" e/ou são mantidos por essas mesmas instituições.[71] No contexto do ecossistema da Internet e do ciberespaço, o multilateralismo é um

66. Os Estados têm a responsabilidade de garantir os direitos de seus cidadãos. O artigo 12 da Convenção sobre os Direitos das Pessoas com Deficiência pode servir de modelo: *https://www.un.org/development/desa/disabilities/convention-on-the-rights-of-persons-with-disabilities.html*
67. Mecanismos de proteção de direitos (RPMs) e procedimentos de resolução de disputas (DRPs). Para mais informações: *https://www.icann.org/resources/pages/rpm-drp-2017-10-04-en*
68. Já identificamos alguns desses princípios gerais, por exemplo, os 3 e's e o caráter dual separado, mas inseparável do ciberespaço.
69. Ver *https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx*
70. Para algumas das propostas mais recentes sobre mecanismos de governança digital, consulte a seção 3.3 de "A Era da interdependência digital", Relatório do Painel de Alto Nível do Secretário-Geral da ONU sobre Cooperação Digital, *https://www.un.org/en/pdfs/DigitalCooperation-report-for web.pdf*
71. O atual modelo de "ombudsman" implantado pela ICANN, embora útil e habilmente diplóide, é fragil por essa razão. Veja: *https://www.icann.org/ombudsman*

princípio importante que deve ser implantado como um princípio básico da governança digital. Como está atualmente implementado, não é independente nem imparcial.

Sob a orientação da DUDH, os Estados são atualmente a primeira linha de defesa contra o que deve ser codificado como violação dos direitos fundamentais dos cidadãos digitais. Na ausência de um amplo envolvimento com as políticas, esses remédios sempre serão parciais e imperfeitos. A tarefa urgente da governança digital é o desenvolvimento de processos políticos competentes e imparciais, e de leis e tribunais cibernéticos competentes.

O SIGNIFICADO DE "ARBITRÁRIO" NO CIBERESPAÇO

Artigo 9: Ninguém pode ser arbitrariamente preso, detido ou exilado.

O Artigo 9 confirma indiretamente o direito de um tribunal competente, (incluindo futuros tribunais competentes ao abrigo do direito cibernético), de ordenar a prisão, detenção ou exílio, se não for arbitrário. A acusação de um tribunal competente pode ser arbitrária ou não. Uma acusação ou punição arbitrária pode parecer aleatória, mas sempre há uma causa ou razão subjacente de "agenda privada". Por exemplo, um locus de poder (Estado, presidente, partido, ditador), pode usar instrumentos à sua disposição, (incluindo a polícia, o judiciário, ou agora a autoridade de comunicações), para intimidar seus cidadãos e incorporar o medo por meio do exílio digital, bem como prisões e punições aleatórias.

À medida que pessoas prejudicadas, como grupos comunitários étnicos e de gênero, recorrem a meios digitais para expressar suas preocupações, expor problemas e se mobilizar para a ação, é cada vez mais provável que ocorra um processo de dois níveis mais direcionado, mas ainda arbitrário. Indivíduos e comunidades inteiras podem experimentar o "exílio digital" no ciberespaço pela prática crescente das autoridades suspendendo o acesso tanto à Internet quanto ao serviço de telefonia celular. Isso pode ser seguido de detenção e prisão arbitrária com base em atividades rotuladas como indesejáveis no ciberespaço por governos impunes.

No ciberespaço, na ausência de políticas e regulamentos, o poder corporativo (mídias sociais, mecanismos de busca, aplicativos) tem amplo escopo para introduzir regras de uso que devem ser seguidas por seus assinantes e usuários. O que está em questão é o que justifica, ou desafia, a legitimidade das restrições e políticas de uso de dados incorporadas às regras do usuário. As regras podem ser justificadas quando beneficiam de forma igualitária todos os usuários digitais e baseiam-se no envolvimento e no acordo de várias partes interessadas. Se o motivo é aumentar o poder corporativo e os usuários não concordam com as regras, é pouco o que eles podem fazer. Discordar pode resultar em suspensão, exílio e "morte digital" na plataforma. Os provedores digitais, ou qualquer outra parte interessada digital, não devem ser capazes de introduzir regras arbitrariamente, ou exigir o uso de padrões e normas injustificadas, que prejudiquem os direitos dos usuários por exclusão ou ameaça de sanções.

A interferência nos direitos da cidadania digital é justificada e não arbitrária quando as tecnologias digitais são usadas para prejudicar terceiros. As tecnologias digitais são usadas para hacking, roubo de identidade, cyberbullying, phishing e pharming (usando técnicas criminosas antigas como chantagem e extorsão).[72] Tecnologias digitais cujo uso é justificado em circunstâncias normais, como criptografia e redes privadas virtuais (VPN), também

72. Em dezembro de 2019, a Assembleia Geral da ONU aprovou uma resolução para criar uma nova convenção internacional sobre crimes cibernéticos. A resolução foi aprovada marginalmente, com muitos temendo que a resolução permitiria reprimir a liberdade de expressão. Ver https://thehill.com/policy/international/476109-un-gives-green-light-to-draft-treaty-to-combat-cybercrime e https://news.yahoo.com/un-backs-russia-internet-convention-alarming-rights-advocates-011310327.html. Esta é apenas uma de uma série de iniciativas relevantes e tratados sobre crimes cibernéticos: Convenção de Budapeste do Conselho da Europa (Estrasburgo), https://www.coe.int/en/web/cybercrime/the-budapest-convention; o trabalho sobre Cibercrime pelo Escritório de Drogas e Crime da ONU (UNODC, Viena), incluindo o Grupo de Trabalho Aberto sobre Crime Cibernético, https://www.unodc.org/unodc/en/cybercrime/index.html, e seu estudo abrangente sobre Crime Cibernético, https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf; finalmente, a Cooperação de Xangai (SCO), que formalizou a cooperação entre os oito países membros (incluindo Índia, China, Paquistão e Rússia) em questões de crime cibernético, https://ccdcoe.org/organisations/sco (os autores agradecem Nigel Hickson por fornecer estes dados em um e-mail de 31/12/2019).

podem ser usadas para evitar a detecção e punição no exercício do cibercrime.

Atos arbitrários e leis excessivamente amplas podem impor a solução radical de remover o acesso individual ou domiciliar aos serviços da Internet, o que resulta em uma forma de exílio digital. Suspender o acesso dos usuários à Internet, junto com a filtragem de conteúdo e os regimes de "não utilização" sem a proteção do devido processo legal resulta em um exílio digital injusto.

Evitar atos arbitrários na lei cibernética exigirá intenso diálogo e consulta em processos competentes de formulação de políticas digitais.

CARACTERÍSTICAS DO TRIBUNAL

Artigo 10: Toda a pessoa tem direito, em plena igualdade, a que a sua causa seja equitativa e publicamente julgada por um tribunal independente e imparcial que decida sobre seus direitos e obrigações ou sobre as razões de qualquer acusação em matéria penal que contra ela seja deduzida.

O Artigo 10 descreve as características do tribunal a que um cidadão tem direito: igualdade, justiça, independência, imparcialidade. O papel do tribunal é restrito a determinar direitos e obrigações se algum ato criminoso foi cometido.

Existe um conflito inerente entre os interesses nacionais baseados na soberania sobre os territórios físicos e a presença do cidadão digital no ciberespaço sem fronteiras. As tentativas dos Estados de afirmar sua soberania territorial no ciberespaço e sobre a cidadania digital de alguém violam o Artigo 10, especialmente se tais tentativas ocorrerem fora dos sistemas judiciais normais. Por exemplo, agências administrativas que concedem a seus funcionários poderes semelhantes aos judiciais para exercer amplos poderes de remoção e injunção sobre os usuários da Internet, violam os direitos do usuário a um tratamento justo e igualitário por um tribunal independente e imparcial.[73]

INOCÊNCIA PRESUMIDA, MAS CULPA ASSUMIDA

Artigo 11: (1) Toda a pessoa acusada de um ato delituoso presume-se inocente até que a sua culpabilidade fique legalmente provada no decurso de um processo público em que todas as garantias necessárias de defesa lhe sejam asseguradas.

Artigo 11: (2) Ninguém será condenado por ações ou omissões que, no momento da sua prática, não constituíam ato delituoso à face do direito interno ou internacional. Do mesmo modo, não será infligida pena mais grave do que a que era aplicável no momento em que o ato delituoso foi cometido.

Conforme discutido acima, alguns Estados estão tentando mitigar a atual falta de leis cibernéticas com sua própria legislação.[74] Ao fazer isso, é importante que eles concedam aos cidadãos o direito ao devido processo legal e o direito de serem presumidos inocentes até que em última instância a prova de culpa seja estabelecida. Os Estados têm o poder de regular o acesso ao ciberespaço, conteúdo digital, aplicativos e atividades por meio de legislação e/ou barreiras técnicas prescritas. A suspensão do acesso à Internet e ao telefone celular tem se tornado cada vez mais comum, assim como a vigilância intensiva por parte do Estado e de interesses comerciais.

Há uma necessidade premente de diálogo com várias partes interessadas na formulação de políticas e de supervisão na implementação de políticas. Os Estados devem ser cuidadosos ao abordar o crime cibernético e a segurança, e a presunção de uso indevido apenas porque existe a

73. Este exemplo se aplica à Lei CASE, em que o Copyright Office dos EUA pretende criar um tribunal especial de remoção de direitos autorais, mas também pode aplicar-se na Europa porque a Diretiva de Direitos Autorais da UE exige que os Estados-Membros criem "mecanismos de reparação extrajudiciais" para resolver disputas de direitos autorais. Nos EUA, algumas dessas disposições de arbitragem forçada foram consideradas inescrupulosas e violam os direitos dos cidadãos ao devido processo legal.

74. Natasha Singer, "What Does California's New Data Privacy Law Mean? Nobody Agrees". *Ver https://www.nytimes.com/2019/12/29/technology/california-privacy-law.html*

possibilidade de uso indevido. Toda a legislação deve ser baseada em evidências, ser sensível aos direitos e motivada pelo interesse público e pelo bem comum. Não pode basear-se no fortalecimento dos interesses próprios do poder político e econômico à custa dos direitos digitais.

Nunca é demais enfatizar que há uma necessidade de uma discussão engajada entre todas as partes interessadas digitais sobre quais princípios devem ser honrados (com relação à DUDH) e quais políticas adequadas precisam ser implementadas para lidar com as questões que envolvem as tecnologias digitais. A coleta, o armazenamento e a vigilância de dados e o uso de AI para a construção de personas digitais abrem inúmeras questões sobre direitos e obrigações digitais.

Quando os redatores da DUDH redigiram o Artigo 11, ainda estavam frescas as memórias de uma Alemanha nazista, onde milhões foram acusados e considerados culpados por razões raciais, políticas ou econômicas, com base em uma fundação instável de leis injustas. Processos e julgamentos ocorreram a portas fechadas e sem o devido processo legal.[75] Os redatores tiveram longas discussões sobre o segundo parágrafo do Artigo 11.[76] A proibição da lei retroativa fazia parte de muitas constituições da época e a questão urgente era se isso significava que os recentes julgamentos de Nuremberg de criminosos nazistas eram ilegais.[77] Na época da redação, não era geralmente aceito que os líderes que haviam abusado de forma tão profunda e generalizada dos direitos humanos em nome de suas ideologias pudessem ser responsabilizados e ter que enfrentar um tribunal internacional.

Hoje, em um ambiente muito menos carregado, estamos enfrentando uma ordem inversa do processo. Os esforços dos Estados envolvem a elaboração de legislação nacional sobre os direitos e obrigações de pessoas ou entidades envolvidas no comportamento digital global. As questões de engajamento de desenvolvimento de políticas adequadas, legislação apropriada e alcance global são agudas hoje, com relação às políticas em torno do comportamento nos espaços digitais locais e globais do ecossistema da Internet.[78]

Embora a visão da Internet fosse "livre e aberta a todos", as partes interessadas, ao defender seus próprios interesses, usaram a linguagem da "ruptura digital" e da "inovação não regulamentada" para se envolver em práticas de negócios digitais em detrimento dos direitos digitais.[79] Em assim fazendo, elas possibilitaram e estabeleceram a exploração e a escravidão digital. No futuro, estamos em busca de legislação e regulamentos adequados que preservem um equilíbrio entre a proteção dos direitos digitais e os incentivos à promoção da inovação.

Uma questão importante é se as ofensas passadas contra os direitos humanos no ciberespaço devem ficar impunes ou sem compensação, devido à falta de legislação em vigor na época. Aqueles cujas personas foram prejudicadas não recebem compensação enquanto os perpetradores continuam a construir impérios baseados em seus ganhos ilícitos? Devemos perdoar e esquecer ou devemos buscar tribunais e restituições de crimes digitais internacionais? Essas questões não são exploradas aqui.

75. Para mais informação: *https://www.un.org/en/sections/universal-declaration/drafters-universal-declaration-human-rights/index.html*
76. "A DUDH estava sendo redigida logo após o julgamento dos crimes de guerra de Nuremberg ter terminado, com um julgamento semelhante ainda em andamento em Tóquio. O respeito do Artigo 11 pela presunção de inocência foi acordado rapidamente. Os redatores tiveram dificuldade com a redação do segundo parágrafo. Eles estavam preocupados que uma proibição de retroatividade pudesse ser usada como um argumento de que os julgamentos de Nuremberg foram ilegais. Eles haviam julgado por "crimes contra a paz" e "crimes contra a humanidade" que anteriormente não existiam nas leis nacionais.
77. Para mais informações: *https://en.wikipedia.org/wiki/Nuremberg_trials*
78. A referência à DUDH e aos Julgamentos de Nuremberg não compara o incomparável do Holocausto com as questões em torno dos direitos digitais, devido processo legal e exploração digital. No entanto, podemos e devemos tomar a história como lições aprendidas e inspiração. Podemos usá-los como um auxílio de navegação e interpretação em uma nova circunstância, o ecossistema global da Internet, onde o local, o global e o pessoal apresentam desafios políticos complexos. Estamos em um momento em que a exploração e exclusão digital são questões urgentes. Podemos olhar para a DUDH para saber o que ela nos diz hoje, como podemos reagir e evitar que o ciberespaço seja usado para repressão, exploração e exclusão.
79. Um dos mais proeminentes e insistentes defensores da ideologia da inovação sem permissão, Vint Cerf, teve que admitir sua limitação: "Toda a abertura levou ao que muitos de nós chamamos de inovação sem permissão, o que foi muito satisfatório para mim, vendo isso crescer de uma forma muito orgânica. Há apenas um pequeno detalhe que não havia penetrado em meu pensamento nos estágios iniciais e que é: o que acontece quando o público em geral tem acesso? " Vint Cerf, IGF dos EUA, Washington, DC, 2017, *https://www.youtube.com/watch?v=J4HxqfJK13I*

CRIMES DE OMISSÃO

Muitas das violações dos direitos descritos na DUDH que ocorrem no ciberespaço baseiam-se em atos de omissão. Para viabilizar e sustentar práticas comerciais digitais predatórias, não foram implementadas as ferramentas tecnológicas necessárias para proteger a privacidade e a segurança dos cidadãos digitais. Grande parte da segurança de dados tem a ver com o detentor dos dados apropriados, garantindo que eles não sejam acessados por concorrentes ou cibercriminosos. Mesmo a forma e o conteúdo por trás do "botão de consentimento" ou das opções de exclusão na maioria dos aplicativos são densos e, na maioria dos casos, exploradores ao extremo. Os usuários ficam mal informados sobre as consequências na vida real do uso de dados e da montagem de persona quando pressionam o botão sempre presente "Concordo" em um aplicativo digital ou site. Eles não têm idéia dos direitos que estão concedendo e das forças às quais estão sendo expostos.

ONDE ESTÁ A LINHA?

Artigo 12: Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei.[80]

Nunca tinha havido uma tecnologia, exceto a escravidão ou o encarceramento, mais adequada para interferir na privacidade de uma pessoa. Além da escravidão, nunca tinha existido um processo ou tecnologia que fizesse da invasão sistemática da privacidade de uma pessoa e da exploração da pessoa a base de seu modelo de negócios. Ao mesmo tempo, nunca tinha havido uma tecnologia com mais promessa de beneficiar a humanidade e ajudar a resolver alguns de seus problemas centrais, aqui por meio da coleta e análise de dados anônimos. Além disso, nunca tinha ocorrido uma tecnologia com potencial para "violar direitos, minar a privacidade, polarizar sociedades e incitar a violência".[81] Com o surgimento das tecnologias digitais, o setor privado, para seus próprios fins, junta-se ao Estado e outras entidades na vigilância dos cidadãos. A coleta e o processamento de dados pessoais são a base das práticas de negócios digitais que alimentam a receita e o crescimento das maiores entidades digitais e, cada vez mais, não digitais do mundo.

Os redatores da DUDH não poderiam ter previsto a importância e relevância da extensão da privacidade além dos dados pessoais limitados, o acesso de terceiros à família, trabalho e dados da comunidade, ou o surgimento de tecnologias intensivas de dados, como mídia social, e-mail , navegação na Web e a consequente mineração de dados e montagem de personas digitais.

Ao usar a palavra "arbitrárias", o Artigo 12 (assim como o Artigo 9) não vê o direito à privacidade como absoluto. A interferência no direito à privacidade deve ser necessária, legítima e proporcional. Tampouco previu dados pessoais e personas digitais construídas como propriedade que pudesse ser negociada, comprada ou vendida sem a permissão de seu proprietário. Isso é semelhante a ser atraído ou seduzido a se vender como escravo digital. As perguntas a serem feitas nos âmbitos legal e ético são:

1. Quais são nossa privacidade digital e direitos de propriedade sobre nossos próprios dados e nossas personas digitais?

80. O Artigo 12 da DUDH encontra seu equivalente no Artigo 17 do "Pacto Internacional sobre Direitos Civis e Políticos". O assunto da privacidade digital foi objeto de várias discussões ao longo dos anos. O Comitê de Direitos Humanos das Nações Unidas sobre o direito à privacidade, família, casa, correspondência e proteção de honra e reputação, nos termos do Pacto Internacional de Direitos Civis e Políticos (PIDCP), expresso em 1988, exige no Comentário Geral nº 16 ao Artigo 17 que a vigilância do Estado esteja sujeita a legislação precisa que salvaguarde o direito do cidadão à privacidade. A Resolução 68/167 da Assembleia Geral das Nações Unidas, sobre o direito à privacidade na era digital, foi aprovada em 18 de dezembro de 2013. Ações adicionais tomadas no âmbito da ONU: Resolução 68/167 incluiu um pedido da Assembleia Geral para que o Alto Comissariado para os Direitos Humanos preparasse um relatório sobre o direito à privacidade. O Conselho de Direitos Humanos com base em sua decisão 25/117 realizou um painel de discussão sobre os direitos de privacidade na era digital, em 2014. O conselho também nomeou em 2015, com base em sua resolução 28/16, um Relator Especial sobre os direitos de privacidade para um período de três anos. É preciso também mencionar o recente Relatório do Painel de Alto Nível do Secretário-Geral da ONU sobre Cooperação Digital, *https://www.un.org/en/digital-cooperation-panel*. Todo esse esforço mostra que embora a ONU esteja levando o assunto da privacidade digital a sério, ela não tem poderes para garantir e implementar o direito à privacidade além de fazer recomendações e esperar pelo cumprimento dos Estados e do setor privado.

81. *Report of the UN Secretary-General's High-level Panel on Digital Cooperation*, página 12.

2. Quais são as nossas obrigações de respeitar os direitos digitais de terceiros?

3. Como as práticas e limites são moldados pela legislação e pelos padrões éticos de comportamento?

O PAPEL ESPECIAL DA PRIVACIDADE NO CIBERESPAÇO

A privacidade assume uma nova importância no ciberespaço. Em um mundo pré-digital, a privacidade era mais fácil de manter e o direito à privacidade era respeitado por leis e regulamentos. As leis estavam em vigor nos casos em que era necessário infringi-las. Muito do tempo gasto e atividades comerciais, comunitárias e sociais em várias frentes passaram despercebidos e despercebidos, oferecendo pouco espaço para recuperação de informações. Até mesmo a perícia tende a trabalhar com conjuntos de dados mínimos. O surgimento do ciberespaço abriu possibilidades até então desconhecidas de acúmulo de dados em massa e vigilância por várias partes. Cada tecla, toque de dedo em um telefone celular, dados de localização e cada passo são coletados, armazenados, identificados e marcados. Isso abre um amplo campo para a manipulação comportamental, o capitalismo de vigilância e a exploração sem fim. O uso comercial indevido de dados pessoais e a construção de personas de uso específico ocorrem sem a permissão e consentimento significativos do usuário e sem supervisão.

Como esses dados em massa devem ser tratados é um assunto muito discutido. O que deve ser protegido como privado depende dos modelos de uso propostos? O que para uma parte representa vigilância em massa, engenharia social e manipulações, outras partes veem como o imperativo e a oportunidade de prevenir o crime, curar os enfermos ou apoiar a inovação. Aplicações ainda mais técnicas, como IA, podem tomar decisões sobre quais entre os mais necessitados recebem benefícios de bem-estar social. No entanto, a IA também é vista como a serviço da solução dos problemas mais urgentes da humanidade. A tecnologia digital coloca quem faz o quê com quais dados no centro das preocupações de uma sociedade sobre integridade e progresso pessoal e social. A agenda de preocupações resultante deve ser colocada no centro das discussões de política da sociedade.

COMBATENDO O PRECONCEITO: SOLUÇÕES TECNOLÓGICAS PARA PROBLEMAS TECNOLÓGICOS?

A criptografia garante a privacidade dos dados gerados pessoalmente, mas não resolve o dilema da privacidade por dois motivos. Muitos dos dados de uma pessoa são gerados além do seu envolvimento direto em uma atividade, e as autoridades sempre insistirão na necessidade de acesso pela backdoor (porta dos fundos) aos dados por razões de segurança. Um bom exemplo aqui é a recusa da Apple em ajudar o Departamento de Justiça dos EUA a desbloquear dois iPhones usados pelo atirador saudita que matou três pessoas em uma base da Marinha em Pensacola, Flórida. Desenvolvimentos recentes mostram que uma postura de princípios de uma empresa não significa que ela resista à pressão.[82] Como a criptografia, os dados pessoais anônimos exigem que o cidadão digital confie e autorize alguma instituição de governança digital competente, governamental, do setor privado ou outro, a supervisionar e controlar os processos. Isso é ainda mais complicado pelo fato de que esses dados "anônimos" podem ser facilmente reconstruídos usando apenas alguns pontos de dados conhecidos. Técnicas aprimoradas de IA, software de reconhecimento facial e outras ferramentas podem reconstruir ainda mais facilmente identidades identificáveis para vários usos. Tanto os cidadãos literais quanto os digitais não têm controle sobre os algoritmos usados ou os usos pretendidos de tais personas digitais. Embora este seja um problema de tecnologia, não há

82. Joseph Menn, Reuters, 21 de janeiro de 2020, "Exclusive: Apple dropped plan for encrypting backups after FBI complained – sources", *https://www.reuters.com/article/us-apple-fbi-icloud-exclusive/exclusive-apple-dropped -plan-for-encrypting-backups-after-fbi-complained-sources-idUSKBN1ZK1CT*

solução de tecnologia para questões de privacidade de dados ou de personas digitais. As soluções sempre exigirão uma combinação de governança baseada em políticas e o desenvolvimento de confiança em torno de normas sociais aceitáveis de comportamento por todos os envolvidos nos ciberespaços do ecossistema da Internet.

Identificamos a universalidade e a inclusividade como características fundamentais do ciberespaço e a necessidade de modelos de governança digital que reconheçam e possibilitem a participação de todos, de todos os lugares, em processos abertos de formulação de políticas. Observamos a necessidade e as atribuições de tribunais independentes e competentes, mas toda solução política ou tecnológica sempre exigirá a confiança humana. A confiança envolve compreensão e respeito mútuos, atitudes que fluem do engajamento aberto no diálogo entre diversos cidadãos digitais dos setores envolvidos.

É surpreendente ver como os princípios fundamentais da DUDH, como universalidade e inclusão total, encontram seu reflexo nos princípios fundamentais para governar as tecnologias digitais. Em muitos aspectos, estamos enfrentando os mesmos problemas que enfrentamos na elaboração da DUDH, só que nos ciberespaços do ecossistema da Internet. O objetivo é ser capaz de traduzi-los nos princípios, políticas e práticas que regem o comportamento na era digital.

O ciberespaço sempre terá áreas contestadas, e as decisões sobre políticas e práticas serão contínuas, tanto quanto a jurisprudência contínua enriquece o significado e a compreensão das leis e políticas legisladas. Os princípios fundamentais são sempre auxílios à navegação e metas a alcançar. Para os próximos passos no caminho de consagrar os princípios fundamentais para os direitos de nossa cidadania digital, temos que estabelecer mecanismos legítimos de governança digital e mecanismos inclusivos criados por e para "Nós, o povo..." tanto no sentido literal quanto digital.

PARTE 4: ARTIGOS 13-15

Aqui discutimos os Artigos 13-15 e tocamos em outros tópicos, como o papel da governança cibernética, cidadania digital empoderada e denunciantes ("whistleblowers").[83] Neste ponto é útil fazer uma pausa e lembrar-nos do propósito desta análise. O crescimento exponencial do ciberespaço digital e do ecossistema da Internet abriu novos territórios virtuais interessantes para a atividade humana e perturbou muitos elementos da ordem social humana existente (literal). Ao mesmo tempo, produziu grandes rupturas no tecido social e impôs desafios ao contrato social subjacente.[84] Nesta série de artigos, tentamos tratar de alguns tópicos relevantes.

Primeiro, examinamos a DUDH e seus princípios subjacentes para ver que orientação a Declaração pode dar para definir ou pelo menos apontar o caminho para a formulação de princípios e políticas que apoiam os direitos e deveres da cidadania digital. Para alguns aspectos, a orientação sobre direitos protegidos é direta. Outras áreas são exclusivas da extensão global do ecossistema da Internet e exigem novas ideias e novas abordagens.

Em segundo lugar, nossa intenção é explorar possíveis mecanismos para buscar caminhos possíveis. Pode não haver um caminho único nem um arranjo único de mecanismos. Existe, no entanto, um ponto de partida único – possibilitado pelo escopo do ecossistema da Internet. Esse ponto de partida, aspiracional neste ponto, começa com partes interessadas digitais engajadas, com o objetivo mais amplo de promover a cidadania digital engajada. Com todas as suas armadilhas e seus usos por aqueles que desejam atacar a democracia e os processos democráticos, o ecossistema da Internet oferece um espaço para o envolvimento democrático multissetorial em políticas e processos de tomada de decisão que até então eram inimagináveis. Para realizar a participação multissetorial, a governança

83. Esta série de artigos é apresentada um pouco como preparar a fundação de uma casa, aqui a casa é a "casa de regulamentos e direitos" na era digital. É necessário compreender os direitos digitais desejados e as armadilhas da política e regulamentação para construir uma plataforma robusta e relevante de direitos digitais.
84. Uma longa lista de exemplos poderia ser dada aqui, variando de questões de privacidade e segurança pessoal, a desintermediação perturbadora nos negócios e processos sociais, aos efeitos tóxicos de notícias falsas sobre eleições, governança e confiança.

da Internet provavelmente incluirá alguma combinação de estruturas e processos nacionais, internacionais e multilaterais.

