Instituto
de Tecnologia
& Sociedade
do Rio

Trabalhos finais do Grupo de Pesquisa 2020

Amanda Leal
Beatriz Souza Costa
Elora Raad Fernandes
Julia Iunes
Juliana Medeiros
Paula Guedes
Rafael Ribeiro Neto

Sumário

Trabalho final do IV Grupo de Pesquisa ITS Rio

Combatendo a desinformação online:

qual o espaço da educação digital nas medidas legislativas propostas pelo Parlamento Brasileiro?

Amanda Leal & Julia Iunes

Democracia e Tecnologia

Introdução

Apesar da longa história da desinformação na sociedade[1], esta palavra vem sendo empregada eminentemente no contexto das "fake news" desde que a expressão ganhou projeção mundial, com as eleições presidenciais americanas de 2016[2]. Durante as eleições presidenciais brasileiras de 2018, a questão da desinformação, no contexto democrático, ganhou ainda mais relevância, sobretudo diante de práticas de disseminação coordenada de notícias falsas, adotadas como mecanismo de manipulação de campanha[3].

Para além do cenário eleitoral, a preocupação mais recente com o tema da desinformação se deu no atual contexto de pandemia, momento em que nos deparamos com uma avalanche de conteúdos falsos relativos ao tema do coronavírus[4] [5], sendo espalhados não apenas por usuários comuns da rede, mas também por autoridades públicas. Houve diversos casos emblemáticos de remoção de postagens em redes sociais relacionadas à pandemia, como ocorrido com o Presidente do Brasil, Jair Bolsonaro[6] e o presidente da Venezuela, Nicolás Maduro[7]. Ainda, pela primeira vez na história, o Facebook removeu uma postagem de um Presidente dos Estados Unidos, após Donald Trump postar conteúdo de uma entrevista em que afirmava que crianças seriam praticamente "imunes ao coronavírus"[8]. Neste cenário, plataformas como o Twitter, Facebook e Instagram realizaram mudanças em seus termos de uso[9] para fundamentar a política de remoção de conteúdos falsos relativos ao coronavírus, além de experimentar novas alternativas de moderação que, ao invés de optar pela remoção do conteúdo, priorizam por conscientizar o usuário da rede social sobre a autenticidade das informações circuladas.

Como exemplo de iniciativa neste sentido, pode ser citada a nova ferramenta do Instagram[10], que notifica os usuários