O ecossistema da Internet mudou a realidade de maneiras mais profundas do que as mudanças da Revolução Industrial no final do século 19 ao início do século 20. Estas mudanças não foram reconhecidas no final da Primeira Guerra Mundial, quando o Tratado de Versalhes impôs condições de paz que contribuíram para quase meio século de consequências terríveis.[85] Embora os princípios contidos na DUDH possam ser robustos e duráveis, o contexto mudou dramaticamente.

Isso exige uma abordagem ecossistêmica e não uma abordagem sintomática simplista para as questões que envolvem os direitos e deveres da presença e residência de alguém no ecossistema da Internet. Exige uma abordagem engajada dos setores envolvidos que combine o progresso na governança e regulamentações com a reconstrução do tecido social e do contrato social adequados.

CONTEXTO HISTÓRICO

A DUDH foi elaborada em um importante período histórico. Foi escrito durante o tempo da perseguição e da migração em massa de judeus europeus, a recusa das nações do mundo em conceder asilo aos migrantes, as limitações britânicas à imigração judaica para a Palestina, a guerra civil entre facções na Palestina, a solução resultante de dois Estados proposta pela ONU em 1947, e a fundação do Estado de Israel em 1948.[86] A questão agora é o que os artigos da DUDH significam neste momento, quando pessoas e outras entidades (comunidades, empresas, governos) fixam residência (migram) para o ciberespaços do ecossistema da Internet. A residência nos ciberespaços do ecossistema da Internet é simultânea à manutenção da residência nos Estados. Não podemos simplesmente traduzir a DUDH para o ciberespaço.

Por outro lado, não há necessidade de reformular a Declaração para a era digital, pois nossos direitos humanos fundamentais permanecem os mesmos e o desafio é como aplicá-los em um novo contexto. Devemos partir dos princípios por trás da DUDH e usá-los como auxiliares de navegação. Devemos contar com a DUDH para nos ajudar a compreender nossos direitos e obrigações no ciberespaço e como construir o respeito pela dignidade digital e pelos direitos dos outros. Devemos também examinar o que precisa ser codificado em pactos formais com relação aos direitos e deveres no ciberespaço, e o que precisa se tornar parte do tecido social e do contrato social subjacente.

Artigo 13:(1) Toda a pessoa tem o direito de livremente circular e escolher a sua residência no interior de um Estado.

Artigo 13:(2) Toda a pessoa tem o direito de abandonar o país em que se encontra, incluindo o seu, e o direito de regressar ao seu país.

O ponto central de qualquer discussão dos Artigos 13 a 15 com relação aos direitos e deveres é revisitar as noções de nação e Estado, conforme elas se relacionam com os ciberespaços do ecossistema da Internet, um assunto já abordado na Parte 1. O Artigo 13:(1) é definido dentro da estrutura do Estado, enquanto o Artigo 13:(2) é definido dentro da noção de país.

85. Ver The Economic Consequences of the Peace, escrito pelo economista britânico John Maynard Keynes e publicado em 1919. Seu apelo por políticas multilaterais foi ignorado após a Primeira Guerra Mundial, mas foi fundamental para o crescimento do multilateralismo após a Segunda Guerra Mundial.

86. Após a Segunda Guerra Mundial, os redatores da DUDH enfrentaram uma situação histórica de imensa complexidade. O domínio britânico da Palestina, confirmado pela Liga das Nações, entrou em vigor em 1923. Para escapar da perseguição na Europa, a imigração judaica para a Palestina ocorreu em ondas, resultando em motins palestinos e árabes em 1920 e 1921. Os britânicos impuseram cotas de imigração para judeus. A Lei de Imigração dos EUA de 1924 proibiu a imigração de judeus para os Estados Unidos. A perseguição na Polônia e na Hungria deixou essas comunidades judaicas com poucas opções de migração. Em 1938, várias centenas de milhares de judeus migraram para a Palestina. Entre 1939 e 1945 as atrocidades nazistas causaram a morte de aproximadamente seis milhões de judeus e, no final da guerra, a migração ilegal acelerou-se. Os britânicos pediram ajuda à ONU e o Comitê Especial das Nações Unidas sobre a Palestina (UNSCOP) propôs "um Estado Árabe independente" e "um Estado Judeu independente". A resolução foi adotada pela ONU em 1947 e seguida pela inação. David Ben-Gurion proclamou a independência de Israel em 1948. É nesse contexto que os redatores da DUDH redigiram os Artigos 13-15.

CIBERESTADO: CONCEITOS BÁSICOS

No ciberespaço, vivemos em construções tecnológicas e sociais e em territórios virtuais. Inicialmente, esses eram os sites que visitávamos e as plataformas sociais (e-mail, mídia social) que usávamos. Cada vez mais, eles agora incluem o universo crescente da Internet das Coisas (IoT) com seu imenso poder de rastreamento e arquivamento de dados. Cada um desses espaços online pode ser comparado a nações em termos de seu processo e controle de dados. Muitas empresas de tecnologia digital agem em seu relacionamento com os Estados como se elas fossem nações por direito próprio.[87] Como as nações do mundo real, os territórios digitais são influenciados e definidos por fatores políticos, econômicos, geográficos, étnicos, religiosos, idiomáticos. Quais são, ou deveriam ser, nossos direitos e obrigações como cidadãos digitais nos territórios digitais do ciberespaço?

Nossa residência digital nos ciberespaços do ecossistema global da Internet contrasta fortemente com nossa residência digital onde fisicamente moramos. Os governos têm soberania e autoridade sobre o ciberestado doméstico. Pessoas e entidades têm cidadania digital e residência definidas pelo Estado. Eles também agora têm uma residência digital semelhante a uma nação no ecossistema global da Internet. No entanto, a governança cibernética, comumente chamada de "governança da Internet" (GI), está em sua infância em ambos os níveis, em termos de abrangência e significado.

Abordagens para a soberania no ciberespaço remontam a 1996, quando John Perry Barlow publicou sua "Declaração da Independência do Ciberespaço".[88] "Vamos criar uma Civilização da Mente no Ciberespaço. Que ela seja mais humana e justa do que o mundo que seu governos criaram".

O estado atual da governança da Internet, em sua infância, não atingiu o status de um ciberestado com mecanismos definidos de governança cibernética. Da mesma forma, a Internet perturbou as normas de comportamento das estruturas sociais predominantes no final do século 20, resultando em grandes rupturas no tecido social e danos ao contrato social subjacente. Reparar o tecido social e chegar a um acordo sobre uma nova base de contrato social é um complemento essencial para o desenvolvimento da governança digital e da cidadania digital. Esta é uma prioridade urgente do momento.

Um Estado justo é construído pela vontade política e engajamento de seus cidadãos. Construir as camadas do ciberestado, do local ao global, exigirá metas aspiracionais compartilhadas e visão entre as partes interessadas. As etapas necessárias para criar um sistema de governança digital dentro do ciberestado de um país estão enraizadas na Constituição do Estado e nas instituições associadas para o desenvolvimento de políticas e sua implementação no mundo literal. Esse trabalho é desafiador e se beneficiará ao começar com os princípios que sustentam a DUDH.

O poder e a legitimidade da governança cibernética derivam do reconhecimento da soberania de um Estado e seu direito de governar o ciberespaço doméstico.[89] Dentro da cidadania de um país, a cidadania digital nacional está sob a governança desse ciberespaço doméstico. Ao mesmo tempo, pessoas e entidades têm uma residência global no ciberespaço e podem ter residências locais em outros países.[90] Isso levanta a questão da migração digital e a capacidade de alguém mudar a residência digital entre Estados e governos, à vontade.

87. Gigantes da tecnologia como Amazon, Facebook e Google se comportaram em parte como se fossem suas próprias nações digitais globais. Alguns (Amazon) até mesmo apropriando-se de nomes de territórios, refletindo suas intenções de operar em escala global e, na ausência de um ecossistema de governança global da Internet, atuar como nações digitais responsáveis apenas por si mesmas.
88. John Perry Barlow "Uma Declaração da Independência do Ciberespaço", *https://www.eff.org/cyberspace-independence*. (Ironicamente, Barlow apresentou sua declaração em Davos, onde o Fórum Econômico Mundial (WEF) reúne-se anualmente e tenta moldar seu próprio ciberestado capitalista). Ao mesmo tempo, Nexusweb declarou sua independência como o primeiro país virtual no ciberespaço e publicou sua própria Declaração de Independência: *https://web.archive.org/web/19970102014217/http://www.inter-nexus.com /nexusweb/declare1.html*. Para informação mais detalhada sobre a Declaração de John Perry Barlow, ver *https://en.wikipedia.org/wiki/A_Declaration_of_the_Independence_of_Cyberspace*
89. Há espaço para alguma aplicação extraterritorial aqui. Na área de abuso infantil, por exemplo, os países podem processar cidadãos por crimes sexuais contra crianças, sejam eles perpetrados no país ou no exterior.
90. Por exemplo, quando a UE implementou o Regulamento Geral de Proteção de Dados (GDPR) em 2018, o Facebook moveu milhões de contas para fora da Irlanda para tirá-los do alcance do Regulamento.

Ao mesmo tempo, isso deixa em aberto nosso entendimento do que significa cidadania digital em nível global. ICANN, responsável pela segurança e estabilidade do endereçamento da Internet global, tem um lema que afirma: "Um mundo, uma Internet". O que isso significa em termos de cidadania digital global, cidadania digital doméstica e governança de um ciberestado ainda está para ser definido. Idealmente, isso será determinado de acordo com e com a ajuda dos princípios da DUDH.

A RESIDÊNCIA NO CIBERESPAÇO REQUER CIDADANIA DIGITAL CAPACITADA

O Artigo 13:(1) dá a todos o direito à liberdade de movimento e residência, dentro das fronteiras de um Estado. Residência e cidadania não são necessariamente iguais, portanto o Artigo 13 não trata dos direitos e deveres relativos à cidadania. A residência no ciberespaço opera tanto dentro do Estado como globalmente fora do Estado.[91] Idealmente, deveria haver apenas um conjunto de políticas e regulamentos do ciberestado, uma cidadania digital para todos. No entanto, os Estados podem e fazem distinção entre residência e cidadania. Eles podem ter políticas diferentes para cada um, políticas que também diferem das de outros Estados. No nível global, não é o caso. No ciberespaço global, todos são residentes globais e, por extensão, cidadãos globais. Não há como diferenciar os dois. Não há como reconhecer a residência global mas negar a cidadania global.

Os Estados estão em processo de construção de suas políticas e regulamentos para o ciberespaço nacional e para os direitos e deveres dos cidadãos e residentes nacionais, virtuais ou literais, nos ciberespaços nacionais. Este foi o motivo que levou o Facebook a mover seus arquivos de usuários para fora da Irlanda no início da GDPR. Os assinantes permaneceram residentes do ecossistema da Internet, mas não tinham mais residência na Irlanda.

Agora entramos em um período de construção da governança do ciberespaço. Conforme os países e regiões agem, há um alto grau de consulta e alguma colaboração. Esperançosamente, eles serão guiados por princípios como os da DUDH e as políticas de boa governança prevalecerão. Na Parte 1 deste texto, afirmamos: "Hoje, o ciberespaço confere a cada um de nós uma cidadania dupla, mas inseparável, física e digital. Mesmo que não conheçamos o ciberespaço, ou não possamos ou decidamos não usar nenhuma das tecnologias digitais, ainda somos cidadãos digitais com direitos (e correspondentes deveres)". O acesso ao ciberespaço torna-se um direito humano, que indiretamente está consagrado nos direitos humanos fundamentais da DUDH.

No nível do ecossistema global da Internet, a questão da cidadania digital global é mais complicada em uma frente e mais fácil em outra. A expansão explosiva da Internet tornou todos residentes de fato e cidadãos globais no ciberespaço. Os direitos e obrigações da cidadania digital global ainda não foram definidos. Além da questão-chave de quais direitos e obrigações devem acompanhar essa cidadania, está a questão-chave de quem deve estar envolvido na formulação desses direitos e obrigações.

É aqui que o DUDH afirma-se de duas maneiras. Os princípios da DUDH constituem os princípios-chave que devem ser consagrados em uma declaração de direitos digitais, ou mais apropriadamente, os direitos de cidadania digital global. Em segundo lugar, todas as estruturas de governança global provavelmente serão consagradas em tratados internacionais ou multilaterais. É improvável que venham de algum tipo de ciberestado abrangente.[92] É essencial para a governança do ciberespaço que as ferramentas de formulação e execução de políticas estejam disponíveis para garantir que os cidadãos digitais globais tenham autonomia nos processos de formulação de políticas, nunca sejam privados de seus plenos direitos (e deveres) de cidadania e de

91. Isso é um pouco como os direitos de alguém em alto mar. Alguns desses direitos foram consagrados em acordos multilaterais de "direito do mar", outros são protegidos pela cidadania nacional e pelos esforços de proteção dos Estados relevantes e, para alguns direitos, não há proteção legal. Por exemplo, no caso de esforços de resgate quando piratas sequestram navios no mar, muitas vezes é difícil determinar quais direitos são aplicáveis.
92. Embora alguns possam desejar uma abordagem de governo mundial que respeite e imponha a cidadania digital global, não é realista acreditar que os Estados abririam mão da soberania para a criação de uma estrutura de governança digital global. É mais provável que o caminho de curto prazo seja internacional e multinacional.

desfrutar de uma residência segura e protegida nos ciberespaços da Internet.

Para delinear entre a cidadania digital nacional e a cidadania nos ciberespaços do ecossistema da Internet, usamos o termo cidadania digital para a primeira e cidadania digital global para a segunda. Em ambos os casos, a democracia efetiva exige cidadania engajada, cidadania digital engajada e cidadania digital global engajada. Aqui, nosso foco está na cidadania digital global engajada multissetorial.

Existem iniciativas estatais e do setor privado para criar cercas em torno de seções do ciberespaço.[93] A criação de ciberespaços isolados vai de encontro à própria natureza e às forças do ciberespaço. Deve-se resistir a tais esforços, visto que desvalorizam os próprios pontos fortes do ecossistema da Internet como ferramenta para a compreensão e o desenvolvimento humanos. Esses espaços murados diminuiriam a cidadania digital global, estabelecendo uma cidadania digital de segunda classe que careceria de acesso aos direitos de alguém como cidadão digital global.

OPTAR PELA EXCLUSÃO: UM ENIGMA

O Artigo 13:(2) refere-se ao direito de deixar qualquer país, inclusive o próprio, e retornar a esse país. Em um nível, isso apresenta um problema simples. Com os avanços em serviços de governo com a governança eletrônica, é mais fácil para os cidadãos engajarem seus governos e se engajarem na governança. Isso também significa que aqueles sem acesso digital adequado têm sua cidadania reduzida. Isso ressalta a necessidade de tratar o acesso digital como um bem público e não apenas mais um consumível privado. No entanto, é virtualmente impossível tornar-se "não residente" em um ciberespaço nacional. Mesmo ao sair fisicamente de um país, a pessoa está sujeita a permanecer sujeita aos direitos e deveres de cidadania digital desse país, mesmo no exílio. Existem muitos exemplos que mostram como é difícil ou mesmo impossível para muitos apagar suas pegadas digitais.

A residência no ciberespaço é, obviamente, totalmente composta de dados, dados marcados com identificadores pessoais. Esses dados vão muito além da entrada de dados pessoais na nuvem de dados por meio de ações transacionais deliberadas. Inclui dados coletados do comportamento de uma pessoa, à medida que ela navega e movimenta-se pela Internet. Mais importante, cada vez mais, também inclui dados ambientais da simples presença física da pessoa. Dados ambientais são dados de telefones celulares, veículos, Internet das Coisas (IoT), vigilância de terceiros e uma miríade de outras fontes.

Esses dados, pessoais ou não, são amplamente marcados com identificadores e usados para construir perfis. É cada vez mais usado em algoritmos fechados de IA para construir personas digitais, usados para marketing, monitoramento e uma ampla gama de outros usos.[94] Embora o Artigo 13:(2) caracterize o direito de sair, no ciberespaço não há para onde ir, nenhum lugar para esconder-se. Ser um residente digital vem com o fato de estar vivo, com residência possivelmente após a morte e até antes do nascimento.[95] O desejo final de alguém pode ser manter a residência digital para sempre.[96] Isso torna o acesso protegido aos direitos e deveres da cidadania digital ainda mais importante.

ASILO DIGITAL: DIREITOS, OBRIGAÇÕES E DEVERES

Artigo 14:(1) Toda a pessoa sujeita a perseguição tem o direito de procurar e de

93. Por exemplo, ver: "A Rússia diz que testou com sucesso uma alternativa nacional para a Internet global", *http://www.circleid.com/posts/20191227_russia_has_tested_country_wide_alternative_to_the_global_internet*
94. A área de software de reconhecimento facial aprimorado por IA é um caso em questão aqui. A China usa essa tecnologia para monitorar o comportamento humano e manter um cartão de pontuação de "crédito social" dos indivíduos. Várias entidades comerciais estão compilando classificações de scorecard (crédito, seguro, saúde, direção) usando práticas de negócios digitais e técnicas de coleta de dados que levantam sérias questões legais e de direitos humanos (privacidade).
95. Ver *https://iapp.org/news/a/pregnancy-tracking-app-drawing-privacy-scrutiny* e *https://www.gamingtechlaw.com/2018/09/iconsumer-deceased-persons-gdpr-data-protection.html*
96. *Ver o mausoléu digital em https://www.google.com/search?client=firefox-b-d&q=black+mirror+san+junipero*

beneficiar de asilo em outros países.

Artigo 14:(2) Este direito não pode, porém, ser invocado no caso de processo realmente existente por crime de direito comum ou por atividades contrárias aos fins e aos princípios das Nações Unidas.

O ciberespaço, por sua natureza, é uma rede de redes baseadas em padrões técnicos comuns que operam no nível técnico independente de quaisquer padrões éticos. Com muitas políticas, regras de conduta e práticas culturais diferentes, o que pode ser permitido em um contexto, pode ser inaceitável ou a causa de perseguição em outro. O que é considerado normal e saudável em uma sociedade aberta pode estar sujeito a censura ou punição sob um regime repressivo.

O direito à liberdade de asilo digital pode ser complicado e precisa ser explorado. Se dentro de uma residência digital alguém foi perseguido ou impedido de acessar, a migração digital ainda deixa a pessoa literalmente aberta à perseguição.[97] Para que o asilo digital tenha significado, pode ter que ser acompanhado por migração física.

Os problemas surgem aqui. Pode haver asilo digital com algumas proteções? Os crimes digitais no exterior podem estar sujeitos à jurisdição territorial da residência física de alguém?[98] Se uma persona digital for perseguida em um espaço digital por entidades que exercem poder político sobre esse espaço, ou se houver uma incapacidade dos poderes políticos de proteger essa persona digital, quais direitos são relevantes aqui? O que significa "direito de sair"?[99] Como o direito de asilo garante o direito à proteção? Se existe um dever de asilo nos espaços digitais, o que isso significa?

Além disso, a residência digital estrangeira pode ser como a dupla cidadania e existir para fins diferentes do asilo. A residência digital pode ser a presença de uma pessoa dentro de um país, apesar de a pessoa não ter cidadania literal.[100] Que direitos o residente de asilo digital tem dentro dos direitos e deveres literais do país anfitrião?

Embora, em princípio, deva existir a extensão do direito de asilo aos residentes digitais, há muito trabalho a ser feito para entender o que é necessário para os direitos e obrigações da residência digital, cidadania digital e asilo digital.

ASILO E MIGRAÇÃO: CRIMES POLÍTICOS E ATOS CONTRÁRIOS

O Artigo 14:(2) restringe a aplicação de pedidos de asilo a situações em que o pedido não seja baseado em um crime político ou em atos contrários aos propósitos e princípios da ONU. No entanto, não é fácil definir o que constitui um crime político. A definição é influenciada tanto pelo contexto quanto pelo ponto de vista do observador, seja o observador pessoas ou instituições:

"[...] um crime político ou ofensa política é uma ofensa que envolve atos ou omissões manifestos (quando há o dever de agir), que prejudicam os interesses do Estado, de seu governo ou do sistema político. Deve ser diferenciado de crime estatal, em que são os Estados que violam tanto suas próprias leis criminais quanto o direito internacional público".[101]

Os Estados podem definir crimes políticos como qualquer comportamento percebido como uma ameaça, real ou imaginária, à sobrevivência do Estado, incluindo violência e não-crimes de

97. Há desafios em aberto aqui. Quanta privacidade deve prevalecer em torno da propriedade do nome de domínio? A propriedade anônima pode esconder criminosos, comportamento predatório e outros. A propriedade revelada pode expor grupos vulneráveis a ataques de inimigos e regimes repressivos. Mesmo a atual controvérsia em torno da venda do registro .org pela Internet Society para um fundo de capital privado levantou questões sobre as proteções concedidas aos detentores de nomes de domínio .org de ativistas sociais. Sobre esta controvérsia, ver C. A. Afonso, "A crise do .org é reflexo de uma crise sistêmica no DNS?", *https://nupef.org.br/node/86*

98. Por exemplo, cidadãos e residentes permanentes canadenses envolvidos em exploração sexual de crianças proibida em um país estrangeiro podem ser processados no Canadá, mesmo que não tenham sido condenados no país estrangeiro.

99. Não pode significar simplesmente o direito de se desconectar quando o acesso é cada vez mais visto como parte integrante dos direitos humanos e digitais. Seria como dizer que se pode escapar das restrições à cidadania literal parando de respirar.

100. A Estônia está oferecendo residência digital (e-residência): *https://en.wikipedia.org/wiki/E-Residency_of_Estonia*

101. Um claro exemplo de crime estatal foi a perseguição de minorias na Alemanha nazista: *https://en.wikipedia.org/wiki/Political_crime*

oposição violentos. Essa criminalização pode restringir uma série de direitos humanos, direitos civis e liberdades. Sob tais regimes, uma conduta que normalmente não seria considerada criminosa per se é criminalizada de acordo com a conveniência do grupo que detém o poder.[102] Os crimes políticos no contexto da DUDH são considerados um abuso dos direitos humanos. Asilo é o mecanismo que protege os direitos humanos contra o poder arbitrário do Estado, seja ele impulsionado por forças políticas, econômicas, religiosas ou outras. Estender essa noção à proteção da residência digital e da cidadania é um dos desafios da agenda global de políticas e governança da Internet.

Os propósitos e princípios da ONU são declarados nos dois primeiros capítulos da Carta da ONU.[103] Ela identifica "membros", "pessoas" e "Estados amantes da paz" que promovem e encorajam o respeito pelos direitos humanos e pelas liberdades fundamentais para todos sem distinção de raça, sexo, idioma ou religião. Povos e Estados são tratados aqui, mas o enfoque final está nos direitos das pessoas. Como no caso dos crimes políticos e do trabalho da própria ONU, o padrão para medir e avaliar o comportamento é a DUDH. Quaisquer atos contrários aos direitos humanos são atos contrários aos propósitos e princípios das Nações Unidas. Essas proteções precisam ser estendidas às personas digitais e à residência nos ciberespaços do ecossistema da Internet.

DENUNCIANTES E A NECESSIDADE DE PROTEÇÕES

Os denunciantes digitais são um exemplo de uma área que precisa de uma análise mais aprofundada e uma exploração à medida que detalhamos os direitos, deveres e proteções em relação à integridade das atividades digitais. Na outra extremidade do espectro, os fornecedores de informações perdidas, "notícias falsas" e informações maliciosas também exigem atenção e responsabilização por suas ações.[104] Esta é uma área complicada e difusa – por isso nos deteremos em vários incidentes recentes.[105]

Muitos Estados veem a publicação de informações classificadas, ou não classificadas, mas embaraçosas, cada vez mais de fontes digitais, não como um crime político, mas como uma atividade criminosa que não merece a proteção do Artigo 14:(1).[106] Quando se trata de denunciantes no contexto do ciberespaço, nomes como Snowden, Assange e Manning vêm à mente.[107] A questão é se seus atos de denúncia merecem proteção e asilo literal ou são crimes apolíticos que não estão sujeitos à proteção dos direitos humanos.

Snowden descreve sua motivação claramente: "[...] Meu único motivo é informar o público sobre o que é feito em seu nome e o que é feito contra ele".[108] Snowden qualifica isso, dizendo que a divulgação de informações deve ser "justificada e servir ao interesse público".[109]

102. Ver *https://wikimili.com/en/Political_crime*
103. *https://www.un.org/en/charter-united-nations*
104. Em ambos os casos, isso pode resultar em estar sujeito à violência física ou envolver-se em atos de violência física. Os mundos literal e digital são partes de uma única realidade maior.
105. Covid19 é um novo exemplo interessante e importante. A velocidade e o volume de desinformação que surgiram sobre a Covid19 têm sido impressionantes. Como passar de uma Internet saturada de desinformação a uma ênfase em um "espaço comum de informações" baseado em evidências, verdade e integridade? De certa forma, este tornou-se uma oportunidade excepcional para a Internet, usando novas abordagens para lidar com circunstâncias da pandemia na velocidade da luz. Processos digitais e atores digitais (empresas, organizações, governos e indivíduos) surgiram como cruciais para as formas como combatemos as doenças. Em outro nível, as práticas emergentes estão levantando questões sobre políticas, práticas e comportamento que terão de ser abordadas quando a sociedade não estiver mais em pé de guerra lutando contra o surto do vírus Covid-19.
106. Pode ser percebido como uma ameaça à autoridade política do Estado se indivíduos distribuírem material contendo informações não censuradas, o que prejudica a credibilidade da mídia de notícias controlada pelo Estado. Ver *https://en.wikipedia.org/wiki/Political_crime*
107. Edward Joseph Snowden vazou informações altamente confidenciais da Agência de Segurança Nacional (NSA) em 2013, depois de ver o Diretor de Inteligência Nacional, James Clapper, mentir sob juramento ao Congresso ao negar que a NSA conscientemente coleta dados sobre milhões de americanos. Em 20 de maio de 2013, Snowden deixou os Estados Unidos para buscar asilo físico e permanece no exterior, com residência permanente na Rússia. Julian Paul Assange, o australiano que fundou o Wikileaks, publicou uma série de vazamentos fornecidos pelo analista de inteligência do Exército dos EUA, Bradley/Chelsea Manning. Depois de uma série de ações de asilo e complicações legais, Assange enfrenta uma acusação legal nos Estados Unidos e continua encarcerado na prisão britânica de Belmarsh em Londres. Chelsea Elizabeth Manning, a ativista americana, denunciante e ex-soldado do Exército dos EUA, foi julgada em corte marcial em 2013 por violações da Lei de Espionagem dos EUA e outros crimes após a divulgação de documentos militares e diplomáticos ao Wikileaks, e foi condenada à prisão em 2017 – em março de 2020 um juiz federal ordenou sua libertação.
108. Laura Poitras, Glenn Greenwald, video, 9-junho-2013, *The Guardian*, Londres.
109. Laura Poitras, Glenn Greenwald, Ewen MacAskill, "Edward Snowden: o denunciante por trás das revelações de vigilância da NSA", 9-junho-2013, The Guardian, Londres.

Em contraste, o governo dos EUA argumentou que a maior parte do conteúdo "[...] não teve nada a ver com expor a supervisão governamental de atividades domésticas. A grande maioria dele estava relacionada às nossas capacidades militares, operações, táticas, técnicas e procedimentos".[110]

Em 2013, Snowden foi parcialmente reconhecido quando um juiz federal dos EUA determinou que a coleta de metadados de telefones do país pela NSA era provavelmente inconstitucional.

Assange e Wikileaks não impuseram critérios sobre quais documentos publicar. Eles publicam dados disponíveis do que eles percebem como "poderes" e deixam o resto do mundo decidir. Eles veem o Wikileaks agindo como uma "caixa de depósito" para garantir que jornalistas e denunciantes não sejam processados por divulgar documentos sensíveis ou confidenciais.

De acordo com o Wikileaks, seu objetivo é "trazer notícias e informações importantes ao público [...] Uma de nossas atividades mais importantes é publicar material original junto com nossas notícias para que leitores e historiadores possam ver evidências da verdade".[111] Este é um terreno jurídico complicado em nível nacional, e mais ainda em nível global. Ele cruza as fronteiras nacionais e as fronteiras entre o digital e o literal. Ilustra a necessidade de um diálogo engajado entre as várias partes interessadas, desde partes interessadas literais e digitais até legisladores e sistemas judiciais, um diálogo que deve preceder qualquer pressa em legislação e regulamentos, tanto a nível nacional como global.

RESIDÊNCIA DIGITAL E OS DIREITOS E OBRIGAÇÕES DA CIDADANIA DIGITAL

Artigo 15:(1) Todo o indivíduo tem direito a ter uma nacionalidade.

O advento das tecnologias digitais criou uma nova realidade importante, o espaço para uma residência digital nos ciberespaços do ecossistema da Internet. Considere a residência digital e como as questões levantadas se relacionam com a DUDH. Para começar, as tecnologias digitais são uma faca de dois gumes.[112] Praticamente todos os vestígios da presença de alguém no ciberespaço são marcados de forma exclusiva com a persona literal de alguém. A identidade virtual de uma pessoa e as várias personas digitais construidas por outros com a ajuda de IA facilitam a integração em novos contextos virtuais e literais de maneiras que não podemos aprovar ou desejar. Isso resulta na oferta de identificadores exclusivos para outras pessoas muito além de nossas noções contemporâneas de privacidade e segurança pessoal.[113]

A nacionalidade, como cidadão ou residente de um Estado, é um conceito fundamental importante da DUDH.[114] Ela define a relação jurídica de uma pessoa com o Estado, atribuindo ao Estado jurisdição sobre a pessoa. Por sua vez, a pessoa goza da proteção de direitos e deveres do Estado. A proteção de direitos e deveres e o respeito pelos cidadãos/residentes e pelo Estado dentro do domínio da residência digital de alguém no ciberespaço é uma área que exige um diálogo multissetorial para explorar as questões e o envolvimento dos vários grupos de interesse no desenvolvimento de políticas.

110. General de Exército Martin Dempsey, Presidente do *Joint Chiefs of Staff*, depondo no *House Armed Services Committee*, março de 2014.
111. Vazamentos de denunciantes podem ser usados para iluminar a verdade ou influenciar os resultados. No início da campanha presidencial dos EUA de 2016, o Wikileaks divulgou documentos relativos à candidata do Partido Democrata, Hillary Clinton. A comunidade de inteligência dos EUA e uma investigação do Conselho Especial concluíram que o governo russo realizou a invasão para interferir nas eleições presidenciais de 2016 nos EUA.
112. Sobre o uso de dados de identidade para perseguir requerentes de asilo, ver *https://www.nytimes.com/2019/10/02/magazine/ice-surveillance-deportation.html*
113. Mesmo a ideia de uma identificação digital permanente é objeto de muito debate. Os benefícios estão sendo comparados a um Estado-babá ou de vigilância observando e intrometendo-se em todos os aspectos dos assuntos pessoais. Essa preocupação é ampliada quando se trata de aplicativos como software de reconhecimento facial aprimorado por IA vinculado a redes de câmeras ubiquas. A atual pontuação pessoal chinesa de "crédito social", baseada em vigilância em massa digital e por vídeo, é um exemplo de tais práticas.
114. A ONU vê como um de seus papéis centrais fazer cumprir o direito à nacionalidade, pois este implica na proteção dos direitos humanos de cada indivíduo em um padrão mínimo, estabelecido na DUDH. Isso reflete-se na grande quantidade de tratados, resoluções e agências da ONU trabalhando sobre o assunto. Ver *https://www.ohchr.org/EN/Issues/Pages/Nationality.aspx*
115. Infelizmente, isso frequentemente acontecia às custas de populações nativas vistas como não tendo nenhum direito e, em alguns casos, consideradas menos do que humanas.

Artigo 15:(2) Ninguém pode ser arbitrariamente privado da sua nacionalidade nem do direito de mudar de nacionalidade.

O mundo está novamente no meio de uma grande migração. De 1850 a 1950, cem milhões de pessoas migraram, principalmente da Europa para áreas coloniais e áreas de população escassa.[115] Estamos à beira de outra grande migração. A agitação social e as mudanças climáticas resultaram em 70 milhões de pessoas deslocadas à força, muitas das quais com poucas perspectivas de "voltar para casa" de qualquer maneira significativa.[116] A migração resulta de fatores de pressão e de atração. Embora a maioria dos migrantes existentes tenha sido "pressionada" por distúrbios políticos, as estimativas sugerem que centenas de milhões a mais serão "empurradas" pela mudança climática nos próximos 20-30 anos.[117]

O Artigo 15 foi motivado pela massa de migrantes decorrente dos terríveis eventos da Segunda Guerra Mundial. Refugiados fugindo de perseguições e dificuldades econômicas enfrentaram uma recepção hostil, mas encontraram destinos acolhedores em outras partes do mundo. Cada vez mais os migrantes são "pessoas deslocadas" presas em uma existência indeterminada em favelas e campos de refugiados, sem ter para onde ir. Eles podem reter a nacionalidade literal ou se tornarem efetivamente apátridas. Privados dos direitos de sua nacionalidade literal anterior, eles têm pouca esperança de mudar de residência ou nacionalidade literal.

Existe alguma margem para melhorar esta situação através da extensão da cidadania digital? Há muito trabalho em andamento em torno da atribuição de documentação de identificação digital aos refugiados para o gerenciamento de serviços imediatos. Muitos foram deslocados sem documentação pessoal e são efetivamente apátridas. No processo de um refugiado, uma identidade digital pode compensar a falta de identificação, mas não pode restaurar a capacidade de exercer os direitos e obrigações de uma identidade literal e deixar em aberto a questão de para que serve uma identidade digital na ausência de uma identidade literal?

Isso deixa em aberto a questão de saber se há algum espaço para melhorar essas situações pessoais por meio da extensão e aplicação da cidadania digital. A resposta curta é que ninguém sabe. Isso depende de como o mundo trata a constituição dos direitos e deveres da cidadania digital, e na ausência de direitos de residência literal, esta é outra área a ser explorada.

Há um pouco mais a explorar em relação aos artigos 15:(1) e 15:(2) da DUDH que serão tratados na Parte 5, juntamente com uma exploração dos artigos 16 e 17 da DUDH. O que está claro até agora é que a DUDH pode e deve servir como referência para a construção de uma compreensão de como devemos abordar os direitos e deveres da cidadania digital, em particular a cidadania digital global, e como precisamos de um diálogo com várias partes interessadas sobre como lidar com os desafios desses direitos e deveres que são exclusivos dos ciberespaços digitais do ecossistema da Internet.

Também reiteramos nossa posição de que não existe um modelo único para o desenvolvimento de nossa compreensão e abordagem da cidadania digital. É necessário o envolvimento multissetorial, tanto para identificar o melhor caminho a seguir quanto para obter a adesão das partes interessadas ao caminho percorrido e aos mecanismos escolhidos.

O caminho a seguir não pode ser completamente regulatório e exigirá atenção para restaurar o tecido social, com possíveis reparos diferentes em diferentes ambientes, e reconstruir o contrato social subjacente para abraçar as atividades humanas em ambas as nossas realidades humanas digitais e literais.

Além disso, e além de como essas tarefas são realizadas no nível nacional em Estados individuais, será necessário haver uma combinação de ação internacional e multilateral para avançar. Esse progresso, embora iluminado por uma perspectiva histórica e especialização, terá que vir do engajamento de múltiplas partes interessadas que foi possibilitado pelos ciberespaços digitais do ecossistema da Internet. Tentar contornar ou causar

115. Infelizmente, isso frequentemente acontecia às custas de populações nativas vistas como não tendo nenhum direito e, em alguns casos, consideradas menos do que humanas.
116. https://www.unhcr.org/figures-at-a-glance.html
117. https://www.climateforesight.eu/migrations/environmental-migrants-up-to-1-billion-by-2050

um curto-circuito nessa rota resultará em atrasos e no risco de falha.

PARTE 5: ARTIGOS 15-17

Já discutimos os direitos e obrigações da cidadania digital. Revisamos agora o Artigo 15 para examinar a cidadania digital e a governança empoderada da Internet, para avançar para os direitos a uma família e propriedade. Em seguida analisamos o Artigo 16 que contribui para a qualificação do real e do virtual. Por fim recorremos ao Artigo 17 para discutir a pertinência da conceituação de propriedade digital.

CIDADANIA DIGITAL CAPACITADA: GOVERNANÇA DA INTERNET E UM FUTURO MELHOR

Este trabalho examina o que a DUDH nos diz sobre o que poderiam ser, e talvez o que deveriam ser, nossos direitos e obrigações nos espaços digitais do ecossistema da Internet. Em todas as comunidades, não é provável que haja um caminho único ou um arranjo único de mecanismos. Aqui, propomos apenas um ponto de partida aspiracional, começando com partes interessadas digitais engajadas como indivíduos e membros de comunidades.

Esta parte do texto está sendo escrita em um momento em que o mundo está dominado por uma pandemia global que está desencadeando doenças e mortes causadas por vírus em uma escala nunca vista em mais de um século.[118] Esta pandemia é uma crise econômica e de saúde , e uma crise na qual contamos como nunca antes com tecnologias digitais para levar adiante nossas vidas pessoais, econômicas e públicas. O acesso à Internet se tornou uma questão quase literal de vida ou morte. As realidades do espaço digital estão impactando e sendo afetadas pela pandemia tanto quanto nossas realidades literais e biológicas. Há uma compreensão crescente de que o virtual e o literal são partes integrantes de nossas realidades individuais e coletivas.

Esta crise está opondo as preocupações de saúde pública às preocupações econômicas, refletidas no debate sobre como equilibrar as estratégias de saúde (testes, isolamento, distância social) com a saúde da economia (empregos, renda, produção). Também está levantando questões em torno dos regulamentos e diretrizes políticas como complementos ou em competição com as normas sociais de comportamento. Essas questões sempre residem logo abaixo da superfície nas discussões sobre cidadania da Internet e políticas da Internet. Como decidimos o tradeoff, sob incerteza durante esta pandemia, quando pensamos em obrigar a proteção da sociedade ao bem comum, equilibrada com os direitos e deveres das pessoas? Vamos lidar com isso por um momento.

> ***"O bem comum é sobre como nós vivemos juntos em comunidade. É sobre os ideais éticos que nós buscamos juntos, os benefícios e encargos que nós compartilhamos, os sacrifícios que nós fazemos uns pelos outros. É sobre as lições que nós aprendemos uns com os outros sobre como viver uma vida boa e decente".*** *– Michael Sandel, filósofo político de Harvard* [119]

"Nós" aparece cinco vezes na definição de Sandel do bem comum. Em contraste, a DUDH é altamente focada no indivíduo, no "Eu".[120]

A definição, a defesa e o exercício dos direitos e deveres de uma pessoa como tal nunca ocorrem fora de seu pertencimento a uma comunidade maior. Enquanto os direitos estão voltados para a pessoa, os deveres estão voltados para a comunidade. A relação entre a pessoa e a comunidade nunca foi mais relevante para a política social e o comportamento social do que na era digital de hoje.

A noção tradicional de comunidade é fortemente

118. Isto está sendo escrito no Dia Mundial da TB (Tuberculose). Seríamos negligentes se não nos lembrássemos que a tuberculose é uma doença mais persistente e contínua, com 10 milhões de novos casos em 2019 e 1,5 milhão de mortes. Chama menos atenção porque suas vítimas tendem a ser os pobres e marginalizados nas margens da economia global.

119. *https://www.nytimes.com/2020/03/24/opinion/covid-ethics-politics.html*

120. Este não é o momento nem o lugar para explorar o equilíbrio entre os direitos individuais e o bem comum na DUDH, a não ser observar que a DUDH estava sendo redigida imediatamente após e sob a sombra de um período de alguns dos mais notórios violações dos direitos e da dignidade das pessoas na história da humanidade.

limitada pelo tempo e espaço e moldada pela experiência histórica. O alcance abrangente e global da Internet significa que, na realidade (literalmente), a presença e residência de uma pessoa estão em várias comunidades que operam no tempo e no espaço. As residências simultâneas online dos povos variam de espaços antigos a comunidades "pop-up" extemporâneas, como a multiplicidade de tais "reuniões" na atual pandemia de Covid-19.

O local global e instantâneo da Internet apresenta um ponto de partida aspiracional para envolver as partes interessadas digitais na formulação de políticas e comportamento para direitos individuais e obrigações sobre como as comunidades vivem juntas.

Os direitos individuais, dentro da governança da Internet, não vêm da simples imposição de um modelo de governança predeterminado ao ecossistema da Internet. Nem pode um tecido social de comportamento aceitável ser simplesmente desejado. Não são decisões simples, como decidir sobre dirigir em qual lado da estrada. Estabelecer os direitos e deveres da cidadania digital provavelmente será um processo de duas etapas.

O primeiro estágio envolverá a identificação e a adesão a um conjunto de princípios básicos, muito parecidos com os da DUDH. A segunda etapa será o processo de mudanças legislativas e comportamentais ao longo do tempo, mudanças que concretizam os direitos e deveres da cidadania digital de uma pessoa, tanto em nível nacional quanto global. Assim como os direitos e deveres da cidadania nacional literal se desenvolveram e mudaram ao longo do tempo, a cidadania nacional digital passará pelo mesmo processo.

É provável que a cidadania digital global se desenvolva em duas direções, para cima a partir do refinamento da cidadania digital nacional e para baixo a partir de princípios e ideias, começando com a noção de uma cidadania digital global que existe além e parcialmente separada da cidadania digital nacional.

Os processos usados para definir a cidadania digital não podem ser independentes do processo de governança usado para governar um país e definir a cidadania digital literal. Isso sugere que os processos usados para definir a cidadania digital são limitados pelos processos de governança existentes e também têm o potencial de abordar algumas das falhas contemporâneas dos processos de governança em países democráticos.

O atual ecossistema da Internet é uma mistura tóxica de boas informações e análises, envenenada por abundantes doses de informações ruins, notícias falsas e mentiras. É um pouco como o estado da medicina no final do século 19, quando os medicamentos variavam de remédios populares a remédios benignos não testados, vendedores de óleo de cobra e os venenosos.

Em nível nacional, os direitos e deveres de uma cidadania digital passarão a ter o mesmo status legal que a cidadania literal. O inverso pode não ser, e não precisa, ser o caso. A Estônia é um país com um forte regime de residência digital. Um estrangeiro pode adquirir uma residência eletrônica digital nacional sem ser um residente literal do país. Um residente digital pode não ter direitos literais de residência.[121]

O desafio diante de nós agora é: quais devem ser os direitos e obrigações da cidadania digital de um residente digital?

Não existe uma resposta pré-embalada "pronta para uso" para essa pergunta. Os direitos e obrigações da cidadania digital global e estadual são, e devem ser, um trabalho em andamento, desenvolvendo-se de cima para baixo na forma de regras e regulamentos e desenvolvendo-nos de baixo para cima à medida que as normas de comportamento são tecidas no tecido social e contrato social implícito. As questões a serem abordadas aqui incluem:

- Como os direitos e deveres da cidadania digital global estão relacionados aos da cidadania digital nacional (em nível estadual)?

- Que níveis de envolvimento das partes interessadas são exigidos no processo de desenvolvimento de políticas em torno dos direitos e obrigações da cidadania digital?

Alguns argumentarão que há necessidade de algo semelhante a um Estado cibernético global supervisionando o desenvolvimento, a administração

e a aplicação dos direitos e deveres da cidadania digital global. Outros farão objeções, argumentando que tal abordagem é impraticável e um Estado cibernético global infringe a soberania do Estado.[122]

No entanto, existe um meio-termo - um com uma longa história em termos de lidar com questões em nível global. Esse meio-termo entre a ausência de governança global e uma governança global desagradável é o uso de acordos multilaterais.[123] Um possível caminho a seguir envolve a exploração de processos políticos (mecanismos) e esforços que envolvem o engajamento de múltiplas partes interessadas na base e o multilateralismo liderado pelo Estado no topo.[124]

Os Estados físicos desempenham um papel ambíguo quando se trata de proteger os direitos de cidadania digital. Eles estão desenvolvendo políticas relacionadas à cidadania digital nacional, enquanto tentam estender esse controle ao ciberespaço global. Essas estratégias estão fadadas a enfrentar dificuldades extremas no ciberespaço sem fronteiras do ecossistema da Internet. Essas questões se tornam ainda mais desafiadoras quando tais políticas nacionais inevitavelmente entram em conflito umas com as outras através das fronteiras jurisdicionais.

Enquanto os Estados não reconhecerem a natureza global sem fronteiras do ciberespaço, seus esforços para proteger seus cidadãos no ciberespaço global sempre serão inadequados. Será necessário que os Estados assinem tratados internacionais que regulamentam as relações digitais entre Estados literais para garantir que os direitos de seus cidadãos sejam respeitados no ciberespaço sem fronteiras.

Em um nível individual, a cidadania digital empoderada deve trazer o direito de acesso ao ciberespaço global, o direito de proteção do Estado e a obrigação do Estado de se envolver em esforços multilaterais para proteger os direitos digitais globais de seus cidadãos. Por outro lado, a interferência estadual no ciberespaço, como a remoção de redes, constitui uma abreviação dos direitos baseados em princípios de cidadania digital no ciberespaço nacional e global.[125]

O Artigo 15:(2) nos confronta com um enigma interessante no ciberespaço global. Embora a residência digital nacional e global de alguém possa ser protegida ou abreviada pelas ações de seu Estado e por acordos multilaterais, o que pode significar mudar a nacionalidade digital de alguém? Da mesma forma, dada a definição fluida de nacionalidade, pode-se muito bem possuir várias nacionalidades digitais. Se os Estados restringem arbitrariamente os direitos de cidadania digital no ciberespaço, quais são as opções do cidadão? É claro que se pode exercer uma participação engajada para tentar consagrar e proteger os direitos digitais. Pode-se resistir quando confrontado com táticas contrárias aos princípios universais consagrados na DUDH, ou consagrados em subsequentes pactos de cidadania digital global.

Alguém tem o direito ou a possibilidade de se separar? A resposta é sim e não. É possível se separar da jurisdição de um Estado pela emigração, mas não se pode se separar dos ciberespaços globais do ecossistema da Internet mais do que se pode se separar da gravidade da Terra. O simples fato de existir agora torna a pessoa um residente do ciberespaço global. É provável que alguém tenha residência antes mesmo do nascimento.

Isso significa que a presença de alguém é predeterminada, que tem o dever e a obrigação de se tornar voluntariamente um cidadão digital engajado

122. Há uma longa história de desconfiança em torno das noções de governança global, tanto porque pode infringir a soberania nacional quanto os direitos e obrigações pessoais garantidos pela jurisdição do Estado. Podem-se ver elementos dessa desconfiança e desagrado nos argumentos pró-Brexit que sustentam a saída do Reino Unido da Comunidade Europeia.

123. O multilateralismo surgiu como um mecanismo pós-Segunda Guerra Mundial baseado nas falhas em torno da cooperação global que assolaram o mundo, com consequências terríveis, entre a Primeira Guerra Mundial e a Segunda Guerra Mundial. Ver *The Economic Consequences of the Peace*, escrito pelo economista britânico John Maynard Keynes e publicado em 1919. Seu apelo por políticas multilaterais foi ignorado após a Primeira Guerra Mundial. Ele foi fundamental para o crescimento do multilateralismo após a Segunda Guerra Mundial.

124. Os exemplos incluem os processos multissetoriais da Organização Internacional do Trabalho (OIT) e os vários acordos multilaterais sobre o mar, a atmosfera, o espaço e outras questões mais específicas. O que pode faltar é o engajamento multissetorial adequado ao longo dos processos de formulação e implementação de políticas.

125. O papel da Internet durante a pandemia Covid-19 sublinhou o crescente entendimento que o acesso à (ou presença na) Internet é um serviço essencial, e cada vez mais visto como um elemento essencial do bem comum, para viver uma vida boa e decente

nos ciberespaços do ecossistema da Internet a partir do momento em que for capaz de uma ação medida e deliberada. Isso não significa um envolvimento da infância nos processos de governança, mas significa um aprendizado e compreensão progressivos do envolvimento com base na integridade em políticas e normas comportamentais que o tornam um cidadão digital responsável e engajado dos ecossistemas nacionais e globais da Internet.[126]

DESENCANTO, GOVERNANÇA DIGITAL E CIDADANIA DIGITAL ENGAJADA

Não se pode optar por sair do ciberespaço mais do que se pode optar por sair da gravidade. Pode-se, no entanto, ficar desencantado com uma residência digital, seja aquela residência digital em que se possui cidadania literal ou uma das várias residências virtuais em comunidades. Pode-se ficar alienado da governança e dos processos socioeconômicos que cercam uma residência digital específica. A maneira como os indivíduos são tratados em sua residência digital tem consequências em suas vidas literais. Pode promover o envolvimento como partes interessadas do cidadão ou o desligamento como cidadãos digitais alienados.

As três fontes de frustração, decepção e preocupação são:

1. mecanismos de governança subdesenvolvidos e normas sociais (embutidos no contrato social da sociedade e no tecido social) que falham em facilitar uma existência segura e protegida na vida literal e virtual de uma pessoa.

2. falta de confiança na integridade dos negócios digitais e práticas de governança à medida que afetam o pessoal (por exemplo, privacidade e segurança). Aqui - a confiança vai além da privacidade e da segurança para confiar na Internet não apenas de uma perspectiva de infraestrutura, mas como uma fonte confiável de informações, comércio eletrônico, etc. A recente fraude associada à nossa atual crise Covid-19 é um bom exemplo de como o a confiança na Internet pode ser corroída se o abuso não for tratado.

3. a ausência de diálogo adequado com as partes interessadas e engajamento no planejamento de políticas, na implementação e na captura e uso das lições aprendidas.

A falta de um mecanismo de governança apropriado e de um contrato social adequado entrelaçado no tecido social pode ser explicada, senão desculpada, pela relativa novidade dos ciberespaços do ecossistema da Internet.

A resultante falta de confiança das partes interessadas e a integridade questionável de muitos negócios digitais e práticas de governança são claramente questões a serem abordadas. O progresso em ambos depende da melhoria do engajamento das partes interessadas no planejamento, implementação e avanços com base nas lições aprendidas.

O desafio em questão é claro. É passar de uma residência desencantada e indiferente para a cidadania engajada no ciberespaço, uma mudança para uma residência engajada que vê os direitos e obrigações da cidadania digital codificados nos níveis apropriados de governança e comportamento aceitável entrelaçados no tecido social.

Aqui, o foco está nos direitos e obrigações em nível global, nos espaços e regiões do ecossistema global da Internet que estão além do alcance de Estados individuais, aqueles espaços onde a residência pode ser em várias comunidades. O progresso aqui provavelmente exigirá cooperação por meio de mecanismos multilaterais, intergovernamentais e internacionais.

A resposta contemporânea às questões de privacidade e segurança pessoal e ao envolvimento com negócios digitais questionáveis e processos de governança é o refrão comum: "alguém deveria fazer algo sobre isso".

O refrão apresenta problemas e abordagens

126. Deve-se observar que o aprendizado envolvido em ser um cidadão digital nacional e global engajado e responsável provavelmente terá lições mapeadas de como ser um cidadão literal nacional responsável e engajado.

sugeridas. O "aquilo" referido no refrão raramente é claro o suficiente para ser o alvo do engajamento das partes interessadas no processo político. É necessário um discurso mais amplo para especificar e atribuir prioridade à lista "aquela" para o desenvolvimento de políticas. É "isso" privacidade de dados pessoais, notícias falsas, análise defeituosa ou o quê? Como a solução pode ser uma mistura de ações de governança e uma reconstrução do tecido social e do contrato social subjacente para acomodar novos comportamentos nas novas realidades da residência digital no ecossistema da Internet?

O "alguém" é igualmente problemático; quem é esse, quem deve fazer o quê? A residência digital no ecossistema global da Internet não está sob a jurisdição dos regimes existentes de governança soberana. Qualquer que seja o processo usado para decretar a política, ele deve passar por algum mecanismo de governança. Isso exigirá uma combinação de instâncias multilaterais, intergovernamentais e internacionais. Esse processo terá que encontrar um equilíbrio entre o que precisa ser codificado e o que deve ser nutrido em um tecido social e um contrato social aprimorados digitalmente.

O "algo" é o elemento mais problemático do refrão. O mecanismo de governança deve operar por meio de um local de participantes soberanos. O algo, como políticas, regulamentos ou o que quer que seja, deve ajudar a definir e respeitar os direitos e deveres da residência digital e da cidadania digital e contribuir para a reconstrução do tecido social e do contrato social subjacente.[127] Como essas são questões difíceis, o resultado freqüentemente volta a não fazer nada. Não fazer nada em face de um dano evidente não é uma abordagem sustentável e apenas corrói ainda mais a confiança do consumidor. Novamente – Covid-19 apresenta um bom estudo de caso para mostrar o quão dependentes todos nós somos neste momento da história da Internet para nos mantermos conectados, para aprendermos, para termos acesso à informação, entretenimento, e-comércio etc.

A noção de nacionalidade contida na DUDH, por mais ambígua que seja, pressupõe que a nacionalidade deve ser respeitada nos termos da lei soberana pertinente. Estender os princípios das proteções DUDH aos residentes digitais globais da Internet é a tarefa central da atividade de Governança da Internet, uma atividade que precisa ser baseada na base das partes interessadas e uma mistura de acordos legislados e esforços de tecido/contrato social.[128]

PRESENÇA E ASSOCIAÇÃO NA ERA DIGITAL

Embora a realidade virtual do ciberespaço e a realidade literal do espaço físico se misturem à realidade vivida mais ampla e contínua, há pontos na DUDH que nos lembram das principais diferenças entre o virtual e o literal.

O Artigo 16, com foco no casamento e na família, é um bom exemplo disso.

> ***Artigo 16:(1) A partir da idade núbil, o homem e a mulher têm o direito de casar e de constituir família, sem restrição alguma de raça, nacionalidade ou religião. Durante o casamento e na altura da sua dissolução, ambos têm direitos iguais.***
>
> ***Artigo 16:(2) O casamento não pode ser celebrado sem o livre e pleno consentimento dos futuros esposos.***
>
> ***Artigo 16:(3) A família é o elemento natural e fundamental da sociedade e tem direito à proteção desta e do Estado.***

Quais são os análogos da família e do casamento no ecossistema da Internet? Além disso, as rupturas desta era digital nos lembram que o tecido social é uma colcha de retalhos, ocasionalmente necessitando de alterações e reparos.

Certas partes do Artigo 16 estão vinculadas aos

128. Embora este assunto não seja explorado em detalhes aqui, parte da reconstrução do tecido social e do contrato social provavelmente envolverá a educação em torno da "cidadania digital", o que significa uma combinação de compreensão dos processos de governança digital e o papel de cada um no ecossistema digital como um cidadão digital engajado.

princípios fundamentais da DUDH e são atemporais, enquanto outras partes refletem as normas sociais da época. Em seu cerne está o tratamento equitativo dos gêneros quanto aos direitos de união legal e proteção da sociedade e do Estado.[129] Uma possível relevância diz respeito às possibilidades de casamento digital, realizado online. Isso simula um casamento literal tradicional, mas e se um oficiante autorizado não estiver presente, o casamento tem legitimidade?[130]

Aqui há lições da atual pandemia de Covid-19. A doença Covid-19 pode surgir repentinamente e com consequências fatais. Muitos correm o risco de chegar à morte iminente sem um testamento, e a quarentena proíbe testemunhar assinaturas. Os governos se ajustaram rapidamente para aceitar testemunho remoto, por vídeo digital. O ponto desse exemplo é que o que era apenas aceitável literalmente será cada vez mais aceito virtualmente, no local digital.

Voltando ao Artigo 16 para percepções sobre o que são as "unidades fundamentais dos grupos da sociedade digital" e seus direitos "à proteção da sociedade e do Estado", o foco da DUDH está na família. Não é necessário focar necessariamente em "A família". Voltando ao artigo 11 da DUDH e à liberdade de reunião e associação, vários agrupamentos digitais, além das várias formas de casamento digital, podem ser considerados como tendo direito a tal proteção.

Personas digitais e agrupamentos de personas digitais (nações digitais) também precisam de proteção no ciberespaço para quaisquer fins que essas relações sejam formadas, desde que estejam dentro dos limites da lei. Esta é uma área premente e difícil, uma vez que os proprietários de sites de mídia social estão tomando decisões independentes, não transparentes e irresponsáveis sobre quais indivíduos e grupos podem ter residência em suas regiões do ciberespaço e quais personas digitais devem ser construídas ou permitidas que existam, com base em parte nos propósitos e intenções dos grupos e, em grande medida, nos interesses comerciais do provedor do site de mídia social.[131]

Esta é uma área em que se exige a reflexão e o diálogo, a fim de traçar normas de práticas empresariais aceitáveis, chegar a um consenso sobre as normas sociais aplicáveis e estabelecer mecanismos de resolução de conflitos.

PROPRIEDADE, POSSE E COMPORTAMENTO NO ECOSSISTEMA DA INTERNET

O advento dos espaços digitais no ecossistema da Internet gerou uma criação maciça de propriedades digitais e uma intensa "apropriação de território". Isso leva à necessidade de uma reflexão mais profunda sobre as noções da sociedade sobre propriedade, posse e uso da propriedade.

Em relação à propriedade (no mundo literal), o artigo 17 da DUDH é muito claro.

Artigo 17:(1) Toda a pessoa, individual ou coletiva, tem direito à propriedade.

Artigo 17:(2) Ninguém pode ser arbitrariamente privado da sua propriedade.

Seja qual for o conceito de propriedade nesses artigos, uma pessoa "individual ou coletiva" tem o direito de posse e o direito de não ser arbitrariamente privada de sua propriedade. Claro, a propriedade pode estar sujeita a uma infinidade de restrições, pactos e direitos, como no caso de

129. Nestes tempos, a sociedade está aos poucos ampliando suas noções e sua compreensão de gênero e do que constituem, sob a permissão e proteção da lei, estados de união legal perante a lei. Pode-se debater se a família é a unidade natural e fundamental de um grupo na sociedade. Outros agrupamentos sociais podem ser tão ou mais importantes, dependendo do contexto e das questões em questão. Há claramente um contexto diferente quando se considera os agrupamentos nos espaços digitais do ecossistema da Internet.

130. *https://www.independent.co.uk/voices/i-just-attended-the-first-stateless-digital-marriage-but-im-not-sure-if-it-can-change-the-world-a6782941.html*

131. Isso não quer dizer que não deva haver restrições, mas que as restrições devem ter alguma responsabilidade e recurso a processos de resolução de disputas. Um grupo que viola a lei (por exemplo, envolvido em abuso infantil) é fácil de lidar. Grupos que defendem casos da comunidade e preocupações de interesse público são mais problemáticos e portanto a presença e a exclusão devem ser guiadas por uma mistura de regulamentações, padrões da comunidade, transparência e mecanismos de resolução de disputas, e não apenas os lucros do fornecedor da plataforma

terras onde há regulamentos de zoneamento e direitos de água ribeirinha.[132]

Qual propriedade é menos clara no ecossistema da Internet? Quais são as "propriedades" das propriedades da Internet? Quais são os direitos e obrigações de posse de tais propriedades? A infraestrutura técnica do ciberespaço, as máquinas, cabos e satélites, os edifícios etc são claramente propriedades no sentido tradicional. Os serviços digitais oferecidos através dessa infraestrutura são uma área mais complicada. Muitos dos serviços só são habilitados por relações legais e regulamentares com governos. Técnica e legalmente, mesmo os nomes de domínio da Internet não são propriedade. Seu uso é feito por meio de um contrato de cessão de posse com um distribuidor de dominios ("registrar") da Internet, que tem um contrato com um registrador ("registry") que, por sua vez, tem um contrato com a ICANN.[133]

Cabos submarinos de propriedade privada precisam de direitos de aterrisagem na costa de um país. Os satélites e os sistemas terrestres sem fio precisam de acesso legal a uma largura de banda limitada de radiofrequência. As políticas governamentais sobre concorrência e monopólios podem ditar o acesso compartilhado pelos concorrentes e os termos desse acesso compartilhado. Existem divergências sobre os regulamentos e os termos de acesso, com base na extensão em que o acesso do usuário deve ser tratado como um bem público e os fornecedores devem ser tratados como serviços públicos regulamentados ou ser deixados ao sabor das forças de mercado.[134]

Muito do valor de uma presença no ecossistema da Internet vem dos direitos de propriedade e/ou acesso a ativos e processos digitais. Embora intangíveis no sentido literal, eles são reais no sentido substantivo, em termos do impacto das realidades da vida, comunidade, comércio e governança. Incluídos nesta cesta de intangíveis estão nomes de domínio, propriedade intelectual, processos digitais e a organização, armazenamento e uso cada vez mais intenso de dados arquivados. Embora a propriedade intelectual esteja incluída na definição de propriedade da DUDH, é importante que não sejam direitos isolados, mas devam ser equilibrados com outros direitos humanos. Por exemplo, se um intermediário da Internet receber uma solicitação de um detentor de direitos de propriedade intelectual hoje para cortar o acesso de uma pessoa à Internet com base em uma alegação de uso indevido, os direitos de propriedade no Artigo 17:(1) devem ser equilibrados com os outros direitos da DUDH. Essa demanda de suspensão deve ser equilibrada com o Artigo 11:(1), que afirma que

> ***Toda a pessoa acusada de um ato delituoso presume-se inocente até que a sua culpabilidade fique legalmente provada no decurso de um processo público em que todas as garantias necessárias de defesa lhe sejam asseguradas.***

Como uma realidade prática que fica clara por ter sobrevivido durante o tempo de uma pandemia global, encerrar o acesso à Internet significaria possivelmente desconectar da Internet um indivíduo, uma família inteira ou até mesmo uma comunidade mais ampla. A Internet é a única forma de os cidadãos digitais acessarem bens e serviços, participarem de sua educação e, para alguns, a única forma de se comunicarem com seus entes queridos. A rescisão do acesso à Internet com base no direito de propriedade entra em conflito com o Artigo 12 da DUDH, que afirma que ninguém deve estar sujeito a interferência arbitrária em sua família, casa ou correspondência. O Artigo 10 confirma que os cidadãos têm direito em plena igualdade a uma audiência justa e pública por um tribunal independente e imparcial, na determinação de seus direitos e obrigações. O Artigo 9 afirma que ninguém deve ser submetido a exílio arbitrário e, neste caso, a suspensão do acesso à Internet com base em alegações de terceiros sobre disputas de direitos de

132. Os direitos ribeirinhos definem um sistema de distribuição de água entre aqueles que possuem terras ao longo de seu trajeto.
133. Noções literais e virtuais de propriedade já estão causando atrito no ecossistema da Internet. Empresas (exemplo: Amazon) adquiriram nomes de domínio (como propriedade intelectual) antes que os países tivessem tempo de se opor e têm havido lutas contínuas entre países cujas características territoriais são cobiçadas por empresas que buscam esses nomes como propriedade intelectual corporativa.
134. Esses não são problemas cabulosos. Durante a pandemia de Covid-19, grandes populações que perderam o acesso à Internet por motivos políticos sofreram riscos de vida muito maiores devido à falta de informação e à incapacidade de usar a Internet e o serviço de telefone celular para ter acesso a serviços e suprimentos médicos essenciais.

propriedade resultaria em uma forma de exílio digital. O Artigo 26 reconhece os direitos de todos à educação, e o Artigo 27 reconhece o direito de participar de eventos culturais, os quais, na atual pandemia, estão disponíveis apenas por meio do acesso online.

A forma como os direitos e deveres da cidadania digital são definidos e respeitados depende de como cada um desses intangíveis é compreendido e tratado, tanto por meio de legislação e regulamentação, quanto por meio de normas comunitárias inseridas no tecido social e em seu contrato social subjacente. Conforme ilustrado pelos exemplos acima, a necessidade de obter esse equilíbrio é essencial.

Com relação ao escopo dos direitos de propriedade, os países podem até divergir sobre o que constitui "propriedade". A lei japonesa declara que "os dados são intangíveis e não estão sujeitos à propriedade de acordo com o Código Civil".[135] O Japão diferencia entre dados pessoais e não pessoais, bem como direitos de propriedade intelectual no ciberespaço digital. No entanto, a lei não aborda o fato que os chamados dados não pessoais, coletados de atividade não transacional (por exemplo, navegação) e de fontes ambientais (aplicativos digitais, Internet das Coisas, reconhecimento facial etc), são no entanto associados a pessoas. Esses dados são usados para construir personas digitais individuais para uma infinidade de fins econômicos, políticos e outros, sem a consciência nem o consentimento da pessoa envolvida.

O ecossistema da Internet é rico em propriedades, e propriedades potenciais, que têm um valor comercial considerável. A noção de propriedade intelectual – sejam marcas registradas, nomes comerciais, materiais sujeitos à proteção de direitos autorais ou proteção de patentes – envolve ativos virtuais que têm valor tangível como propriedades comerciais digitais. Grande parte desse valor tangível depende dos dados que fluem pela infraestrutura da Internet, dos aplicativos digitais usados para processá-los e dos usos finais para os quais são concebidos.

Isso apresenta uma série de questões sobre quais são os parâmetros dessas propriedades. Quais são os direitos e obrigações desses donos/proprietários? Quais são os processos aceitáveis no ciberespaço digital? Quais são os direitos e obrigações daqueles cujos dados são a matéria-prima que alimenta esses processos e dá valor a essas propriedades e processos? Que direitos o indivíduo tem sobre as personas construídas para avaliar seu comportamento e tendências pessoais, comerciais e políticas, e quais são os direitos sobre os usos dessas personas?

O que está claro aqui é que há uma rica agenda de trabalho a ser realizada com relação ao entendimento das noções de propriedade dentro do ecossistema da Internet. Esse entendimento é essencial para construir uma governança da Internet responsável e eficaz, bem como para tecer normas de comportamento aceitável no tecido social.

Esses entendimentos e acordos em torno dos mesmos são essenciais para a elaboração de regulamentações apropriadas para os direitos e deveres da cidadania digital no ecossistema da Internet. O envolvimento multissetorial é essencial na governança e é parte integrante dos esforços da sociedade para reconstruir um tecido social desestruturado e um contrato social subjacente que resulte em uma matriz de orientação para um comportamento aceitável no ecossistema da Internet.

É necessária uma estrutura de governança que produza governança efetiva da Internet e uma reconstrução do tecido social liderado pelas partes interessadas, a fim de identificar e proteger os direitos e deveres da cidadania digital engajada.

É importante lembrar que, embora os dados sejam virtuais, eles tornam-se tão reais quanto uma pedra em nossas mãos quando impactam nossas realidades individuais e coletivas. Os dados intangíveis tornam-se tangíveis pelo efeito que têm em nosso mundo literal. Como já discutido, os reinos digital e literal podem ser considerados "separados, mas inseparáveis". Juntos, eles constituem a realidade em que vivemos agora.[136]

135. O governo japonês, no entanto, ao mesmo tempo diferencia dados pessoais dos não pessoais. "Os dados são intangíveis e não estão sujeitos à propriedade de acordo com o Código Civil. Os dados não pessoais podem, em princípio, ser usados livremente – com base em contratos pessoais, por exemplo – exceto para propriedade intelectual legalmente protegida abrangida por direitos autorais, segredos comerciais ou outros estatutos legais". – Ministério da Economia, Comércio e Indústria, METI: https://www.meti.go.jp/english/press/2017/pdf/0530_002b.pdf

136. Rolf Landauer. "The Physical Nature of Information". 217 Physics Letters A 188, 188 (1996). Esta afirmação é baseada em seu artigo anterior "Information is Physical", 44 Physics Today 23-29 (1991).

PROPRIEDADE DE DADOS E ASSUNTOS RELACIONADOS À PROPRIEDADE INTELECTUAL: "MEU CARRO ME ESPIONA"

Nada se torna propriedade até que tenha valor de uso. Terras comuns de aldeias medievais inglesas e terras tribais em todo o mundo eram comunais. Foram "fechadas" (privatizadas) quando a exclusão e o direito de acesso trouxeram benefícios para alguns, enquanto diminuíam os direitos de outros. A propriedade e o valor dos dados estão passando por um movimento de "fechamento" semelhante como resultado de três fatores que estão surgindo ao mesmo tempo.

Os dois primeiros fatores são os saltos exponenciais na capacidade de armazenar e processar dados. O terceiro é o rápido crescimento da tecnologia de comunicações sem fio de quinta geração (5G) para redes celulares e outros dispositivos fixos ou móveis.

Juntos, eles expandem a capacidade da Internet das Coisas (IoT) na geração e compartilhamento de dados em tempo real.[137] Por exemplo, veículos autônomos compartilham dados nas velocidades necessárias para permitir o movimento autocontrolado em tempo real. Esses dados estão disponíveis em tempo real e são arquivados para outros usos. Registros históricos de veículos e telefones celulares já são padrão para rastrear "pessoas de interesse" na ficção da televisão, filmes e vídeos online populares, mas já têm sido usados por países como a Coreia do Sul para rastrear o movimento humano durante a pandemia da Covid-19 no esforço de administrar o contato e o isolamento.

Os dados veiculares armazenados incluem tempo, localização e processo e já são usados por fabricantes, seguradoras e outros.[138] Quem tem quais direitos sobre o quê e em que condições, em termos dos dados que produzo, e os dados capturados sobre mim por dispositivos ambientais? Meu carro, meu celular e meu monitor cardíaco, todos compartilham dados sobre mim com outros (quem?) em outro lugar no ecossistema da Internet. Compartilham com que finalidade?

Meu carro está me espionando, não tenho certeza para que, e provavelmente não gosto disso. Mesmo os dados considerados anônimos podem ser usados prontamente para reidentificar um indivíduo com apenas alguns elementos de dados adicionais. Este exemplo demonstra que a propriedade de uma "coisa" IoT (no caso, o carro) significa que possuir a coisa não estabelece propriedade de dados nem controle de dados.[139] As características das propriedades digitais, bem como os direitos e deveres dos produtores e controladores de propriedades digitais, são áreas de desenvolvimento contínuo de políticas. É crucial que esses processos políticos envolvam participação multissetorial efetiva, enquanto, ao mesmo tempo, a sociedade define as noções fundamentais dos direitos e deveres da cidadania digital.

Compartilhamos hoje territórios comuns tal como na vila medieval inglesa, se reconhecermos esses interesses comuns. A pandemia global levou alguns a reconhecer que os direitos de propriedade intelectual podem levar a obstáculos sociais para encontrar curas e tratamentos urgentes. Algumas empresas de tecnologia recentemente anunciaram que removerão bloqueios que protegem a propriedade intelectual e concederão licenças temporárias gratuitas para suas tecnologias patenteadas e protegidas por direitos autorais para

137. Há uma tendência de tratar a Internet das Coisas como todos os dispositivos e aplicativos conectados que surgiram depois do computador pessoal e do telefone celular. No entanto, em termos de funcionalidade e questões relacionadas à propriedade de dados, governança da Internet e os direitos e deveres de uma pessoa digital e literal, os computadores e telefones celulares devem ser considerados como pertencentes ao universo da Internet das Coisas.

138. Por exemplo, muitas jurisdições estão discutindo a instalação de câmeras de tráfego para ajudar a gerenciar fluxos de tráfego e multas de trânsito. Os fluxos de dados de veículos aprimorados por IA tornarão essas câmeras redundantes, e a questão política e legal será quem tem quais direitos sobre os dados gerados.

139. Em algumas áreas, isso já resultou em legislação e regulamentos. Os fabricantes de automóveis recusaram o acesso das oficinas licenciadas independentes aos manuais técnicos e dispositivos especializados para fazer a manutenção de seus veículos. Gradualmente, a legislação estadual dos EUA exigiu o direito das oficinas licenciadas de comprar os manuais e dispositivos. Um problema semelhante surgiu no setor agrícola. Atualmente, a parte eletrônica do trator John Deere só pode ser reparada por um técnico da John Deere. A John Deere argumenta que o trator é vendido, mas o software é cedido sob contrato.

permitir que outros busquem tratamentos e curas sem medo de ramificações legais por violação de direitos. O "Open Covid Pledge" (Compromisso do Covid Aberto) é um exemplo inovador de como os bens comuns globais podem ser invocados para proteger o bem público mais amplo quando ele é mais necessário.[140]

MERCADO DE DADOS E DIREITOS DO PROPRIETÁRIO/ CONTROLADOR DOS DADOS

Existem mercados maciços para dados, mercados para subconjuntos de dados específicos e mercados para os chamados *big data*. O uso de tais dados pode ser para aprendizado e pesquisa, como estudos epidemiológicos de saúde, para fins comerciais ou políticos, ou para propósitos de crimes cibernéticos. Mesmo quando os usos são proibidos, como quando as agências de aplicação da lei não têm permissão para usar aplicativos que rastreiam o uso de telefones celulares, as agências podem recorrer a terceiros que extraem, compram e vendem dados de torres de celular da operadora.[141]

Diferentes regiões do globo estão em diferentes estágios de avanço sobre legislação e regulamentos para lidar com propriedade intelectual, propriedade de dados e privacidade de dados. O GDPR da UE possui elementos de extraterritorialidade e impõe obrigações a organizações em qualquer lugar, desde que envolvam ou coletem dados relacionados a pessoas na UE. O Congresso dos Estados Unidos realizou audiências sobre questões de privacidade e propriedade de dados, mas houve pouco movimento em termos de legislação. Em 2019 o ex-candidato presidencial Andrew Young incluiu "dados como um direito de propriedade" como plataforma política central de sua campanha.[142] A proposta não progrediu. Tanto a UE quanto os EUA estão considerando uma revisão geral das leis de propriedade intelectual e proteção contra a responsabilidade de acordo com a Lei de Direitos Autorais do Milênio Digital dos EUA e a Diretiva de Comércio Eletrônico da UE. Em consequência, novos direitos de propriedade intelectual eventualmente poderão resultar em novas responsabilidades e impactar negativamente os cidadãos, bem como os direitos de uso da Internet.

Estamos no início das discussões necessárias sobre os direitos e termos de acesso aos dados, como esses direitos e termos são conciliados em relação aos direitos e obrigações da cidadania digital e como esses direitos são protegidos e essas obrigações são cumpridas. Os dados pessoais como um bem negociável, ou a sua utilização pelo controlador dos dados, arriscam o estabelecimento de uma forma de escravatura digital, onde uma persona digital está a serviço de outra. Isso constituiria não apenas um atentado aos direitos digitais de alguém, mas, em um mundo onde o digital e o literal são "separados, mas inseparáveis", constituiria um atentado aos direitos humanos fundamentais de uma pessoa sob a DUDH.

Nós nos concentramos no lado dos direitos da presença digital de alguém, a posse de propriedades digitais. Neste artigo, abrimos um pouco a porta sobre as obrigações digitais, mas pouco foi dito sobre as obrigações que vêm com a propriedade digital. Esse lado da moeda será tratado quando chegarmos ao Artigo 29:(2) da DUDH, que afirma:

> ***"No exercício deste direito e no gozo destas liberdades ninguém está sujeito senão às limitações estabelecidas pela lei com vista exclusivamente a promover o reconhecimento e o respeito dos direitos e liberdades dos outros e a fim de satisfazer as justas exigências da moral, da ordem pública e do bem-estar numa sociedade democrática".***

O escopo e a escala existentes de práticas de negócios digitais predatórias e de baixa integridade que operam nos ciberespaços do ecossistema da Internet não são desejáveis nem sustentáveis. Muitos deles violam as noções de decência e confiança que eram parte integrante do tecido social e do contrato social subjacente que construímos para nosso mundo

140. *https://www.law360.com/ip/articles/1265926/tech-titans-commit-to-freeing-ip-to-aid-pandemic-response*
141. *https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html*
142. *https://www.nytimes.com/2019/10/15/opinion/andrew-yang-privacy-internet.html*

literal. Os desafios aqui oferecem uma oportunidade de promover integridade nas práticas de negócios digitais e cultivar o aprendizado e a participação das partes interessadas engajadas nesses esforços. A novidade do contexto digital e a longa história de defesa dos direitos humanos universais oferecem uma oportunidade para a participação engajada de todos os setores na formação da realidade digital dentro dos princípios que orientaram a DUDH.

Nossa jornada até agora pela DUDH nos mostrou a necessidade de um processo de governança com seus alicerces em uma cidadania digital empoderada. Os princípios básicos da governança da Internet, em todos os níveis, podem basear-se amplamente nos princípios nos quais a DUDH se baseia.

À medida que continuamos e concluímos nossa jornada pelo restante dos Artigos da UHDR, entenderemos mais profundamente como esses princípios podem servir como blocos de construção para os direitos e deveres da residência digital e da cidadania nos ciberespaços do ecossistema da Internet.

PARTE 6: ARTIGOS 18-19

Nossa discussão agora explora os artigos 18 e 19 da DUDH. Os princípios da DUDH que orientam os direitos humanos em tempo e espaço literais servem como ponto de partida para os princípios necessários que orientam os direitos digitais no ecossistema da Internet. Aqui, além de lidar com a liberdade de pensamento e opinião no ciberespaço, exploramos alguns aspectos do desenvolvimento da governança da Internet e o trabalho do relator especial da ONU sobre a promoção e proteção do direito à liberdade de opinião e expressão.

> ***Artigo 18: Toda a pessoa tem direito à liberdade de pensamento, de consciência e de religião; este direito implica a liberdade de mudar de religião ou de convicção, assim como a liberdade de manifestar a religião ou convicção, sozinha ou em comum, tanto em público como em privado, pelo ensino, pela prática, pelo culto e pelos ritos.***[143]

O Artigo 18 da DUDH, com sua ênfase na religião e na crença, foi fortemente influenciado pelos terríveis eventos dos anos entre guerras na primeira metade do século 20. O Artigo 19 generaliza as preocupações e princípios encontrados no Artigo 18, e termina com as palavras proféticas para a era da Internet – por isso o repetimos aqui:

> ***Artigo 19: Todo o indivíduo tem direito à liberdade de opinião e de expressão, o que implica o direito de não ser inquietado pelas suas opiniões e o de procurar, receber e difundir, sem consideração de fronteiras, informações e idéias por qualquer meio de expressão.***

Nossas discussões exploraram a relação entre a DUDH e as estruturas sociais e políticas de países, nações e Estados. Os artigos 18 e 19 dão maior atenção ao papel e aos direitos do indivíduo. A liberdade de pensamento e opinião são essenciais para proteger a autonomia do indivíduo das demandas do Estado e para informar o Estado sobre os desejos de seus cidadãos.

As ações de um indivíduo podem ser classificadas em três categorias legais: proibidas, permitidas ou obrigatórias. Os Artigos 18 e 19 colocam a liberdade de pensamento e opinião firmemente na categoria permitida e limitam a capacidade de um Estado de proibi-los ou exigi-los. No entanto, surgem questões de contenção formal ou comportamental quando a opinião expressa é contrária a outros princípios da DUDH, por exemplo, o apoio ao racismo, à herança patrimonial e outras formas de discriminação, e a crescente questão da circulação de informações falsas em plataformas digitais.

MANIFESTAÇÃO DO INTANGÍVEL

O Artigo 18 protege não apenas o pensamento, a consciência e a religião, mas também suas manifestações por um indivíduo ou grupo. Quaisquer tentativas de proibi-los ou exigir conformidade são ilegais ou permitidas somente quando os direitos

143. O Artigo 18 é espelhado e ampliado pelo Artigo 18 do Pacto Internacional sobre Direitos Civis e Políticos. Ver *https://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx*. Os autores não alteraram o tratamento de gênero da redação original.

de terceiros são afetados.[144] Pensamentos, crenças, religião e dados digitais são intangíveis. Eles se tornam reais por meio de suas manifestações como ações e por meio de comportamentos sociais e estruturas e processos institucionais. Encontramos mais uma vez o princípio de separado, mas inseparável, conforme discutido na Parte 1 deste trabalho sobre a DUDH.

LIBERDADE DE PENSAMENTO NÃO SIGNIFICA LIBERDADE DE PENSAR PELOS OUTROS

Bertrand Russell refletiu sobre a liberdade de pensamento:

"O que torna um livre-pensador como tal não são suas crenças, mas a maneira como as mantém. Se ele as segura porque os mais velhos lhe disseram que eram verdadeiras quando ele era jovem, ou se as segura porque se não o fizesse ficaria infeliz, seu pensamento não é livre; mas se ele as detém porque, depois de pensar cuidadosamente, encontra um equilíbrio de evidências a favor delas, então seu pensamento está livre, por mais estranhas que suas conclusões possam parecer".[145]

O pensamento individual sempre estará exposto a influências externas, mas não deve refletir essas influências. Deve ser como uma luz que passa por um prisma, para se dividir em seus componentes, para avaliação crítica a partir do diálogo com os outros. O diálogo é necessário para determinar como meu pensamento afeta os direitos dos outros e para chegar a um consenso sobre como meu pensamento pode se manifestar em comportamento sem causar danos.

O pensamento livre não pode existir quando as informações/dados nos quais ele se baseia são corrompidos por desinformação. Historicamente, a desinformação, ou falta de informação, resultou de censura, repressão ou falta de acesso. Hoje, com facilidade de acesso e rapidez de disseminação, esse problema é agravado por rumores, notícias falsas e fatos falsos por meio do ecossistema da Internet. Isso impede, ou mesmo perverte, a avaliação dialógica e a construção de um consenso comum.

LIDERANÇA DE PENSAMENTO

O pensamento precisa da capacidade de descobrir o novo, de cruzar fronteiras e ser compartilhado sem medo de represálias. A liberdade de pensamento é a base da inovação e tem sido o principal impulsionador do progresso na era digital. No entanto, o local digital abre a espada de dois gumes da chamada liderança de pensamento impulsionada por líderes de pensamento "influenciadores" da mídia social, impactando em opiniões e comportamento.[146]

Não podemos subjugar nossa liberdade de pensamento às opiniões dos outros, especialmente quando em apoio acrítico à inovação técnica ou social. Não podemos curvar-nos a uma liderança que postula a superioridade de um pensamento sobre outro, independente de evidências, lógica e moralidade, ou pensamento que exige aceitação sem responsabilidade. A inovação com integridade é prejudicada pela liderança quando essa liderança busca preservar e fortalecer interesses especiais, frequentemente em detrimento dos direitos humanos e do bem-estar.

Um sinal de verdadeira inovação e liderança com integridade é que ela permite e nutre os processos de pensamento livre, avaliação, diálogo e consenso. Essas quatro etapas são essenciais para o processo de formulação de políticas sólidas de governança da Internet.

144. Legislação recente do governo da província de Québec (Canadá), que proíbe símbolos religiosos em alguns empregos do setor público, está sendo contestada e vista por muitos como uma violação dos direitos civis e contrária ao Artigo 18: *https://www.nytimes.com/2019 /06/17/world/canada/quebec-religious-symbols-secularism-bill.html*

145. Bertrand Russell. *The Value of Free Thought – How to Become a Truth-Seeker and Break the Chains of Mental Slavery.* Girard, Kan., Haldeman-Julius Publications: 1944.

146. Discutimos essa área sob inovação não regulamentada na Parte 3, na seção "Inocência presumida, mas culpa assumida". Ver também *https://www.merriam-webster.com/dictionary/influencer* e *https://pt.wikipedia.org/wiki/Celebridade_da_internet*

JUDICIÁRIO INDEPENDENTE

A DUDH considerou os tribunais competentes como um importante mecanismo de controle e equilíbrio.[147] Como a história mostrou, as facções dentro dos estados que buscam a autopreservação e o avanço de seu poder frequentemente restringem as capacidades dos tribunais nacionais. Portanto, em casos como crimes de guerra e crimes contra a humanidade, tais tribunais foram estabelecidos acima e além do Estado.[148]

O exercício do pensamento livre e de suas manifestações no ciberespaço requer, conforme discutido na Parte 3 deste trabalho, o reconhecimento sem discriminação e a ausência de meios arbitrários de repressão ou presunção de culpa. Essa liberdade só pode ser garantida dentro da governança da Internet quando essa governança é criada e mantida por meio do engajamento empoderado de todas as partes interessadas.

Os Estados têm sua própria jurisdição e soberania e exercerão controle sobre a governança doméstica da Internet. Assim como a governança doméstica de direitos humanos, com base nos princípios da DUDH, essas políticas e comportamentos devem respeitar os princípios por trás dos direitos digitais globais. Nunca haverá um ciberestado global no sentido de um estado digital independente com soberania sobre seu território digital. Mas os direitos da cidadania digital exigem os princípios de uma declaração universal universal de direitos digitais, apoiada por um judiciário internacional, empoderada por Estados e operando com sua própria independência jurisdicional. É aqui que se sobrepõem separadamente, mas inseparáveis. O envolvimento das partes interessadas no diálogo global, bem como no diálogo interno dos organismos nacionais e internacionais existentes, é necessário para chegar a um acordo sobre os princípios e mecanismos para acordos internacionais em torno dos direitos (e obrigações) da cidadania digital, para estabelecer instituições judiciárias e processos apropriados, e para informar a integridade comportamental.

LIBERDADE DE CONSCIÊNCIA

O direito à liberdade de consciência protege o indivíduo de ser forçado ou coagido a participar de uma atividade que vai contra seus valores. Ao acessar um serviço, ninguém deve ser recusado arbitrariamente, ou forçado a dar consentimento relutante, ou ser sujeito a discriminação. Esta é uma questão urgente quando trata-se de consentimento obrigatório aos termos do contrato para acesso a muitos dos serviços, aplicativos e atividades enfrentados por um cidadão digital no ecossistema da Internet.

Muitos aplicativos digitais, alguns deles vitais para o exercício de nossa cidadania digital empoderada, só estão disponíveis após concordar com termos e condições que são contrários aos interesses e direitos dos usuários. As tecnologias digitais e os termos sob os quais podem ser usados precisam estar em conformidade com os direitos humanos básicos, expressos como direitos digitais básicos. Coagir indivíduos a sacrificar ou comprometer seus direitos humanos e digitais por meio da negação de serviços, por exemplo, por meio de formulários de consentimento "legais" não razoáveis e a falha em divulgar totalmente os verdadeiros usos de dados pessoais, são antiéticos e comparáveis a dar a uma pessoa a escolha de optar pela escravidão ou morrer de fome.[149] O acesso universal à Internet deve ser um direito fundamental e não estar sujeito a restrições questionáveis sobre direitos e liberdades pessoais ou práticas de uso de dados digitais de integridade questionável.

LIBERDADE DE RELIGIÃO, PRESERVANDO A UNIDADE DE CORPO E MENTE

A liberdade de religião, tal como se manifesta e é exercida no ciberespaço, apresenta problemas especiais? Requer direitos e proteções especiais? A religião é uma tentativa de unir a natureza separada, mas inseparável, da mente e do corpo humanos, o chamado problema mente-corpo.[150] Como meu corpo físico relaciona-se

148. Ver a Corte Criminal Internacional: *http://www.icc-permanentpremises.org*

149. Pode-se traçar um paralelo com o fato de que na escravidão não existe um "bom dono de escravos". Em termos de uso que comprometem os direitos digitais, não existe algo como "integridade do provedor de serviço digital".

150. Ver *https://pt.wikipedia.org/wiki/Problema_mente-corpo*

com meu ser baseado na religião (virtual)? Construir as ligações entre o virtual e o físico é a chave para a segurança e a autopreservação da personalidade de alguém. A "residência" virtual de alguém no ecossistema da Internet apresenta questões semelhantes.

A religião, em sua essência, é virtual, com "residência" dentro de um espaço de crença. Para os crentes, esse espaço de crença é verdadeiro. Os não crentes expressam dúvida ou descrença. Religião e filosofia fornecem fundamentos e rituais para satisfazer múltiplas necessidades pessoais e sociais. Crentes e não crentes entendem que o impacto da religião na vida literal é real. A residência virtual de uma pessoa no ecossistema da Internet tem a mesma relação pessoal e social virtual-real.

Desafiar o sistema de crença religiosa de uma pessoa equivale a questionar o estado de mente e corpo de um crente. Desde as origens das comunidades religiosas, ameaças e exortações de líderes religiosos levaram seus seguidores a acreditar que atos extremos, como cruzadas, caça às bruxas e terrorismo, são necessários e justificados. Este "fascismo de pensamento" permite que múltiplos meios terríveis sejam implantados para atacar as crenças religiosas e perseguir aqueles que as possuem, quando essas crenças são diferentes das suas, como foi testemunhado em meados do século 20.

A DUDH coloca a religião no mesmo nível do pensamento e da consciência, e reafirma no Artigo 18 o direito de um crente de manter e "mudar de religião ou de convicção, assim como a liberdade de manifestar a religião ou convicção, sozinho ou em comum, tanto em público como em privado, pelo ensino, pela prática, pelo culto e pelos ritos". O princípio central aqui pode ser aplicado à noção e proteção de pensamentos e comportamento em uma residência digital.

CAPITALISMO E FASCISMO DE PENSAMENTO TECNOLÓGICO

No início do século 21, o capitalismo está sob o microscópio. A era recente da política neoliberal (pró-mercado) produziu importantes avanços tecnológicos e econômicos. Ao mesmo tempo, produziu concentrações extremas de renda e riqueza e aumentou a marginalização. Esses resultados estão levando a uma reflexão séria sobre se o capitalismo de mercado pode ser reformado ou precisa ser substituído, sem nenhuma ideia clara de como reformá-lo ou do que colocar em seu lugar.

Os sistemas de crenças satisfazem nossa necessidade de integridade física e espiritual, atuando como "sistemas de posicionamento global" pessoais e fornecem conforto e segurança. Eles também ajudam a tecer a estrutura da sociedade. O papel do capitalismo, como motor de tecnologia dentro desse tecido, é evidente. No entanto, seus impactos no rápido desenvolvimento do ecossistema da Internet estão levando a uma revisão crítica de seus impactos socioeconômicos e da integridade de suas práticas de negócios digitais.

Uma área de particular preocupação é o capitalismo de vigilância – a prática comercial digital emergente de coletar e monetizar dados digitais pessoais identificáveis. Isso levanta questões sobre a integridade das práticas de uso de dados digitais e como elas se relacionam com os direitos digitais e literais das pessoas. O processamento de dados digitais para o marketing de bens e serviços e para fornecer informações (válidas ou falsas) arrisca o uso da tecnologia digital a serviço do fascismo de pensamento. Esses riscos não são novos. Eles surgiram com a imprensa, com o rádio, com o cinema e a televisão. Os riscos aos direitos humanos representados por tais práticas no ciberespaço são maiores hoje, devido ao escopo, escala e velocidade com que as informações podem fluir na Internet. Podem haver razões e esperança para acreditar que a humanidade será capaz de lidar com esta ameaça, na visão de Russell:

> ***"... [Um] sumário final cuidadoso indica o comercialismo como o grande perigo para o pensamento livre futuro; mas parece legítimo esperar que os grandes interesses econômicos ligados à ciência, juntamente com a difusão da educação, impeçam qualquer retorno às superstições mais nocivas do passado".***[151]

Embora se possa esperar passivamente por

151. Bertrand Russell. "A History of Free Thought". *The Tribune* (Londres): 4 de junho de 1906. Ver *https://users.drew.edu/~jlenz/br-on-robertson1.html*

resultados de princípios com integridade, é melhor trabalhar na identificação de princípios e na formulação de políticas por meio do envolvimento da cidadania digital capacitada.

LIBERDADE DE PENSAMENTO, OPINIÕES FIRMES E GOVERNANÇA DA INTERNET

Exercitar a liberdade de pensamento no ciberespaço requer uma compreensão, quase uma mudança de paradigma, para pensar sobre a "residência" de alguém no ecossistema da Internet. É preciso pensar não apenas nos direitos digitais, mas também nos deveres (obrigações) digitais como cidadão da Internet. Como no caso da cidadania literal, os deveres evoluem e tornam-se parte do tecido social. A maioria não é obrigatória ou transmitida em políticas e regulamentos, mas desenvolve-se como parte das convenções sociais. Pessoalmente, mentir ou espalhar boatos falsos são práticas desaprovadas. Politicamente, votar é um ato de boa cidadania, mas geralmente não é obrigatório.

As opiniões expressas, como contribuição para o diálogo e o consenso, não devem conter falsidades ou lapsos flagrantes de lógica. Freqüentemente, eles não enfrentam sanções legais quando ocorrem. Esta é uma área difícil hoje em dia com relação às mídias sociais, onde falsidades são amplamente divulgadas, tanto inocentemente quanto com más intenções. Qualquer sistema de governança, incluindo a governança da Internet, depende de uma combinação dinâmica de políticas vinculantes e de comportamentos individuais e privados geralmente acordados mutuamente. As opiniões devem ser contribuições para o diálogo onde a sabedoria comum diz: "Uma pessoa tem direito à sua própria opinião, mas não aos seus próprios fatos".

Os processos políticos multicamadas, multilaterais e com várias partes interessadas incluem o diálogo como parte dos processos para determinar a política, esperançosamente com base no que é certo, justo e com base em fatos reais acordados. Existe um grande desafio para a sociedade aqui hoje. Muito do tráfego atual (não posso chamá-lo de diálogo) nas mídias sociais dos ecossistemas da Internet é livre de evidências, notícias falsas e até afirmações de conspiração infundadas. Esse tráfico não é muito mais do que um cabo de guerra em que as respectivas facções passam para ganhar adeptos e influenciar a política, muitas vezes sem saber os custos em termos de danos e o que está em jogo.

A liberdade de pensamento no século 21 envolve mais do que a liberdade das formas de perseguição que estão por trás dos Artigos 18 e 19. É sobre a integridade que entra nesses pensamentos à medida que se manifestam como opinião e ações. A era digital trouxe novos riscos à liberdade de pensamento e opinião.

Há um século Bertrand Russell escreveu sobre a "máquina de perseguição", que "garantiu o triunfo de suas próprias visões".[152] Um século depois, enfrentamos novas formas de "máquinas de perseguição" como residentes do ecossistema da Internet. A vigilância digital no sentido mais amplo, combinada com algoritmos de IA, cria perfis digitais de nós (personas digitais) para moldar as informações, os diálogos e os contextos que vemos no espaço digital. Isso está moldando nosso senso de identidade e de quem somos em um sentido virtual e literal.

Este é um sério ataque à nossa liberdade de pensamento e opinião agravado por uma mistura tóxica de práticas de negócios digitais (movidas pela ganância?) e enganosas (movidas pela falibilidade?), e por informações falsas ou equivocadas, conforme formamos opiniões e pensamentos socioeconômicos e políticos nos envolvemos em ações sociais e políticas.[153]

Onde o pensamento livre não é perseguido e onde o diálogo determina e respeita os limites

152. Bertrand Russell. "A History of Free Thought", op.cit.

153. Bertrand Russell, em Political Ideals (1917): "Todo o domínio do pensamento e da opinião é totalmente inadequado para o controle público; deve ser tão livre e espontâneo quanto possível para aqueles que sabem em que os outros acreditaram. O estado tem justificativa para insistir que as crianças devem ser educadas, mas não tem justificativa para forçar sua educação a prosseguir em um plano uniforme e ser direcionada à produção de um nível morto de uniformidade eloquente. A educação, e a vida da mente em geral, é uma questão em que a iniciativa individual é a principal coisa necessária; a função do Estado deve começar e terminar com a insistência em algum tipo de educação e, se possível, um tipo que promova o individualismo mental, não um tipo que por acaso se conforma com os preconceitos dos funcionários do governo".

dos direitos, há maior probabilidade de formação e manifestação de consenso. Isso pode ajudar a superar os obstáculos ao consenso, postados por visões de interesse próprio semelhantes a silos, e a criar novos comportamentos no ecossistema da Internet que apoiem uma governança da Internet baseada no livre arbítrio de cidadãos digitais empoderados.

A governança competente da Internet nascerá desse novo tipo de diálogo. Sua responsabilidade é possibilitar e educar o diálogo baseado na liberdade de pensamento e no respeito aos direitos dos outros. A responsabilidade da governança da Internet competente será apoiar a educação e o conhecimento como bases para pensamentos e opiniões, mas não para controlar pensamentos ou opiniões, ou delegá-los a algoritmos.[154]

O Artigo 19 é um dos principais artigos da DUDH e poderia ser chamado de "artigo da DUDH na Internet". Seu "sem consideração de fronteiras, informações e idéias por qualquer meio de expressão" prenuncia a Internet e expressa os valores fundamentais a serem aplicados às tecnologias de comunicação digital. Expressa um conceito-chave que conecta e une todos os seus artigos. Sua importância é destacada pela Comissão de Direitos Humanos das Nações Unidas, que em 1993 estabeleceu o mandato para o Escritório do Relator Especial.[155] Em 2008, essa relatoria substituiu a Comissão de Direitos Humanos e seu mandato continua a ser renovado. Mais recentemente (agosto de 2020), Irene Khan foi nomeada Relatora Especial da ONU para a Liberdade de Opinião e Expressão e é a primeira mulher a ocupar este mandato.[156] O anterior titular do cargo, David Kaye, resumiu o mandato e as atividades do relator desta forma:

> ***"Reunir todas as informações relevantes, onde quer que ocorra, de discriminação, ameaças ou uso de violência e assédio, incluindo perseguição e intimidação, dirigido a pessoas que procuram exercer ... contra profissionais no campo da informação ... ou para promover o exercício do direito à liberdade de opinião e expressão..." [157]***

Os relatórios do relator apresentados desde 2010 contêm uma grande riqueza de informações sobre tópicos relevantes sobre o direito à liberdade de opinião e expressão na era digital, tais como: discurso de ódio online, vigilância, IA, regulamentação de conteúdo, papel dos provedores de acesso digital, proteção de fontes e denunciantes, criptografia e anonimato, direito da criança à liberdade de expressão, proteção de jornalistas e liberdade de imprensa, questões do sistema de saúde, sistema de justiça criminal e novas tecnologias, segurança nacional, direitos das mulheres etc.[158]

Em declarações à Assembleia Geral 2017/18 2017/18, o relator David Kaye dirigiu-se aos Estados-membros sobre o estado-da-arte do Artigo 19. Os seus comentários resumem o que o Artigo 19 significa no contexto do ciberespaço:

> ***"No ano desde meu último relatório, a crise pela liberdade de expressão aprofundou-se em todo o mundo. Jornalistas foram assassinados, seus assassinos raramente ou nunca levados à justiça. Indivíduos foram presos meramente por postar críticas online a políticas ou autoridades governamentais. Nossa segurança online, essencial para nossa capacidade de tirar proveito da revolução digital, foi minada por governos e trolls privados e patrocinados***

154. Philip Alston, relator especial das Nações Unidas sobre pobreza extrema e direitos humanos, em sua "Declaração sobre a visita aos EUA" (Washington, 2017), expressou alarme com a ética questionável de "algoritmos de avaliação de risco de IA desenvolvidos pelo setor privado sendo usados para prever os pensamentos e intenções criminosas de uma pessoa". Usando "[...] instrumentos de avaliação de risco pré-julgamento atuarial, (APRAIs) [...] dados sobre o acusado, [são] alimentados em um algoritmo computadorizado e geram uma previsão da probabilidade estatística de a pessoa cometer alguma conduta imprópria no futuro..." Esta ferramenta de avaliação de "caixa-preta" "[...] levanta sérias questões de devido processo que afetam os direitos civis [principalmente] dos pobres no sistema de justiça criminal". Ver *https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22533*

155. Um relator especial é um especialista independente nomeado pelo Conselho de Direitos Humanos. Este cargo é honorário e o especialista não é funcionário das Nações Unidas nem pago por seu trabalho.

156. *https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/OpinionIndex.aspx*

157. Para o texto completo do mandato, ver: *https://www.ohchr.org/Documents/Issues/Expression/Statement_GA73_DavidKaye%202018.docx*

158. Para obter uma lista completa e outras indicações, ver: *https://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx*. A riqueza e o valor desses relatórios e declarações não podem ser subestimados.

pelo governo. A confiança do público na informação foi, e continua a ser, atacada por demagogos políticos e seus representantes. As ameaças aos ativistas da sociedade civil continuam inabaláveis, sujeitas a ataques digitais, vigilância, investigações e acusações infundadas, xenofobia e muito mais. E os atores corporativos no espaço digital são atacados por autoridades e ao mesmo tempo crescem em poder que, para muitos Estados e observadores, parece inexplicável e opaco".

Em 2017 Kaye fez recomendações específicas que estabelecem o caminho a seguir para os Estados-membros em relação à governança da Internet:

"Espero que os órgãos políticos das Nações Unidas, especialmente a Assembleia Geral e o Conselho de Direitos Humanos, e outras organizações intergovernamentais: (a) promovam a adoção de políticas de acesso à informação por meio de resoluções e outros mecanismos de governança; (b) assegurem o desenvolvimento de funções de monitoramento e supervisão; (c) forneçam informações abrangentes sobre os mecanismos de governança organizacional, incluindo processos de eleição e seleção ou nomeação, e credenciamento mais amplo e simples de organizações para participar e monitorar atividades organizacionais; (d) promovam o conhecimento do acesso às políticas de informação, inclusive por meio do fornecimento de informações claras em sites da Web e da divulgação e promoção ativas dessas políticas para funcionários e partes interessadas".[159]

Todos os relatórios e declarações incluem recomendações claras e apelos à ação aos Estados-membros e partes interessadas.

A crescente frustração por parte do relator especial é aparente. Suas recomendações são ignoradas e até mesmo contrariadas por ações tomadas pelos Estados-membros.[160] Ele prossegue:

"Peço desculpas por ter começado com uma nota sombria, mas embora eu passe alguns minutos descrevendo meu relatório formal, não poderia começar ignorando o grande sofrimento que principalmente os governos estão causando às pessoas em todo o mundo hoje. A repressão da expressão é a repressão da democracia e do Estado de direito. É a repressão da inovação, auto-exploração e conexão. Não posso recomendar com mais veemência que tomem medidas para reverter e resistir a essa tendência. Exorto seus líderes a falarem a linguagem do respeito por relatar como o guardião público crucial. Exorto-os a implementar de fato as importantes medidas normativas que o Conselho de Direitos Humanos adotou no início deste mês em sua resolução sobre a segurança de jornalistas. A ONU não pode continuar com compromissos de alto nível e implementação limitada. Essa é uma receita para o cinismo sobre o trabalho que vocês fazem aqui, e eu sinceramente espero que vocês possam mudar isso".[161]

DAR VOZ À DUDH NA GOVERNANÇA DA INTERNET

David Kaye prosseguiu apresentando uma discussão extensa e altamente recomendada em seu relatório de 2018 sobre os aspectos práticos da regulamentação do conteúdo online gerado pelo usuário.[162] Mas ele também conhece o jogo que os estados membros jogam. Eles querem ter uma boa aparência e ser tutores da DUDH, mas sem responsabilidade. Por esta razão, eles instalam cargos como relatores especiais e permitem que publiquem relatórios críticos, mas ao mesmo tempo garantem que os relatores e seus relatórios sejam absolutamente impotentes e não tenham

159. David Kaye, Relator Especial sobre a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão. Assembleia Geral - Terceiro Comitê, Item 69 (b & c), 24 de outubro de 2017, Nova York. Ver: *https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=22300&LangID=E*
160. Para um exemplo recente,ver: "U.N. Aprova a resolução para combater o crime cibernético apesar da oposição da UE, os EUA e outros": *http://www.circleid.com/posts/20191230_un_approves_resolution_to_combat_cybercrime_despite_opposition*
161. *https://www.ohchr.org/Documents/Issues/Expression/Statement_GA73_DavidKaye%202018.docx*
162. Relatório A/HRC/38/35 Ver: *https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/096/72/PDF/G1809672.pdf*

consequências vinculantes que obriguem a ação sobre as recomendações.

Os relatórios de Kaye são uma voz importante da DUDH dentro da ONU, a questão é como fazer com que seja ouvida. O relator reporta, em última instância, aos Estados-membros e aos seus cidadãos. Seus relatórios são importantes para todas as organizações do IG. Uma maneira de garantir que tenham um impacto real seria colocá-los na pauta para discussão nas principais sessões das reuniões anuais dos fóruns de governança da Internet, como IGF, WSIS e ICANN.[163] Os relatórios não devem ser apenas discutidos. As organizações devem relatar ao relator como suas instituições planejam tratar as preocupações do relator. As organizações não devem ser capazes de esquivar-se da responsabilidade quando os problemas de sua competência têm suas raízes na DUDH.[164]

LIBERDADE DE OPINIÃO E NOMES DE DOMÍNIO

Os sites, incluindo aplicativos de mídia social, rapidamente se tornaram meios cruciais e essenciais para exercer o direito de liberdade de opinião e expressão.[165] Os nomes de domínio facilitam (do que os endereços IP) o acesso aos sites. Os nomes de domínio também podem transmitir significado e valores, e apontar para conteúdo relevante. O Sistema de Nomes de Domínio (DNS) com mais de 1.200 domínios de nível superior de uso genérico (gTLDs) – como .org, .com, .net etc –, além de mais de 250 domínios de topo de países (ccTLDs) – cada com com milhares ou milhões de subdomínios –, fazem a ponte mnemônica entre a infraestrutura técnica e o conteúdo do ciberespaço.

O DNS, ao mapear nomes a endereços IP, e os motores de busca são os meios que dão vida ao acesso à Internet e à dinâmica do ecossistema da Internet. Sem o DNS, nas palavras do pioneiro da Internet Jon Postel, não há o "de onde para onde" que torne o ecossistema da Internet facilmente acessível.[166]

A importância dos nomes de domínio mudou nos últimos anos. Os mecanismos de pesquisa tornam o conhecimento do nome de domínio específico de um site menos necessário. Possuir um nome de domínio e manter um site não são necessários para que um agente divulgue conteúdo digital específico. Os usuários podem escolher entre mídias sociais e outras plataformas para hospedar suas operações e sua presença na Internet. Marcas e diálogos fortes baseados na Internet podem existir sem seu próprio nome de domínio, usando "hosts" como YouTube, Facebook, Amazon, LinkedIn e Shopify, ou uma ampla gama de outras mídias sociais.

A relevância dos domínios para a liberdade de expressão ainda é significativa. Para expressar uma opinião específica no ciberespaço, um indivíduo ou organização só tem controle total sobre o conteúdo com base na posse do nome de domínio e no controle de um determinado site. As palavras que substituem o endereço IP (numérico) de um site podem ter um significado. Isso é parte da lógica por trás da explosão exponencial de gTLDs, como .cat, .coffee, .farm, .fish, .xxx etc. Um nome de domínio terminado em .org transmite uma mensagem um pouco diferente de um nome de domínio terminado em .com. Mecanismos de busca e algoritmos de IA podem diminuir a importância dos nomes de domínio, mas uma mensagem contida em um site com seu próprio domínio pode carregar mais significado do que uma mensagem em uma plataforma de hospedagem com milhares de mensagens semelhantes ou contraditórias. Plataformas servem para a finalidade de seus criadores. Usá-las como base para o exercício da liberdade de informação e opinião pode significar restrições, manipulação e perda de controle.

163. Embora seja parte da missão da ICANN a segurança e estabilidade da Internet, ela está atualmente mantendo discussões internas sobre sua função na governança técnica da Internet (TIG) dentro de sua competência e na governança da Internet (IG) de maneira mais geral.
164. O Estatuto de Direitos Humanos da ICANN e o Quadro de Interpretação e Considerações relacionado (ver *https://www.icann.org/resources/pages/governance/bylaws-en* e *https://www.icann.org/en/system/files/ files / ccwg-acct-ws2-attach-3-hr-foi-final-recs-27mar18-en.pdf)* são exemplos de como interesses especiais defendem os direitos humanos da boca para fora, mas envolvem-se em evasões aos direitos humanos em espírito e ações.
165. Isso é óbvio quando se considera a rapidez com que líderes políticos, incluindo chefes de estado, têm recorrido às mídias sociais para transmitir mensagens, posições e até mesmo notícias falsas ao público e seus constituintes.
166. Scott Bradner, em sua palestra no NANOG 68, observou que a IANA, o órgão que gerencia as camadas técnicas de endereçamento da Internet, tratou de três tópicos, mas o que interessava à maioria das pessoas era: onde estava o dinheiro; onde estavam os problemas de marca registrada; onde os advogados estavam; onde estavam os políticos; onde estavam os que atreviam-se a propor políticas, e era tudo que a mídia noticiosa podia entender, ou pensar que sim.

A posse do nome de domínio tem seus riscos. Para grupos da sociedade civil, os termos de acesso aos dados de posse (nomes, localizações) podem sujeitar os ativistas a riscos de autoridades repressivas ou oponentes. Isso faz parte dos debates complexos e contínuos sobre privacidade e acesso ao banco de dados global de nomes de domínio conhecido como "Whois".

REFLEXÕES FINAIS

A linguagem e os princípios dos artigos 18 e 19 da DUDH são fortemente moldados pelos traumas (Primeira Guerra Mundial, Depressão, Holocausto e Segunda Guerra Mundial) e pelas violações dos direitos humanos na primeira metade do século 20. O desafio aqui é entender o que os princípios significam para a existência de alguém como residente do ecossistema da Internet, para os direitos e deveres de um cidadão digital no ecossistema da Internet e como esses princípios, direitos e deveres devem ser consagrados na governança da Internet e informar a integridade do comportamento no ecossistema da Internet.

Essas questões foram discutidas nesta reflexão sobre os artigos 18 e 19, mas é prematuro extrair as lições aprendidas. Essa tarefa está reservada para a peça final nesta exploração da relevância da DUDH para a residência digital e a cidadania digital no ecossistema da Internet e para a governança da Internet. Seguimos trabalhando. ■

Bruna Martins dos Santos *

Uma avaliação do Modelo de Responsabilidade de Intermediários do Marco Civil para o desenvolvimento da Internet no Brasil

I. O Marco Civil da Internet no Brasil

Construído entre os anos de 2007 e 2014, o Marco Civil da Internet[1] foi uma resposta direta à "Lei Azeredo"[2] (projeto de lei nº 84/99), que tinha como objetivo coibir a utilização maliciosa da Internet ao estabelecer penas duras que poderiam resultar na criminalização de condutas banais de usuários. Apesar dos debates em torno da Lei Azeredo estarem bastante conectados com os debates estadounidenses que resultaram em projetos como SOPA[3] e PIPA[4], pode-se dizer que ao combater a tentativa desproporcional de criminalizações promovidas pela Lei Azeredo, o Marco Civil da Internet acabou importando visões sobre responsabilidade de intermediários semelhantes (mas não integralmente coincidentes) com aquelas presentes na seção 230 do *Communications Decency Act*.[5]

1. Presidência da República. Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Ver *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm*
2. Presidência da República. Lei nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil (Marco Civil da Internet). Ver *http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm*
3. O SOPA, "Stop Online Piracy Act", é um projeto de lei que tramita no Congresso dos EUA e que trata de medidas antipirataria e proteção de propriedade intelectual. Ver *https://web.archive.org/web/20111209080021/http://judiciary.house.gov/hearings/pdf/112%20HR%203261.pdf*
4. O PIPA, "Protect IP Act", é outro projeto de lei que tramita no Congresso dos EUA, de teor parecido ao do SOPA, cujo objetivo é combater sites que vendem ou distribuem produtos piratas na Internet e violam direitos de propriedade intelectual. Ver *https://www.govtrack.us/congress/bills/112/s968/text*
5. *A Seção 230 é um dos trechos da lei americana que trata sobre "decência" (sic) nas comunicações e um dos alicerces do desenvolvimento da Internet no país. Aprovada em 1996, a Seção 230 basicamente prevê a isenção de responsabilidade para provedores de "serviços interativos de computador" que publiquem conteúdos fornecidos por terceiros. Ao compreender como papel do estado americano a promoção do desenvolvimento da Internet, preservação da característica competitiva do livre mercado, e encorajar o desenvolvimento de tecnologias que permitissem ao usuário o controle sobre as informações recebidas, a lei americana acabou optando por conceder imunidade às empresas de Internet com relação a conteúdos de terceiros. Ver https://www.law.cornell.edu/uscode/text/47/230*

* **Bruna Martins dos Santos** é coordenadora de incidência na Associação de Pesquisa Data Privacy Brasil e Consultora em temas de Direitos Humanos na Era Digital. Este trabalho contou com o apoio de Diego Rafael Canabarro, gerente sênior de políticas públicas para a América Latina e o Caribe na Internet Society, e de Paula Corte Real, mestranda em "Media and Communications Governance" na London School of Economics and Political Science. Os pontos de vista expressos neste trabalho são de responsabilidade da autora e não refletem, necessariamente, a política ou posição oficial da Internet Society a respeito do tema.

O Escopo Da Lei Brasileira

O modelo brasileiro de responsabilidade dos intermediários de Internet foi construído com base em três pontos principais:

- a diferenciação entre serviços de provimento de acesso à Internet e aplicações de Internet;

- a necessidade de salvaguardar as atividades relativas ao provimento de conexão e dissociá-las de práticas de usuários que porventura causem danos a terceiros; e

- evitar a responsabilização imediata e direta de provedores de aplicações de Internet por conteúdos de seus usuários.

Nesse sentido, a lei brasileira trata de dois atores:

- provedores de conexão à Internet;
- provedores de aplicações de Internet.

Para começar a compreender as nuances entre a atuação dos dois, vale prestar atenção nas definições presentes no artigo 5º do Marco Civil da Internet:

***V** - conexão à Internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP;*

[...]

***VII** - aplicações de Internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet;*

O Marco Civil, portanto, traçou uma divisão clara entre a camada de infraestrutura de acesso (concentrada nos provedores de conexão à Internet) e a camada de aplicações, serviços e conteúdos (relativa aos provedores de aplicações de Internet). De uma maneira geral, pode-se dizer que o texto optou por uma abordagem tecnologicamente neutra, ao passo que escolheu não definir tipos específicos de provedores para além da dualidade entre "conexão à Internet x aplicações".

As categorias de provedores colocadas na lei ficaram restritas à dualidade entre camada de infraestrutura e de aplicações. Sobre os provedores em si, são dois os tipos de isenções de responsabilidade civil e os seus motivos:

- isenção de responsabilidade absoluta: garantida aos provedores de acesso/conexão à Internet com o objetivo de preservar o princípio geral de inimputabilidade da rede[6] e preservar os serviços que garantem acesso;

- isenção de responsabilidade parcial: garantida aos provedores de aplicações de Internet que, de acordo com modelo brasileiro, só devem ser responsabilizados ante a denotada inércia de conteúdo judicialmente reconhecido como nocivo e objeto de ordem judicial.

Importante mencionar que a diferenciação feita no texto da lei não esgota os diferentes tipos de provedores existentes e, inclusive, debatidos no próprio ordenamento jurídico brasileiro. Conforme destacado em acórdão do Superior Tribunal de Justiça, "na Internet, há uma multiplicidade de atores oferecendo diferentes tipos de serviços e utilidades para os usuários".[7] Essa decisão também destaca que, eventualmente, determinados tipos de provedores podem oferecer mais de uma modalidade de serviço de Internet e que as diferenciações

6. Princípio da Inimputabilidade da Rede: "O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos". Princípio nº 7, Princípios para a Governança e Uso da Internet, CGI.br, 05-07-2009. Ver *https://principios.cgi.br*

7. AgInt no RECURSO ESPECIAL Nº 1.593.873 - SP (2016/0079618-1). Ver *https://www.Internetlab.org.br/wp-content/uploads/2017/02/STJ-REsp-1.593.873.pdf*. Nesse sentido, acórdão proferido pela ministra Nancy Andrighi já destacava o seguinte trecho de decisão do REsp 1.316.921/RJ (REsp 1.316.921/RJ (Terceira Turma, julgado em 26/06/2012, DJe 29/06/2012): (i) provedores de backbone (espinha dorsal), que detêm estrutura de rede capaz de processar grandes volumes de informação. São os responsáveis pela conectividade da Internet, oferecendo sua infraestrutura a terceiros, que repassam aos usuários finais acesso à rede; (ii) provedores de acesso, que adquirem a infraestrutura dos provedores backbone e revendem aos usuários finais, possibilitando a estes conexão com a Internet; (iii) provedores de hospedagem, que armazenam dados de terceiros, conferindo-lhes acesso remoto; (iv) provedores de informação, que produzem as informações divulgadas na Internet; e (v) provedores de conteúdo, que disponibilizam na rede os dados criados ou desenvolvidos pelos provedores de informação ou pelos próprios usuários da Web.

entre eles são relevantes para o debate sobre responsabilidade. No entanto, o texto do Marco Civil da Internet optou por ser menos específico na descrição das atividades e acabou indicando apenas as duas categorias mencionadas anteriormente.

Sobre essa diferenciação vale mencionar que, em seu artigo 18, a lei optou por resguardar os provedores de conexão à Internet de eventual responsabilização civil por danos gerados por conteúdos de terceiros. Dessa maneira, o texto da lei consagrou a ideia de que os provedores de conexão devem ser completamente isentados de responder por atos praticados por terceiros aos quais concedeu acesso à Internet, uma vez que a conduta passível de causar eventual dano consiste em comentários, textos e conteúdos veiculados por terceiros, e não as atividades de "habilitação de um terminal para envio e recebimento de pacotes de dados pela Internet, mediante a atribuição ou autenticação de um endereço IP" (a definição de conexão à Internet adotada pelo Marco Civil).

Ainda sobre a diferenciação entre conexão e aplicações, é importante mencionar que o artigo 19 do Marco Civil da Internet é o responsável por estabelecer um modelo de responsabilidade para os provedores de aplicações. No texto, essa responsabilidade é residual e restrita, ou seja, somente deve ser direcionada a esses atores em caso de descumprimento de ordem judicial específica que tenha solicitado eventual bloqueio de conteúdos.

Os efeitos práticos da introdução do Marco Civil da Internet na ordem jurídica brasileira

A introdução do Marco Civil da Internet no ordenamento jurídico brasileiro trouxe novas interpretações sobre eventuais limitações às atividades dos provedores de aplicações de Internet. Além de deixar clara a ausência de relação entre o dano causado por conteúdos de terceiros e o provimento de conexão à Internet, a lei também resguardou os usuários e provedores de aplicações de Internet ao estabelecer que:

- a decisão sobre um conteúdo ser ilegal ou não tem que passar por uma terceira parte capacitada para deliberar sobre o tema (o Judiciário, no caso concreto); e

- aos provedores de aplicações só cabe a responsabilização subsidiária e na excepcionalidade do descumprimento de ordem judicial que demande a supressão de determinado conteúdo.

Nesse sentido, o modelo de responsabilidade civil sedimentado no Marco Civil da Internet tem como um de seus objetivos principais a garantia da liberdade de expressão, impedindo a censura prévia praticada por provedores de aplicações. Assim, o provedor de aplicações de Internet somente será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica que ordene a remoção de determinado conteúdo, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço, tornar indisponível o conteúdo apontado como ilegal.

Dessa maneira, o artigo 19 deixa claro que o Judiciário é a instância legítima para decidir contenciosos a respeito da legalidade ou não da oferta de determinado conteúdo, bem como a existência ou não de danos a serem indenizados por seu responsável (desonerando o provedor de aplicações de tais tarefas). Um bom exemplo dessa nova cultura são os dados extraídos a partir do relatório do blog Dissenso.org,[8] que contava com 152 decisões catalogadas até agosto de 2018, evidenciando que apenas 33,5% dos casos envolvendo pedidos de remoção de conteúdo na Internet foram reconhecidos ou confirmados em segunda instância, com mais de 60% dos casos de remoção tendo sido considerados ilegítimos, infundados ou abusivos.

A ausência de dispositivos específicos a respeito do desenvolvimento de regras de moderação de conteúdos pelos provedores de aplicações de Internet infere, também, que a remoção de conteúdo não está restrita à existência de ordem judicial, podendo o provedor retirar conteúdos que violem suas políticas e termos de uso deliberadamente.[9]

8. Dissenso. Casoteca: Conheça casos envolvendo liberdade de expressão no ambiente digital. Ver *http://dissenso.org/casoteca*
9. Chiara Spadaccini de Teffé, Maria Celina Bodin de Moraes. "Redes sociais virtuais: privacidade e responsabilidade civil Análise a partir do Marco Civil da Internet". Pensar, Fortaleza, v. 22, n. 1, p. 108-146, jan.-abr. 2017.

A introdução das notificações judiciais como esfera ensejadora de obrigação efetiva de remoção de conteúdo acabou deixando para trás a prática de notificações extrajudiciais e o uso do modelo de *notice-and-takedown.*[10]

Antes do Marco Civil da Internet a ausência de um regime de responsabilidade de intermediários específico para provedores de aplicações de Internet abriu espaço para que os tribunais brasileiros proferissem decisões divergentes sobre o mesmo tema, que iam desde a responsabilização de provedores em função da exibição de determinados conteúdos até a solicitação de cumprimento de notificação extrajudicial privada. Essa incerteza sobre o regime de responsabilidade era prejudicial para o desenvolvimento da Internet no país, já que qualquer um poderia ser responsabilizado pelo comportamento e por conteúdos gerados por terceiros (o que gera enorme insegurança jurídica e desincentiva o investimento no setor).

Com isso, ao instituir o modelo de responsabilização subsidiária para os provedores de aplicações de Internet, o texto do MCI também reconhece que, nas hipóteses de conteúdos ilegais, não cabe ao provedor de aplicações decidir sobre a retirada ou não, tampouco sobre os danos por eles causados.[11] A participação do Judiciário neste processo permite que a análise dos conteúdos seja feita de maneira menos discricionária – evitando o prosseguimento de pedidos de remoção infundados de conteúdos legítimos – e confere mais segurança jurídica para a atuação dos provedores de aplicações de Internet.

A importância do modelo de responsabilidade subsidiária instituído para os provedores de aplicações de Internet com a sanção do MCI e seu artigo 19 pode representar a existência de mais segurança jurídica para aquelas empresas cujas atividades envolvem ofertar *funcionalidades que podem ser acessadas por meio de um terminal conectado à Internet*, mas que não necessariamente envolvem atividades relacionadas com a divulgação de conteúdos de terceiros (algo que se explora nas seções III e IV abaixo).

De uma maneira geral, para além das regras de responsabilidade civil, é possível dizer que o Marco Civil também reconhece como legítimos os termos de uso e as políticas dos provedores de aplicações (quaisquer que sejam elas) como regras aplicáveis para a ponderação a respeito da licitude ou não de determinada ação ou postagem por parte de um usuário, com a ressalva de que tanto os termos de uso quanto a ação do provedor com base nestes seguem sujeitas ao escrutínio judicial.

Outra questão relevante é que ao interferir de forma limitada nas atividades de moderação de conteúdos que alguns provedores de aplicações de Internet realizam e dar espaço à responsabilização somente após a verificação do não cumprimento de ordem judicial determinando a supressão, a lei coloca em pé de igualdade grandes e pequenos provedores de aplicações (uma vez que é sempre mais fácil aos grandes desempenharem atividades de monitoramento e ação prévia, bem como atender a uma quantidade considerável de notificações extrajudiciais). É importantíssimo reconhecer o papel do MCI para garantir que as barreiras de entrada para pequenos provedores, com capacidades e recursos limitados para moderar conteúdo de terceiros, não sejam obstáculos ao desenvolvimento da economia digital no país.

Semelhanças e diferenças entre o regime de responsabilidade civil do Marco Civil e a Seção 230 do CDA

A Seção 230 do *Communications Decency Act* (CDA)[12] é construída de forma a evitar a influência na atividade das empresas provedoras de serviços e afasta destas a responsabilidade pelo conteúdo criado pelo usuário.[13] Adicionalmente, os curtos dispositivos da lei americana permitiram o desenvolvimento de regras próprias de moderação de conteúdo pelas plataformas sem nenhum tipo de intervenção ou penalidade do governo.

10. Ver *https://en.wikipedia.org/wiki/Notice_and_take_down*
11. Carlos Affonso Pereira de Souza. "Responsabilidade civil dos provedores de acesso e de aplicações de Internet: evolução jurisprudencial e os impactos da Lei 12.695/2014 (Marco Civil da Internet)". In: G. S. Leite, R. Lemos (Coord). Marco Civil da Internet. São Paulo: Atlas, 2014. p. 791-816.
12. *https://en.wikipedia.org/wiki/Communications_Decency_Act*
13. Jess Miers. A primer on Section 230 and Trump's executive order. Brookings. Ver *https://www.brookings.edu/blog/techtank/2020/06/08/a-primer-on-section-230-and-trumps-executive-order*

Outro conceito relevante para compreender as diferenças entre as leis dos EUA e do Brasil é a noção de *good Samaritan* que protege os provedores de aplicações de qualquer responsabilização – seja ela intervenção ou penalidade do governo – relativa a atividades de moderação de conteúdos que sejam obscenos, violentos ou até abjetos, uma vez vislumbrada a boa-fé no julgamento subjetivo empreendido pelo provedor.

Apesar de isentar os provedores de aplicações de Internet em um primeiro momento, o Marco Civil trata de responsabilidade civil subsidiária por conteúdos de terceiros e não deve ser confundido com a cláusula do bom samaritano. Aqui, a "proteção" estendida pelo artigo 19 do Marco Civil aos provedores de aplicações de Internet não diz respeito a eventuais medidas de moderação de conteúdos adotadas de maneira proativa por estes agentes ou aquelas baseadas em seus termos de uso.[14]

Ao contrário da lei americana, que resguarda o direito de moderação, a lei brasileira nada diz sobre as remoções de conteúdos baseadas em termos de uso e políticas dos serviços. Nesse sentido, a isenção de responsabilidade do Marco Civil restringe-se à "responsabilização por atos de terceiro". Os "atos próprios do provedor" (como, por exemplo, a decisão individual e autônoma – mesmo que baseada em termos de uso – de supressão de determinado conteúdo online) seguem sujeitos ao regime geral de responsabilidade previsto no Código Civil, segundo o qual: "aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito" (art. 186); e "também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes" (art. 187). São isentos de responsabilidades, nesses casos, os "atos praticados em legítima defesa ou no exercício regular de um direito reconhecido" ou sempre que se imponha "a deterioração ou destruição da coisa alheia, ou a lesão a pessoa, a fim de remover perigo iminente".

Ainda sobre o ponto das eventuais remoções de conteúdos, é importante ressaltar que a exigência de uma ordem judicial não é hipótese exclusiva para a remoção de conteúdos. O texto do artigo 19 dispõe sobre um modelo de responsabilidade civil com base em conteúdos de terceiros que possam eventualmente ser identificados como ilícitos por um juiz de direito.

Ao desenvolver os chamados "safe harbors" capazes de resguardar a atuação das empresas no cenário americano e permitir a existência de notificações extrajudiciais de remoção de conteúdos relativos a direito do autor, a Seção 230 também determina que os provedores de aplicações não devem ser tratados como responsáveis editoriais pelos conteúdos dos seus usuários. Em uma breve comparação com o Marco Civil da Internet, no Brasil, os únicos provedores que recebem tratamento semelhante ao conferido pela Seção 230 aos provedores de serviços interativos de computador são os provedores de conexão. Nesse sentido, apesar de resguardar em alguma medida os provedores de aplicações de Internet, o MCI promoveu apenas isenções parciais de responsabilidade.

Por fim, no que se refere às exceções do modelo de responsabilidade do MCI, o texto da lei tratou de duas:

- conteúdo referente a direitos autorais (art. 19, parágrafo 2º); e
- divulgação não consensual de imagens íntimas (art. 21).

Sobre o primeiro, o texto tenta preservar o disposto na Lei de Direitos Autorais (Lei nº 9.610/98) – assim como o CDA – , mas ainda condiciona a responsabilização dos intermediários ao cumprimento de ordem judicial disposto no caput do artigo 20, segundo o qual "sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de Internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em

14. Carlos Affonso Pereira de Souza, Chiara Spadaccini de Teffé. "Responsabilidade dos provedores por conteúdos de terceiros na internet". Consultor Jurídico. Disponível em: *https://www.conjur.com.br/2017-jan-23/responsabilidade-provedor-conteudo-terceiro-Internet*

juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário". Isso significa que, sempre que bloquear determinado conteúdo de um de seus usuários em virtude de uma questão de direito autoral, o provedor de aplicações no Brasil deverá notificá-lo do ocorrido para que, se quiser, recorra ao Poder Judiciário para fazer valer eventual direito que lhe socorra. A disseminação não consensual de imagens íntimas, disposta no art. 21, é o único caso de onde o provedor pode ser responsabilizado pelo não cumprimento de notificação extrajudicial, do/a envolvido/a ou de seu representante legal.

Críticas ao regime de responsabilidade civil constante do Marco Civil da Internet

Apesar dos aspectos positivos no ecossistema digital brasileiro apontados anteriormente, o regime do Marco Civil tem atraído críticas por quem se esforça para fazer prevalecer dois aspectos:

- uma lógica de responsabilização objetiva (direta) dos provedores de aplicações pelas ações de seus usuários, empregando uma lógica própria do direito do consumidor; ou

- uma lógica de responsabilização subjetiva e solidária, sublinhando a importância da notificação extrajudicial como forma de dar dinamismo aos pleitos de remoção de conteúdo online.

Nesse sentido, a constitucionalidade do artigo 19 será analisada pelo Supremo Tribunal Federal, no âmbito do Recurso Especial nº 1037396, cujo relator é o Ministro Dias Toffoli. Caso o STF julgue que o dispositivo é inconstitucional e deve ser extirpado do ordenamento jurídico, o ecossistema digital em uma perspectiva ampla (que não se restringe às aplicações que oferecem espaço para o exercício da liberdade de expressão de seus usuários) poderá ser forçado a se conformar a um dever de fiscalização das atividades de terceiros desenvolvidas em seus ambientes (incluindo o que ocorre em marketplaces,[15] plataformas, portais de conteúdo, podcasts etc).[16]

A abordagem de responsabilização da camada de aplicações de Internet foi fundamental para permitir o desenvolvimento de serviços e produtos e, ao mesmo tempo, não exercer uma influência em seus modelos de negócios. No entanto, o texto da lei brasileira optou por não definir os tipos de serviços e empresas que se enquadram na categoria para evitar promover entendimentos superados e não ficar sujeito à obsolescência característica da constante inovação e evolução dos serviços de Internet. Apesar do MCI ter suprido uma lacuna legislativa no ecossistema digital brasileiro e ter alçado efeitos práticos e ganhos indiscutíveis para a proteção dos direitos e liberdades fundamentais do usuário, a dualidade entre "provedores de conexão" e "provedores de aplicações" não é livre de problemas. Enquanto o conceito de provedor de conexão encontra-se pacificado doutrinariamente, o conceito de provedor de aplicações de Internet ainda merece amadurecimento, principalmente em relação a sua enorme abrangência.

Adicionalmente, a conjuntura sob a qual o Marco Civil foi desenvolvido acabou levando o debate para o campo das redes sociais. Nos anos que antecederam a aprovação e discussão da Lei 12.965/2014, alguns casos de judicialização de conteúdo postado em plataformas de rede social como o Youtube ficaram famosos por terem resultado em bloqueio requisitado pelas vias judiciais ante a impossibilidade da plataforma em manter inacessível o conteúdo objeto de ação judicial.[17]

Por fim, presumindo os benefícios para o fomento da inovação e do ambiente digital no Brasil apresentados com a sanção do Marco Civil da Internet, o artigo 19 e seu modelo de responsabilidade ainda precisam ser testados para além da Web e das redes sociais a fim de avaliar de que forma a norma se relaciona com as mais diversas atividades existentes em um ecossistema tão complexo como o existente na camada de aplicações, serviços e conteúdo da Internet: marketplaces, computação em nuvem, redes de entrega de conteúdos (CDNs), entre outros. Para além do caráter

15. Um marketplace é um centro de e-serviços funcionando como um "shopping center" virtual, que reune várias lojas e serviços comerciais.
16. Cristina de Lucca. "Google e Twitter pedem que julgamento sobre Marco Civil no STF seja adiado". Blog Porta 23, UOL. Ver *https://porta23.blogosfera.uol.com.br/2019/11/24/google-e-twitter-pedem-que-julgamento-sobre-o-marco-civil-seja-adiado*
17. Fabiano Cândido. "Justiça dá razão ao YouTube no caso Cicarelli". Revista Exame. Ver *https://exame.com/tecnologia/justica-da-razao-ao-youtube-no-caso-cicarelli*

principiológico por trás do artigo 19, sua importância prática transcende serviços e plataformas geralmente associadas à produção de conteúdos de terceiros, e é requisito para garantir também a livre concorrência e iniciativa, bem como a inovação e o desenvolvimento tecnológico em outras esferas do ecossistema digital brasileiro, sobretudo naquelas mais próximas do provimento de infraestrutura a partir da qual se desenvolvem atividades e serviços online em geral.

Para além da Seção 230 e do regime do Marco Civil da Internet: o papel da isenção de responsabilidade dos intermediários como princípio norteador para o desenvolvimento da Internet

Historicamente, o desenvolvimento de regimes relacionados aos limites e aos casos de responsabilização dos intermediários da Internet esteve umbilicalmente ligado ao tema da liberdade de expressão online, uma vez que muitos dos provedores de aplicações de Internet trabalham com atividades relativas à publicação de conteúdo gerado por terceiros.

Ao longo do desenvolvimento da Internet, diferentes modelos de responsabilidade de intermediários foram apresentados a fim de oferecer proteções aos usuários ante a disseminação de conteúdos abusivos ou garantia de direitos, bem como resguardar o ecossistema digital, a livre iniciativa e desenvolvimento dos atores nele envolvidos. Em 2018, o atual Relator Especial da ONU para Liberdade Expressão, David Kaye, em relatório para o Conselho de Direitos Humanos,[18] destacou que a pressão da responsabilização dos intermediários da Internet costuma resultar em um aumento dos casos de remoção de conteúdos lícitos, o que interfere diretamente no grau de tutela conferido à liberdade de expressão no ambiente digital.

O uso de notificações extrajudiciais, comumente utilizadas nos EUA ("Strategic Lawsuit Against Public Participation" ou "SLAPP"),[19] tem o condão de intimidar aqueles que têm o poder de impedir que determinados conteúdos circulem. Estes modelos extremos (baseados em notificação privada ou em responsabilização direta por conteúdos de terceiros) têm demonstrado que os intermediários muitas vezes pecam por excesso de zelo e removem ou bloqueiam conteúdo perfeitamente legítimo, sem submeter sua decisão ao crivo de um tribunal ou órgão independente capaz de aferir a legalidade ou não do conteúdo. Isto gera críticas em termos de transparência e responsabilização, bem como de falhas no devido processo legal e no direito à contestação à remoção nos modelos de "safe harbor".

No caso brasileiro, cientes dessa questão, diversos grupos de interesse passaram a defender um modelo diferente, baseando-se em argumentos ligados a direitos como liberdade de expressão e acesso à informação, segurança jurídica para a inovação e o desenvolvimento tecnológico, de forma que os intermediários não sejam responsabilizados por atos de seus usuários até que haja uma decisão judicial capaz de aferir se a pretensão de remoção de um conteúdo por parte de uma pessoa (física ou jurídica) deve prosperar ou não. Aqui procura-se assegurar que políticas e termos de uso que aplicam-se à Internet comportem, por princípio, a divulgação ampla e plural de conteúdos.

Com o regime atual do MCI, assegura-se a continuidade dos conteúdos online até que haja decisão judicial declarando-os ilícitos. A partir desse ponto, se os provedores de aplicações que restarem inertes em relação à supressão do conteúdo passam a ser considerados responsáveis pela manutenção do mesmo, eventuais danos gerados por esse conteúdo poderão ser-lhes imputados diretamente. Essa sistemática ataca os estímulos econômicos que existem para a remoção de conteúdos de maneira preventiva de forma a afastar riscos operacionais desnecessários.

Apesar de excluir o conteúdo relacionado ao direito autoral (Art. 19, §2º)[20] do seu escopo, de

18. Human Rights Council. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/HRC/38/35. Ver *https://freedex.org/wp-content/blogs.dir/2015/files/2018/05/G1809672.pdf*
19. Public Participation Project. What is a SLAPP? *Ver https://anti-slapp.org/what-is-a-slapp*
20. Art. 19, § 2º: "A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5º da Constituição Federal".

estabelecer regras diversas para casos que digam respeito à divulgação não consensual de imagens íntimas (Art. 21),[21] e de ser bastante parecido com a Seção 230 do CDA, o artigo 19 do Marco Civil vai além e se consolida como um exemplo internacional de como proteger a liberdade de expressão e o acesso à informação na rede de acordo com o próprio Frank La Rue,[22] ex-relator especial da ONU para o tema. Além disso, em pesquisas recentes o InternetLab concluiu que "o crivo judicial do Art. 19 é essencial para garantir que pedidos de remoção infundados não suprimam conteúdos legítimos"[23]e "o modelo regulatório em vigor no Brasil previne o uso de notificações extrajudiciais como forma de cerceamento à expressão".[24]

O tema da responsabilidade de intermediários, entretanto, transcende a importante questão da liberdade de expressão dos usuários de Internet. Ele é também importante como elemento impulsionador do próprio desenvolvimento da infraestrutura da Internet pelo planeta, porque "criou certeza e previsibilidade: as regras de responsabilidade do intermediário permitiram que os provedores de Internet (infraestrutura e conteúdo) elaborassem estratégias de conformidade com base em um conjunto limitado de leis e seus Termos de Serviço (ToS). Por causa da responsabilidade de intermediários, as empresas podem projetar negócios que atendam às suas necessidades. [...] E, também, porque colocou a responsabilidade pelo conteúdo onde ela pertence: ela afirmou que o cumprimento de diferentes tipos de leis que regulam o conteúdo pertence a quem produz o conteúdo e não àqueles que o hospedam".[25]

Nesses termos, segundo a Internet Society, a delimitação precisa dos casos e hipóteses de isenção de responsabilidade dos intermediários da Internet é essencial para que esta siga sendo uma rede aberta, de propósito geral e tecnologicamente neutra, capaz de sustentar uma gama sempre crescente de serviços e aplicações, que podem ser desenvolvidas sem a necessidade de se pedir autorização a nenhum ponto central de controle. Tais características, juntamente com algumas mais específicas, conformam o "modo Internet de interconectividade", que está por trás do êxito e do alcance que a rede tem hoje.[26]

Com a evolução da Internet, entretanto, "[a]s empresas de Internet são maiores, se dedicam a mais atividades e oferecem mais serviços. A própria Internet também mudou. Não é mais uma tecnologia separada por camadas discerníveis, mas uma teia de dependências com um número crescente de jogadores".[27] Com o passar do tempo, o aumento da pluralidade de serviços e aplicações existentes, bem como o aumento da convergência e interdependência entre provedores que operam nas distintas camadas que estruturam o ecossistema da Internet têm gerado tensões e questionamentos relativos ao futuro da questão da responsabilidade dos intermediários no Brasil e no mundo.

Parte disso decorre da natural dissociação entre a velocidade do desenvolvimento tecnológico e seu impacto na vida em sociedade, em contraposição à velocidade com que as instituições políticas e jurídicas são capazes de se adaptar a uma realidade social em permanente transição. Entretanto, não se pode confundir os princípios e os valores que orientam a isenção de responsabilidade de intermediários da Internet em determinadas situações com sua operacionalização em regras jurídicas específicas. Essas últimas tendem à obsolescência à medida que o tempo passa, enquanto que os princípios e valores inerentes à responsabilidade dos intermediários têm caráter mais permanente.

21. Art. 21: "O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo".
22. Frank La Rue. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, A/HRC/17/27. Ver *https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf*
23. Dissenso, *op.cit.*
24. Dennys Antonialli. "Indenizações por dano moral ameaçam liberdade para se fazer humor na internet". *Consultor Jurídico. Ver https://www.conjur.com.br/2016-ago-31/dennys-antonialli-dano-moral-ameaca-liberdade-humor-Internet*
25. Konstantinos Komaitis. Intermediary Liability: *The Hidden Gem*. Internet Society. Ver *https://www.internetsociety.org/blog/2020/03/intermediary-liability-the-hidden-gem*

Diante disso, a seção a seguir procura dar voz a atores envolvidos com o tema da responsabilidade de intermediários no Brasil com a finalidade de colher seu testemunho a respeito dos impactos (positivos e negativos) decorrentes do regime de responsabilidade civil decorrente do MCI e das lacunas atualmente existentes, de modo a saber, a partir da experiência presente, o que se pode projetar para o futuro. Apesar de estar centrado no Brasil, espera-se, ao fim, apontar os desafios e perspectivas não apenas para a letra da lei no país, mas, também, para a própria noção de responsabilidade de intermediários em uma perspectiva mais ampla.

II. A percepção de atores selecionados a respeito do regime de responsabilidade civil do Marco Civil

Conforme observado na sessão anterior, o modelo de responsabilidade de intermediários introduzido pelo MCI preocupou-se em exercer uma interferência mínima em modelos de negócios dos provedores de aplicações de Internet no Brasil ao determinar que a responsabilização civil somente poderá ocorrer após a infringência de ordem judicial solicitando a remoção do conteúdo. E, "como os provedores gozam de isenção de responsabilidade antes da ordem judicial, eles devem tomar o exercício da liberdade de expressão como vetor de suas atividades, sendo medidas de filtragem, bloqueios ou remoção uma solução excepcional".[28]

No entanto, a lei brasileira não coloca impedimentos para que provedores de aplicações de Internet removam conteúdos que violem suas políticas e termos de uso[29] a fim de resguardar seus produtos e serviços. Pode-se até dizer que, em um primeiro momento, a preocupação do Marco Civil da Internet não foi a moderação de conteúdos per se, mas sim aquela que era realizada com base em denúncias infundadas ou com pouca justificativa por parte dos provedores – e sem a devida apuração dos direitos envolvidos ou garantia de contraditório –, muito comum no momento anterior a aprovação da lei.

A fim de compreender os efeitos práticos deste modelo no provimento de serviços e de acesso a conteúdos online, a seção seguinte tem por objetivo fornecer um olhar mais robusto e claro sobre os modelos de provedores de aplicações de Internet existentes no Brasil.

O modelo brasileiro de responsabilidade de intermediários do Marco Civil pela ótica de especialistas envolvidos com o tema

Além da pesquisa bibliográfica, o presente estudo realizou entrevistas, entre os meses de maio e agosto, com quatro especialistas em temas relacionados com "Internet e Sociedade", "Internet e Políticas Públicas", e "Direito da Internet", e que historicamente tiveram envolvimento com o processo de elaboração do Marco Civil da Internet. O propósito das entrevistas foi coletar percepções a respeito do modelo de responsabilidade de intermediários brasileiro, possíveis limitações impostas pelas duas

26. A Internet Society identificou as propriedades críticas que definem o "Modo Internet de Interconectividade" (IWN, "Internet Way of Networking") e que sustentam o crescimento e a escalabilidade da Internet. Os benefícios dessas propriedades possibilitaram o desenvolvimento econômico e tecnológico que a Internet trouxe ao redor do mundo. As cinco propriedades críticas do IWN são: (1) uma infraestrutura acessível com um protocolo comum, que é aberta e tem poucas barreiras de entrada; (2) uma arquitetura aberta de blocos estruturais interoperáveis e reutilizáveis, baseada em processos de desenvolvimento de padrões abertos adotados voluntariamente por uma comunidade de usuários; (3) gerenciamento descentralizado e um sistema de roteamento distribuiido único, que é escalável e ágil; (4) identificadores globais comuns que são inambíguos e universais; e (5) uma rede tecnologicamente neutra, de propósito geral, simples e adaptável. Ver *https://www.internetsociety.org/resources/doc/2020/internet-impact-assessment-toolkit/critical-properties-of-the-internet* (inglês) e *https://isoc.org.br/noticia/documentos-sobre-a-consulta-publica-policy-development-process-da-internet-society-sobre-internet-way-of-networking* (português). Para a organização, o tema da responsabilidade dos intermediários relaciona-se diretamente com as propriedades críticas descritas nas propriedades [2], [3] e [5] acima. Ver *https://www.internetsociety.org/resources/doc/2020/internet-way-of-networking-use-case-intermediary-liability*

27. Konstantinos Komaitis, *op.cit.*

28. Carlos Affonso Pereira de Souza, Chiara Spadaccini de Teffé, op.cit.

29. Carlos Affonso Pereira de Souza. *O futuro foi reprogramado: como a tecnologia está transformando as leis, a política e os relacionamentos*. Rio de Janeiro: Obliq Press, 2018.

categorias de provedores delimitadas no Marco Civil da Internet e em que medida o modelo fomenta a inovação e desenvolvimento da Internet no Brasil.

De uma maneira geral, os entrevistados reconheceram o valor do Marco Civil como uma solução de política pública que teve por objetivo equilibrar os direitos e responsabilidades de indivíduos, corporações e setor público. Sobre esse primeiro ponto, os entrevistados apontaram de maneira unânime que a lei foi um projeto ambicioso e à frente de seu tempo, que optou por dar voz aos diferentes atores da sociedade – visíveis e invisíveis. Aqui, o papel do poder executivo, ao oferecer uma resposta imediata para as demandas da sociedade foi a chave para que chegássemos a uma lei equilibrada e que inovou ao colocar temas como neutralidade da rede, privacidade e proteção de dados pessoais, e responsabilidade de intermediários no ordenamento jurídico brasileiro.

Ainda sobre esse primeiro ponto, a lei brasileira foi apontada como inovadora também por estabelecer um primeiro exemplo de regulação estatal dedicada à Internet com uma abordagem principiológica e baseada em direitos. E, nesse cenário, o Decálogo de Princípios para a Governança e Uso da Internet no Brasil,[30] de autoria do Comitê Gestor da Internet no Brasil (CGI.br), serviu como texto inicial para a construção do debate e legitimação da participação multissetorial como abordagem.

"Quando o Marco Civil começou a ser discutido, o nosso entendimento sobre Internet não era o mesmo de hoje. Inclusive, falar de infraestrutura de Internet com a facilidade com a qual a comunidade da Internet no Brasil fala hoje, não era comum. [...] pensar, em detalhes, como fazer regulação de temas como neutralidade da rede, privacidade e liberdade de expressão naquele momento foi inovador e trouxe segurança jurídica para os provedores conexão e de aplicações de Internet". – **(Entrevista #3, Setor Acadêmico, Mulher)**

"[...] o Marco Civil representou uma primeira fase que gerou a oportunidade de uma organização de interesses com relação à regulação da Internet de uma forma mais clara e isso foi uma novidade para vários agentes. [Para a academia] Podemos olhar para a lei como um momento de fala mais organizada da sociedade civil com entidades dispostas a encontrar consensos e aprender a navegar no ambiente do Congresso Nacional; [Para o setor privado] O Marco Civil representou também o desafio de ir além da caixinha dos grandes players internacionais e entender como o ecossistema de inovação brasileiro precisava ser acionado a fim de que essas empresas pudessem entender o que estava em jogo no debate da lei brasileira". – **(Entrevista #2, Setor Acadêmico/ Sociedade Civil, Homem)**

Sobre as políticas de moderação de conteúdos e liberdade de expressão, uma das entrevistadas também apontou a importância do artigo 21 da lei[31] em função da discussão de gênero apresentada pela ideia de "remoção imediata de material com nudez ou ato sexual, sem autorização de seus participantes". A única exceção à necessidade de apreciação por parte do Poder Judiciário sobre o conteúdo possui relevância ao passo que introduz uma abordagem mais protetiva a grupos como mulheres e pessoas não-binárias vítimas de violência online[32] e rejeita a ideia de que determinados tipos de conteúdos não devem ser moderados imediatamente.

Sobre a eventual potencialidade do modelo de responsabilidade de intermediários funcionar como catalisador da inovação no Brasil e na região, ao contrário do que ocorre atualmente com a Seção 230, um dos entrevistados apontou que o modelo local ainda não passou pelo teste de robustez e amplo debate. Assim, o regime brasileiro atingiu um modelo equilibrado, possível naquele momento, com uma equiparação de poderes conveniente para os atores e redação concisa o bastante para que

30. Comitê Gestor da Internet no Brasil, CGI.br, *op.cit.*

31. Art. 21, já citado. § único: "A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido".

32. Sobre a remoção de conteúdos correspondentes à divulgação não consentida de imagens íntimas, a discussão tem sido abordada por acadêmicos como Danielle Citron ante a necessidade de uma resposta legislativa capaz de proteger as vítimas dos abusos cometidos por parceiros ao não considerarem que o consentimento abarca não só o momento da foto mas também o seu compartilhamento. Ver *https://slate.com/technology/2014/10/revenge-porn-laws-sample-text-for-state-lawmakers.html*

não promovesse dúvidas ou insegurança jurídica e não caducasse em pouco tempo. Seria relevante, portanto, reconhecer e compreender o artigo 19 do Marco Civil como um texto legal que permite a inovação no país.

Diferentemente do debate norte-americano, as discussões que resultaram na aprovação do Marco Civil promoveram pouca convergência entre temas como desenvolvimento econômico ou inovação e liberdade de expressão. A Seção 230 promove um ambiente jurídico propício para a inovação baseada em entendimentos da Primeira Emenda à Constituição dos Estados Unidos; enquanto isso, o ordenamento jurídico brasileiro e da América Latina é menos categórico quanto à proteção e utilização, como princípios, do livre discurso e da não intervenção. No entanto, o Marco Civil da Internet representa uma tentativa relevante de preservação de modelos de negócio existentes, e autonomia privada para o desenvolvimento de suas capacidades de inovação.

"Quando se pensa no artigo 19 do Marco Civil, inevitavelmente pensamos nas grandes empresas americanas e, sobretudo, nas grandes redes sociais. Com isso, tiramos de esquadro uma série de empresas que dependem dessa isenção inicial de responsabilidade para que elas possam desenvolver seus modelos de negócio e inovar". – **(Entrevista #2, Setor Acadêmico/Sociedade Civil, Homem)**

Sobre a isenção imediata de responsabilidade promovida pelo artigo 19 do Marco Civil da Internet, além de salvaguardar a liberdade de expressão no país, a medida também se encarrega de permitir que provedores de aplicações de Internet, baseados na disseminação de conteúdos de autoria da sua comunidade que possuem juízo de valor sobre terceiros, existam e funcionem no ambiente digital.

"O ecossistema de inovação ampliado da Internet depende de algum grau de proteção que um artigo como o art. 19 do Marco Civil oferece. No entanto é importante discutir como podemos calibrar a proteção à inovação". – **(Entrevista #2, Setor Acadêmico/Sociedade Civil, Homem)**

É inegável, nesse sentido, a abordagem mais protetiva do MCI em torno de direitos e garantias para os usuários da Internet. No entanto, a previsão geral de promoção da "inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso"[33] também pode ser vista como uma tentativa de uma legislação equilibrada que também fixa obrigações para agentes econômicos – provedores de conexão e aplicações de Internet.

"A lei fala de incentivos para iniciativas públicas de fomento à cultura digital e de promoção da Internet como ferramenta social (art. 27), mas seria interessante também pensar na promoção de uma análise de impacto social e econômico do modelo de responsabilidade de intermediários. [...] abordar melhor as questões de direito público pode ser uma maneira de superar as batalhas antigas e trabalhar no fomento da indústria digital no país inovação". – **(Entrevista #1, Setor Público, Homem)**

Algo abordado pelos quatro especialistas foram os novos desafios colocados pelo cenário atual de provedores de aplicações de Internet e os pontos não abarcados pelo Marco Civil da Internet.

A lei, elaborada entre os anos 2007 a 2014, não se ocupa diretamente de alguns dos fenômenos em discussão na atualidade e seu impacto para a Internet – modelos de negócios e de precificação de produtos e serviços oferecidos pelos provedores de aplicações, financiamento de conteúdo publicitário e impulsionamento de conteúdos em redes sociais, estratégias de espalhamento de desinformação por meio de aplicações e serviços acessíveis por meio da Internet. Alguns dos especialistas entrevistados apontaram, inclusive, que há riscos inerentes à proteção ampliada conferida aos provedores de aplicações de Internet, o que resultaria na necessidade de atualização da lei de modo a preservar o verdadeiro espírito original buscado com o regime de responsabilidade de intermediários constante do Marco Civil:

33. Art. 4º, inciso III da Lei 12.965/2014.

"Essa liberdade de inovar pode ser um combustível para a criação de um mundo diametralmente oposto ao que construímos. Plataformas estão trabalhando até o momento que a lei chega, no entanto o momento da regulação sempre será tardio para conter os avanços e eventuais abusos cometidos pelos provedores de aplicações contra a privacidade". – **(Entrevista #3, Setor Acadêmico, Mulher)**

"A responsabilização deve acontecer em cima do mau uso dos elementos constituintes da Internet, mas eles devem estar disponíveis para atividades e empreendedorismo". – **(Entrevista #4, Executivo envolvido com IXPs e serviços DNS, Homem)**

Sobre as duas categorias abarcadas na lei – provedores de acesso e conexão ou provedores de aplicações de Internet – é importante pensar na definição de Internet para se compreender a relação entre as isenções de responsabilidade e desenvolvimento da inovação.

"A Internet é um conjunto de blocos constituintes que montam coisas. Uma defesa da Internet não representa a concordância com os maus usos [de alguns desses blocos constituintes]. O que é construído sobre a Internet não pode macular a Internet em si". – **(Entrevista #4, Executivo envolvido com IXPs e serviços DNS, Homem)**

A discussão de responsabilidade de intermediários evoluiu bastante entre os anos de 2010 e 2020. Se um modelo de ecossistema justo e equilibrado era um incentivo ou fomento para a economia digital há 10 anos, a lógica de publicação de terceiros em sites que permeia a Internet do passado evoluiu para plataformas conglobantes e serviços fechados, com um papel cada vez mais determinante na modulação e moderação de comportamentos dos usuários, onde a isenção de responsabilidade talvez precise ser rediscutida.

"O paradigma do MCI é a caixa de comentários do UOL, e saber se portais de comentários respondem ou não [pelos danos causados por comentários deixados pelos seus usuários]. A lógica se aplica a redes sociais sem muitas mudanças, mas a regra inicial não contemplava a abertura para interação sem a existência de isenção. [...] e talvez seja o caso de termos protegido o desenvolvimento das empresas dominantes no tema". – **(Entrevista #1, Setor Público, Homem)**

A constante evolução da Internet e dos serviços ofertados (seja na camada de infraestrutura, seja na camada de aplicações) chama os atores à inovação constante. A percepção dessa ferramenta como um ambiente de inovações técnicas e sociais permite concluir que a elaboração de políticas públicas e legislações devem sempre prezar pela não obsolescência e pela capacidade de moldar-se uma realidade social em constante mutação. Apesar de ainda existirem hoje alguns exemplos de provedores de aplicações de Internet que estavam no centro do debate de regulação da Internet à época da sanção do Marco Civil, as funcionalidades ou inovações desenvolvidas na camada de aplicações ao longo dos anos em relação a esses serviços (ou até mesmo ao surgimento de serviços inteiramente diferentes) fazem com que não seja tão simples enquadrar os intermediários como provedores de conexão e/ou provedores de aplicações no que diz respeito à sistemática de responsabilização dos intermediários pelos danos causados por conteúdos de terceiros. Para além de uma abordagem formal (baseada na letra fria da lei), é necessária uma avaliação funcional (focada nas funções desempenhadas por cada intermediário) para determinar se incide ou não o regime específico previsto no Marco Civil.

Obviamente, não é de se esperar que o Marco Civil aplique-se para além daquilo que está previsto em seu texto e nem se pode esperar que suas regras sejam capazes de abarcar todas as atividades exercidas por provedores de aplicações de Internet na atualidade. Entretanto, é preciso entender de que maneira a avaliação da responsabilidade dos intermediários (no que transcende o escopo normativo do Marco Civil) pode ser conciliada com a preservação do princípio geral de atribuir a responsabilidade por conteúdos e comportamentos na Internet aos verdadeiros responsáveis por eles.

Percepções adicionais a respeito do regime de responsabilidade civil do Marco Civil a partir da ótica de representantes do setor privado

O presente relatório buscou conversar, ainda, com atores do setor privado, representantes de alguns dos modelos de provedores de aplicações de Internet e de serviços na camada de infraestrutura que servem de suporte às aplicações de Internet, a fim de coletar percepções adicionais sobre o modelo de responsabilidade de intermediários e o valor da lei brasileira para seus modelos de negócio, conforme destacamos a seguir. Os indivíduos entrevistados atuam em empresas brasileiras e uma internacional, e foram selecionados por representarem serviços e produtos diretamente afetados pela aprovação do Marco Civil da Internet (ainda que não tenham sido diretamente visados no desenho da solução legislativa constante do artigo 19).

A importância do Marco Civil da Internet para as discussões sobre Internet no Brasil é inegável. E uma primeira diferenciação positiva da lei é a separação entre a infraestrutura da rede e os serviços e produtos oferecidos na Internet (camada de conteúdos).

"Em termos de inovações legislativas, os eixos principais são os artigos 9 (neutralidade da rede) e 19 (isenção de responsabilidade civil parcial para provedores de aplicações de Internet). A parte de consolidação de direitos aos usuários da Internet é de fato relevante (mas pode-se dizer que já encontra respaldo na Constituição, no Código de Defesa do Consumidor e até no Código Civil).No entanto, a separação entre as camadas de infraestrutura e de conteúdo, bem como a tentativa de proteger a neutralidade da rede são os fatores mais relevantes do Marco Civil da Internet. [...] A lei é relevante para uma separação eficaz entre as camadas, as responsabilidades e os ofertantes de serviços e produtos de modo a atribuir a cada um a devida responsabilidade[?]". – **(Entrevista #9, Setor Privado, Mulher)**

Acerca dos possíveis avanços alcançados com a lei, alguns atores apresentaram a lei como um esforço interessante para delimitar a função social dos atores – provedores de conexão, provedores de aplicações, governo e sociedade civil. No entanto, algumas das visões apresentadas argumentaram que a lei poderia ser mais equilibrada em relação às obrigações colocadas para os provedores de aplicações e de conexão, bem como para o poder público. Vide transcrições abaixo:

"O Marco Civil poderia focar mais no setor público, foi uma primeira tentativa brasileira de se regular a Internet no Brasil e ante as respostas necessárias ao escândalo de vigilância da época - Snowden. Um ponto de desequilíbrio da lei, portanto, é o foco exclusivo em empresas privadas e o fato dela não perceber o setor público como um ente que pode realizar atividades que se assemelham aos provedores de conteúdos de forma indistinta. Aqui, os atores devem poder ser responsabilizados por conteúdos abusivos, independentemente do meio onde o comentário foi postado". – **(Entrevista #5, Setor Privado, Homem)**

"O Marco Civil consolidou a garantia dos direitos dos usuários da Internet, o tema é um dos motivos de existência da lei. Sobre os entes privados, a lei não é equilibrada, os provedores de conexão têm mais responsabilidade do que os provedores de aplicações. E o Poder Público ficou com um rol de responsabilidades bastante etéreas e que poderiam ter sido mais fortes". – **(Entrevista #6, Setor Privado, Homem)**

"O Marco Civil da Internet representa uma solução mediana de equilíbrio entre direitos e responsabilidades de usuários individuais, corporações e setor público. No entanto, uma revisão das responsabilidades colocadas para os provedores de conexão e aplicações de Internet é necessária para aparar as ainda existentes arestas - exemplo: ausência de disposições sobre guarda de logs e provedores de trânsito". – **(Entrevista #8, Setor Privado, Homem)**

Sobre a isenção parcial de responsabilidade civil introduzida no artigo 19 da lei brasileira, alguns dos atores entrevistados apontaram a discussão como chave para o desenvolvimento de determinadas plataformas e serviços. Adicionalmente, a aplicação do

princípio da inimputabilidade da rede – e a sua inclusão no texto do Marco Civil – devem ser discutidos com parcimônia já que foram introduzidos para garantir o desenvolvimento da rede e não para oferecer imunidade a atividade dos provedores de aplicações.

"Questões como a imunidade de intermediários (no caso da seção 230) ou a isenção parcial de responsabilidade civil (no caso do MCI) são fatores críticos para a existência de plataformas coletivas de gestão de conteúdos como a Wikipedia. Em modelos de gestão coletiva e baseados em decisões da comunidade, especialmente, as isenções de responsabilidade são pontos chave para garantir a produção e disseminação de conteúdos de terceiros, bem como a sustentabilidade das plataformas". – **(Entrevista #7, Setor Privado, Homem)**

"Princípios como o da Inimputabilidade da Rede funcionam para manter um sistema em pé, ou seja, o fluxo de dados e informações (a rede) na camada física ou na lógica. Mas o princípio não deveria ser aplicado para resguardar os serviços em si e nem para isentar completamente os provedores de aplicações da responsabilidade por conteúdos. Em se falando de responsabilidade, é interessante pensar sobre a responsabilização de intermediários por impulsionamentos/conteúdos impulsionados - a prestação pecuniária recebida em troca do conteúdo poderia ser a hipótese que permite a responsabilização direta". – **(Entrevista #6, Setor Privado, Homem)**

Outro fator que merece atenção é a segurança jurídica conferida às atividades dos provedores de aplicações de Internet a partir da implementação de um modelo brasileiro de responsabilidade de intermediários na medida em que há maior previsibilidade da eventual responsabilização desse tipo de intermediário. Antes da lei, a ausência de um sistema de isenções ou qualquer dispositivo legal capaz de resguardar as atividades dos provedores de aplicações de Internet era um fator que gerava risco e incerteza para o setor.

"O custo operacional de se gerenciar operações de empresas e oferta de serviços em um cenário de dúvida que existia antes da sanção do Marco Civil era muito grande. Na época, assumir a curadoria de pedidos extrajudiciais de remoção de conteúdos ante a possibilidade de judicialização era um processo que gerava muitos riscos. A introdução do modelo de responsabilidade do Marco Civil, portanto, aumentou a segurança jurídica, o compromisso das empresas com o ordenamento jurídico brasileiro, com o investimento no país e abriu espaço para inovação". – **(Entrevista #9, Setor Privado, Mulher)**

Apesar de representar um retrato da Internet brasileira até 2014, um modelo de responsabilidade de intermediários capaz de conciliar e fomentar a entrada de novos provedores de aplicações de Internet no cenário brasileiro foi condição determinante para o desenvolvimento do ambiente de inovação no Brasil. E a isenção parcial de responsabilidade colocada pelo artigo 19 do Marco Civil foi fundamental para tal, conforme destacado abaixo:

"A tentativa de estabelecimento de um modelo de responsabilidade de intermediários do Marco Civil da Internet buscou exercer uma interferência mínima nas empresas. E as proteções estabelecidas pela isenção parcial de responsabilidade civil sobre os conteúdos é o que garante que empresas de menor porte possam ser atuantes no mercado brasileiro. A importância do modelo também está localizada na intenção de conciliar a necessidade de criação de um ambiente saudável de competição e não prejudicar os novos entrantes - empresas menores e startups. Nesse sentido, a responsabilização imediata de provedores de aplicações sobre conteúdos de terceiros é hipótese que teria resultado na adoção de medidas de mitigação dos danos de maneira imediata e regras de moderação mais restritivas - responsabilização do vetor de conteúdo x responsabilização do autor do conteúdo".

"[...] São fatores como o fomento à livre iniciativa e inovação presentes no Marco Civil - e a ideia de intervenção mínima nos produtos e serviços - que permitiram o surgimento de empresas que ocupam grande parcela do mercado brasileiro". – **(Entrevista #5, Setor Privado, Homem)**

"Em se falando do Brasil, o regime de responsabilidade de intermediários do MCI traz segurança jurídica para provedores de aplicações que trabalham diretamente com conteúdo. No entanto, para as demais aplicações de Internet que ofertam serviços que não sejam exclusivamente conteúdo ou informações (ex. Fintechs), o regime pode não ter garantido segurança jurídica o bastante a ponto de tangenciar o ambiente de inovação". – **(Entrevista #10, Setor Privado, Mulher)**

No entanto, na visão de um dos entrevistados, esse modelo precisaria de revisão a fim de permitir um ambiente ainda mais propício à inovação e, inclusive, abarcar pontos como tributação de serviços online.

"Sobre as possíveis proteções à inovação e desenvolvimento da indústria, o modelo de responsabilidade de intermediários age de maneira protetiva e pode, de maneira indireta, defender o poder econômico dos grandes provedores de aplicações. A lei protege os provedores, mas não foi capaz de criar um ambiente de incentivos à inovação ao passo que não trata de questões como diminuição de carga tributária. A lei brasileira precisa de uma revisão urgente, mas é uma lei importante. Quando pensamos em Internet e serviços de valor adicionado, o texto é relevante, no entanto ele ainda precisa ser contemporizado com questões como regulamentação de infraestrutura de telecom". – **(Entrevista #8, Setor Privado, Homem)**

De uma maneira geral, os representantes do setor privado entrevistados corroboraram com a percepção sobre as discussões de moderação de conteúdos online e uma maior incidência dos provedores de aplicações na regulação dos fluxos no âmbito de suas plataformas não terem sido centrais à época do debate do Marco Civil da Internet, apesar de relevantes. Alguns dos comentários destacaram as diferentes formas de moderação e políticas que podem ocorrer entre os diversos atores e produtos e a necessidade de se resguardar direitos fundamentais como liberdade de expressão nesse contexto, especialmente ante desafios novos como a disseminação de notícias falsas ou acirramento do debate político online.

"O debate sobre moderação de conteúdos é um dos pontos mais críticos sobre a discussão de Internet - fakenews, pirataria, direito autoral e disseminação de conteúdos atentatórios à vida são temas que permeiam práticas de moderação de conteúdos e alguns dos problemas que enfrentamos hoje em dia. No entanto, a Internet pode ser vista puramente como um espaço de fluxo de informações e, aqui, reduzir a circulação de conteúdos pode representar uma redução da Internet como ferramenta. Práticas de redução de circulação de conteúdos podem afetar todos os tipos - bons e ruins". – **(Entrevista #5, Setor Privado, Homem)**

"Pensar nos propósitos que orientam alguns tipos de serviços e produtos é importante para abordar a questão da moderação de conteúdos - e compreender que ela pode ocorrer de maneira mais simples. Em sites como Reddit, TripAdvisor ou em fóruns do Yelp, orientados por um tema, a moderação pode ficar restrita a temas que estão fora do escopo ou de conteúdos que caracterizam spam. E modelos de serviços 'community-based' podem apresentar uma atenção reforçada para questões como direitos autorais e outras questões legais, uma vez que a constante moderação coletiva promovida por seus usuários pode ajudar a trazer novos aspectos e interpretações sobre determinados conteúdos".

"A criação de leis para a Internet não pode ser orientada exclusivamente pelas atividades de empresas como Google ou Facebook e deve promover uma coordenação com os vários modelos de negócios existentes, para não correr o risco de eliminá-los". – **(Entrevista #7, Setor Privado, Homem)**

Ante as entrevistas descritas acima, pode-se dizer que há um determinado consenso sobre a lei brasileira representar uma solução equilibrada entre direitos dos usuários e obrigações para as empresas. No entanto, o foco quase exclusivo nas atividades de provedores de aplicações é voltado a oferecer espaço de publicação de conteúdos aos usuários, com pouca ou nenhuma incidência na regulação/moderação do comportamento individual e do discurso dos usuários. Nesse sentido, a evolução da camada de serviços e

aplicações da Internet (em direção a um horizonte onde cada vez mais os provedores intervêm no fluxo comunicacional de seus usuários) tem imposto novos desafios e aberto novos debates relacionados ao futuro do regime de responsabilidade civil do Marco Civil da Internet no Brasil.

Por um lado, as isenções parciais de responsabilidade apresentadas pelo Marco Civil aos provedores de aplicações de Internet foram inegavelmente responsáveis por resguardar a atividade desses atores ante o conteúdo abusivo postado por seus usuários e, ao mesmo tempo, oferecer incentivos para que esses atores se afastem de práticas de moderação e remoção de conteúdos mais discricionárias e próximas do *overblocking*.[34] Com isso, o Marco Civil contribuiu com a geração de um cenário de segurança jurídica e um ambiente de menos risco para os provedores de aplicações de Internet, permitindo o seu livre desenvolvimento.

A partir das duas seções precedentes, a seção a seguir procura apontar alguns dos desafios atuais e as perspectivas mapeadas ao longo da pesquisa para o futuro da responsabilidade civil dos intermediários de Internet no Brasil.

III. Desafios atuais ao modelo de responsabilidade de intermediários do MCI

A construção do Marco Civil da Internet levou em consideração pontos como o respeito à livre iniciativa, a livre concorrência e a defesa do consumidor, bem como a preservação da liberdade dos modelos de negócios promovidos na Internet (art. 3º), para criar um regime de isenção de responsabilidade civil parcial (para provedores de aplicações de Internet) capaz de permitir o desenvolvimento de um ecossistema complexo e robusto e, ao mesmo tempo, respeitar as peculiaridades dos diversos modelos.

Conforme destacado na fala de alguns dos entrevistados na seção anterior, a segurança jurídica fornecida pelo artigo 19 e pela lei serviram de base para que muitos provedores de aplicações desenvolvessem suas próprias políticas de moderação de conteúdo, adaptadas ao tipo de serviço e produto ofertados e respeitando as particularidades de seus usuários.

O cenário atual existente no Brasil sobre a regulação da Internet apresenta desafios ao modelo de responsabilidade de intermediários de Internet em temas originalmente não abordados no contexto de desenvolvimento e adoção da lei: moderação de conteúdos, disseminação de discurso de ódio, desinformação, financiamento de anúncios e impulsionamento de conteúdos ou tributação de serviços online e direito da concorrência. Apesar desses temas coincidirem com os desafios colocados para os provedores de aplicações de Internet atualmente, boa parte deles já está abarcada em outras porções do ordenamento jurídico brasileiro (e não necessariamente se confunde com o tema da responsabilidade dos provedores por atos de terceiros).

O principal desafio identificado: a moderação de conteúdo como "ato próprio" do provedor

A complexidade do ecossistema de provedores de aplicações de Internet no Brasil é uma questão relevante para que possamos entender a importância de um modelo de responsabilização de intermediários que resguarde a liberdade de expressão dos usuários da Internet e exerça influências mínimas nas políticas internas dos provedores de aplicações. Conforme explicitado anteriormente, a lei brasileira optou por um modelo de governança dedicado especificamente aos provedores de aplicações de Internet e que, ao mesmo tempo, reservou a possibilidade de responsabilização desses atores ante a desobediência de ordem judicial e fomentou o desenvolvimento desses atores e de regras específicas de moderação de conteúdos.

Para o Marco Civil, a preocupação principal do esforço legislativo foi a de conter as remoções discricionárias de conteúdos produzidos por terceiros e, também, de garantir o livre fluxo de informações e bens na camada de serviços e

34. Clara Iglesias Keller. "Policy by judicialisation: the institutional framework for intermediary liability in Brazil". International Review of Law, Computers & Technology. DOI: 10.1080/13600869.2020.1792035. 2020.

aplicações. Nesse contexto, a lei brasileira pode ser vista como uma primeira tentativa de regulação de fluxos de informações por meio da preservação do caráter colaborativo e coletivo da Internet. No entanto, ao contrário do paradigma americano, o Brasil optou por uma solução equilibrada que permita, ao mesmo tempo, um nível menor de interferência do Estado e a responsabilização por atos de terceiros ante a inércia após edição de ordem judicial que demandar a retirada.

Se, em um primeiro momento, as leis sobre a Internet se dedicaram a estabelecer um ambiente mínimo para o crescimento do mercado digital, passados mais de 30 anos desde a criação da Web, provedores de aplicações passaram a internalizar sistemas e políticas de gestão dos conteúdos a fim de garantir a continuidade dos seus serviços e segurança dos usuários.

Apesar do Marco Civil não falar exclusivamente sobre regras de moderação de conteúdos ou realizar qualquer fomento a este tipo de atividade em provedores de aplicações de Internet, alguns acabaram por adotar diferentes modelos de controle dos fluxos de informações de acordo com a natureza de seus serviços. Nesse sentido, conforme destacado em uma das entrevistas transcritas acima, vale lembrar que o enfoque pensado para o Marco Civil tinha mais a ver com o tema da moderação de conteúdos de terceiros em aplicações, e um pouco menos incidentes na moderação de conteúdos e modulação de condutas (a caixa de comentários no site de notícias ou o provedor de espaços para publicação de blogs).

Plataformas como marketplaces e sites de comércio eletrônico podem possuir interesses diferentes daqueles tradicionalmente associados aos provedores de redes sociais na adoção e implementação de políticas de moderação de conteúdos. Aqui, as políticas têm menos incidência no discurso e ficam mais restritas à experiência do cliente. Portanto, para resguardar e proteger os seus consumidores (de fraudes, da comercialização de produtos falsificados, da circulação de produtos que atentem à saúde pública etc), esses provedores podem agir para conter a comercialização de itens cuja venda é reconhecidamente ilegal/ilícita. Outros meios de controle da comercialização dos anúncios/produtos ofertados por essas plataformas podem ser também o respaldo nas leis vigentes e controles impostos a determinados produtos e serviços *(law enforcement)*.

Em se falando de plataformas de comércio eletrônico ou marketplaces, um ponto chave das práticas de "moderação" gira em torno da proteção à propriedade intelectual – direitos de marca, autoria, modelos e projetos industriais, patentes e modelos de utilidade. Nesse sentido, vale destacar políticas como o *Brand ProtectionProgram (BPP)*[35] adotada pelo Mercado Livre, que permite que uma comunidade de titulares de direitos possa denunciar (com alcance transfronteiriço) anúncios de vendedores que supostamente estejam infringindo seus direitos – em todos os países que trabalham com a plataforma. No caso do BPP, uma simples denúncia por violação de propriedade intelectual resulta em uma pausa na veiculação do anúncio para análise por titular e anunciante e, caso não haja resposta, o conteúdo pode ser excluído.[36] Ainda sobre marketplaces, vale destacar que o ordenamento jurídico brasileiro vem interpretando o artigo 19 do Marco Civil da Internet de forma a eximir essas plataformas de responsabilidade por transações realizadas no âmbito das mesmas,[37] reconhecendo o direito dessas plataformas de adotar políticas de moderação de conteúdos.

Em casos como serviços de streaming ou portais de notícias, a moderação/controle de conteúdos segue também a linha de valorização da experiência do usuário (para além do papel tradicional de

35. Mercado Livre. Brand Protection Program. Ver *https://www.mercadolivre.com.br/brandprotection/enforcement*
36. Mercado Livre. Brand Protection Program: o que é e como usar. Ver *https://vendedores.mercadolivre.com.br/brand-protection-program-o-que-e-e-como-usar*
37. "Comércio digital – Ação cominatória (abstenção de comercializar produto) – Improcedência – Inconformismo – Desacolhimento – Art. 132, III, da Lei 9.279/96 – Princípio do Exaurimento da Marca – Apelada que se destina a intermediar a venda e compra de produtos – Fiscalização prévia dos anúncios que não lhe é imposta – Inteligência do art. 19, do Marco Civil da Internet – Responsabilidade configurada apenas diante de eventual inércia, ausente in casu – Contrafação que foi retirada do ar tão logo apontada – Precedentes deste E. TJSP e do C. STJ – Improcedência acertada – Sentença mantida – Recurso desprovido." (TJSP, Apelação n. 1053947-08.2017.8.26.0114; Rel. Min. Grava Brazil; 2a Câmara Reservada de Direito Empresarial; DJe 17.7.2019)

controle editorial dos conteúdos aferecidos por meio da Internet). Esses serviços realizam uma curadoria de conteúdos – autorais e de terceiros – veiculados com base em padrões de produtos com os quais trabalham e têm princípios como liberdade de expressão e imprensa como norte, o que gera responsabilidade jornalística e editorial sobre os conteúdos produzidos (algo já contemplado pela legislação aplicável à categoria).

Outro caso interessante é o das plataformas de gestão coletiva de conteúdos. Plataformas como Reddit, Chans e Wikipedia são exemplos que possuem políticas de governança de conteúdos baseadas em suas comunidades e onde as regras são, em sua maioria, estabelecidas por voluntários e usuários da rede. Outra característica peculiar desse tipo de provedor de aplicações é que eles também se baseiam fortemente na confiança entre pares – voluntários e usuários – e numa presença quase mínima da pessoa jurídica do provedor de aplicações no desenvolvimento de políticas de uso da plataforma.

A Wikipedia, a enciclopédia virtual de acesso livre criada em 2001, é um dos formatos mais notáveis de plataformas colaborativas e com um modelo de moderação baseado na comunidade. A ferramenta, que é diferente de páginas de discussão de artigos ou páginas de discussão de usuários, tem por objetivo a disseminação de conteúdos criados e reeditados por voluntários da plataforma e se organiza em linhas de canais, ao invés de sucursais nos países. Não existe uma Wikipedia Brasil, mas sim um canal Wikipedia em português que atende a Comunidade de Países de Língua Portuguesa, por exemplo.

Outro ponto que vale destacar de plataformas como a Wikipedia e o *Reddit* é que a inclusão dos voluntários nos processos de decisão sobre conteúdos é algo que traz à tona a importância de inclusão de valores e contextos sociais nas discussões de moderação de conteúdos.[38] A introjeção de normas sociais pode ser uma experiência arriscada e que, no caso da Wikipedia, tem sido sustentável. Com aproximadamente 6,15 milhões de artigos e 40 milhões de usuários cadastrados na sua versão em inglês, a administração descentralizada da plataforma deu espaço a usuários mais preocupados com o tipo de conteúdo que circula nela. E um dos interesses principais da plataforma é proteger a independência dos seus voluntários.

Enquanto as regras de moderação de plataformas coletivas como a Wikipédia atingiram um desequilíbrio positivo onde os voluntários definem políticas e regras, os demais provedores de aplicações de Internet funcionam de maneira bastante diversa e possuem políticas determinadas de maneira unilateral (empresa-usuários).

Um caso recente de retirada de conteúdo praticado por parte das redes de distribuição de conteúdos, os CDNs, foi a "expulsão" do site antissemita e supremacista branco chamado *Daily Stormer* da Cloudflare. Em agosto de 2017, após muitas denúncias sobre o discurso de ódio propagado pelo portal, a Cloudflare terminou seu contrato com o *Daily Stormer* sugerindo que o site procurasse um outro espaço para hospedar seu conteúdo. O caso gerou muitas dúvidas em toda a comunidade de governança da Internet e muitos consideraram a medida como um precedente perigoso uma vez que os CDNs também são provedores de infraestrutura técnica e deveriam ter uma postura neutra com relação à conteúdos.[39] No entanto, ao olhar para as definições do Marco Civil, serviços como os CDNs são vistos como provedores de aplicações de Internet (nos mesmos termos dos serviços elencados acima) e estão sujeitos ao modelo de responsabilidade solidária instituído na lei.

O debate sobre a Cloudflare e o caso do Daily Stormer ilustram bem o momento atual da Internet. Ante o crescimento de conteúdos ofensivos que podem colocar em risco a vida e a integridade dos usuários da Internet, entramos em um momento de políticas de Internet onde esses atores são chamados a agir contra determinados tipos de informações e agentes. Em 2020, resumir a elaboração de políticas para a Internet à dualidade em torno das definições de "editors" x "publishers" e toda a noção de isenção de responsabilidades pode ser uma pedra no caminho

38. Justin Clark, Robert Faris, Urs Gasser, Adam Holland, Hilary Ross, Casey Tilton. *Content and Conduct: How English Wikipedia Moderates Harmful Speech.* Harvard University: Berkman Klein Center for Internet & Society. 2019. Ver *https://dash.harvard.edu/handle/1/41872342*
39. Catherine Wilson. "Toeing the Line Between Censorship and Content Moderation". *New America Foundation.* Ver *https://www.newamerica.org/weekly/toeing-line-between-censorship-and-content-moderation*

de medidas que busquem enfrentar os problemas gerados pela instrumentalização da Internet para a disseminação de discurso de ódio, por exemplo.

Outros desafios e perspectivas futuras

Os assuntos destacados abaixo são os principais eixos de discussão no debate sobre responsabilidade de intermediários e representam as principais arenas em que se discutirá o tema da responsabilidade de intermediários no Brasil.[40]

Constitucionalidade do Artigo 19 do Marco Civil – Discussão colocada perante o Supremo Tribunal Federal, na ocasião do RE 1.037.396/SP.[41] Caso a obrigação de "necessidade de prévia e específica ordem judicial de exclusão de conteúdo para responsabilização civil de provedor de Internet, websites e gestores de aplicativos de redes sociais por danos decorrentes de atos ilícitos praticados por terceiros"[42] seja declarada como inconstitucional pelo STF, podemos retomar o estado onde a simples possibilidade de responsabilização de provedores de aplicações de Internet resultará em práticas mais restritivas sobre os conteúdos e perfis aceitos – resultando em um chilling effect na liberdade de expressão.

Fake News – O Congresso Nacional Brasileiro tem questionado o papel dos provedores de aplicações de Internet e a sua contribuição para fenômenos como a disseminação de desinformação, discurso de ódio e afins. Apesar de o debate seguir concentrado nos provedores de aplicações que são redes sociais e aplicativos de mensageria, investigações como as realizadas pela Comissão Parlamentar Mista de Inquérito das Fake News[43] verificaram que esses provedores não estão sozinhos nos esquemas de disseminação de conteúdos de campanhas ou desinformação e que pode ser necessário olhar para outros atores como provedores de hospedagem de sites e até mesmos serviços da camada de infraestrutura que oferecem suporte às aplicações de Internet, como CDNs.[44] Adicionalmente, a aprovação do Projeto de Lei 2.630/2020, sobre fake news, pode resultar em um modelo de responsabilidade de intermediários segmentado (redes sociais x demais provedores), com fronteiras conceituais imprecisas e capazes de afetar um conjunto de atores mais amplo do que o pretendido com o projeto de lei.

Disseminação de discurso de ódio como ferramenta de silenciamento – O acirramento no debate online tem resultado em uma maior incidência do discurso incitador de ódio contra minorias e propagador de discriminação. Esse debate tem trazido à tona argumentos em prol da criminalização desse tipo de conteúdo e eventualmente da participação na disseminação destes tipos de conteúdo no modelo de negócio de alguns intermediários.[45]

Financiamento de anúncios e impulsionamento de conteúdos – O surgimento de movimentos como o Sleeping Giants[46] têm introduzido questões sobre uma possível responsabilização por financiamento de esquemas de desinformação e discurso de ódio. Outro fator relevante é o recente escândalo da Cambridge Analytica e o seu direto impulsionamento na aprovação de uma lei

40. A Internet Society vem monitorando as discussões sobre o modelo de responsabilidade de intermediários do Marco Civil da Internet realizadas no âmbito do Congresso Nacional e Poder Judiciário ao longo do ano de 2020. O monitoramento tem produzido relatórios trimestrais oferecidos ao capítulo brasileiro para apoiar as atividades da ISOC Brasil a respeito do tema.
41. Supremo Tribunal Federal. Repercussão geral n. 987. Ver *http://www.stf.jus.br/portal/jurisprudenciaRepercussao/verAndamentoProcesso.asp?incidente=5160549&numeroProcesso=1037396&classeProcesso=RE&numeroTema=987*
42. Francisco de Mesquita Laux. "O Supremo Tribunal Federal debate o artigo 19 do Marco Civil da Internet". *Consultor Jurídico. Ver https://www.conjur.com.br/2019-nov-04/stf-debate-artigo-19-marco-civil-Internet*
43. Congresso Nacional. Comissão Parlamentar Mista de Inquérito das Fake News. Ver *https://legis.senado.leg.br/comissoes/comissao?0&codcol=2292*
44. A CPMI das Fake News chegou a solicitar a transferência de sigilo dos registros de acesso e de conteúdo relacionado ao *Bulkservice* hospedado na Cloudflare.
45. Um exemplo relevante é o do crescente movimento Stop Hate for Profit, que tem pautado boicotes a plataformas como Facebook ante a inércia para remover conteúdo de ódio e racista da rede social.
46. Yuri Ferreira. "Sleeping Giants: a luta contra as fake news que tira o sono de políticos no Brasil e no Mundo". Ver *https://www.hypeness.com.br/2020/05/sleeping-giants-a-luta-contra-as-fake-news-que-tira-o-sono-de-politicos-no-brasil-e-no-mundo*

brasileira de proteção de dados pessoais capaz de proteger os usuários ante práticas como micro-direcionamento e segmentação de usuários em categorias específicas para este fim.

Transparência algorítmica – O debate sobre mais transparência sobre práticas de oferta de conteúdos, segmentação de usuários em grupos de interesse e discriminação algorítmica segue ganhando corpo e, com ele, a demanda de discussão de padrões éticos para a implementação de sistemas algorítmicos e IA.

Ante os temas elencados acima, um desafio imediato é a necessidade de se defender o princípio da isenção de responsabilidade de intermediários como o modelo equilibrado e capaz de conciliar os interesses privados e direitos dos indivíduos. Apesar dos desafios de 2020 alimentarem um ethos de "fazer alguma coisa" em termos de regulamentação da Internet, substituir um sistema de proteções que funciona e é capaz de garantir direitos por visões míopes hiper-simplificadas de como funciona a Internet é algo arriscado e com implicações sistêmicas maiores.

IV. Conclusão

Pode-se dizer que a importância de uma lei como o Marco Civil da Internet recai na conciliação entre os direitos dos usuários e a promoção de uma compreensão mais técnica sobre a Internet e os produtos e serviços estruturantes para as camadas de conteúdo e infraestrutura (bem como suas limitações).

Sobre a garantia da liberdade de expressão e fomento à inovação, a separação promovida pelo Marco Civil da Internet entre provedores de infraestrutura e conteúdo é um fator que permitiu o desenvolvimento de novos serviços e produtos de maneira irrestrita. O cenário de segurança jurídica introduzido com o modelo brasileiro de responsabilidade de intermediários foi um acontecimento que permitiu não apenas uma ponderação apropriada entre os direitos dos usuários, mas também a eliminação de riscos nas atividades de curadoria de conteúdos por parte dos provedores de aplicações de Internet.

A adoção de medidas que tivessem por objetivo responsabilizar um ponto específico ou categoria de provedor acabaria por inviabilizar a atuação de muitos outros que estivessem na mesma categoria, inclusive em casos onde ocorre a integração vertical e um mesmo agente atua nas diversas camadas estruturantes do ecossistema da Internet. A complexidade e diversidade das atividades desenvolvidas por essas empresas – que perpassam desde os serviços de hospedagem de websites até as redes sociais, passando pela gestão de redes de entrega de conteúdo e até mesmo pela infraestrutura de telecomunicações associadas a seus serviços – são fatores relevantes para se compreender a natureza adaptável e em permanente evolução dos serviços e produtos ofertados.

A compatibilização de algumas das demandas colocadas ante os desafios postos ao modelo de responsabilidade de intermediários do Marco Civil da Internet deveria resguardar as ideias elencadas na lei brasileira – preservação da livre atividade dos provedores de conexão como pressuposto de garantia do acesso à Internet e a ideia de isenções parciais de responsabilidade civil dedicada a intermediários de Internet por conteúdos que não sejam de sua autoria. Conforme destacado por um dos entrevistados da presente pesquisa, "a criação de leis para a Internet não pode ser orientada exclusivamente pelas atividades de empresas como Google ou Facebook e deve promover uma coordenação com os vários modelos de negócios existentes, para não correr o risco de eliminá-los".

Nesse sentido, a necessidade de defesa do modelo de responsabilidade de intermediários do MCI é indispensável e, junto dela, reaparece a necessidade de se promover uma compreensão mais granular dos provedores de aplicações de Internet e a relação de suas funções com o acesso dos usuários a determinados conteúdos.

A compreensão a respeito das diferenças entre o que é a Internet e o que é tudo aquilo que é montado a partir dela segue sendo fundamental para que medidas legislativas direcionadas a um ponto desse ecossistema complexo não acabem por impactar de maneira indesejada e contraproducente outros pontos que são absolutamente cruciais para que a

Foto: Gustavo Lima/Câmara dos Deputados

rede siga sendo "aberta, global, segura e confiável para todas as pessoas em todos os lugares".

Em 1995 (quando foi criado o CGI.br), ou até em 2014, o paradigma de regulação do tema da responsabilidade dos intermediários era o de se garantir um ambiente mínimo para o exercício da liberdade de expressão e livre discurso e, ao mesmo tempo, preservar a inovação trazida pela Internet a qualquer custo. No entanto, um dos principais desafios que o Marco Civil da Internet e seu modelo de responsabilidade de intermediários enfrentam em 2020, na prática, transcende o tema específico das isenções totais ou parciais de responsabilidade aos intermediários da Internet. Ele diz respeito, de maneira mais ampla, à própria natureza dos tipos de intervenções legislativas que são capazes de potencializar todos os benefícios que a Internet é capaz de gerar para o desenvolvimento socioeconômico e humano.

Para além do Brasil, os EUA, a Europa e diversos outros países estão no meio de batalhas legislativas sobre o futuro da responsabilidade dos intermediários, algo que certamente influenciará outros países da América Latina nos desdobramentos futuros a respeito do tema. Entre os assuntos discutidos estão reflexões sobre quais tipos de serviços merecem de fato serem salvaguardados, quais são as principais ameaças e até os reais efeitos de novas regulamentações na Internet como a conhecemos.

As respostas dadas a essas perguntas são essenciais para saber de que forma as políticas públicas e os marcos regulatórios que serão adotados daqui em diante impactarão a Internet. No caso brasileiro é importante defender o modelo de responsabilidade do Marco Civil da Internet como a solução equilibrada entre direitos e obrigações que a lei dedicou-se a apresentar, algo alinhado e capaz de potencializar o "modo Internet de interconectividade". É extremamente importante, nesse sentido, assegurar que eventuais reformas que ocorram no futuro no ordenamento jurídico brasileiro mantenham esse alinhamento e não impactem negativamente aquilo que serve como fundação para uma Internet aberta, global, segura e confiável para todas as pessoas em todos os lugares. ●

POLITICS 31

ANO XIII

EDITOR CARLOS A. AFONSO • TRADUÇÕES OONA CASTRO E CARLOS A. AFONSO • REVISÃO OONA CASTRO E PAULO DUARTE • COORDENAÇÃO TÉCNICA PAULO DUARTE • PROGRAMAÇÃO VISUAL LIQUIDVISION

Os textos publicados aqui são de responsabilidade de seus autores, não necessariamente representando os pontos de vista das entidades às quais estão vinculados, salvo indicação explícita em contrário.

A tiragem das nossas edições é pequena. Se você quiser receber gratuitamente a edição impressa, envie um e-mail para **politics@nupef.org.br** com seu nome, endereço completo - incluindo o CEP - e a sua área de atuação.

Todas as edições estão disponíveis em https://politics.org.br

ISSN: 1984-8803

*A POLI**TICS** procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro). Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuizo ao conteúdo, aderência ao SI. Para mais informação: http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp*

Originais compostos em LibreOffice e Linux.

O Instituto Nupef é uma organização sem fins de lucro, dedicada à reflexão, análise, produção de conhecimento e formação, principalmente centradas em questões relacionadas às Tecnologias da Informação e Comunicação (TICs) e suas relações políticas com os direitos humanos, a democracia, o desenvolvimento sustentável e a justiça social.

Além de realizar cursos, eventos, desenvolver pesquisas e estudos de caso, o Nupef edita a POLI**TICS**, a Rets (Revista do Terceiro Setor) e mantém o projeto Tiwa – um centro de serviços Internet que serve de apoio técnico aos projetos do instituto e das entidades parceiras.

POLITICS

instituto nupef

https://nupef.org.br . https://politics.org.br . https://espectro.org.br . https://rets.org.br . https://tiwa.org.br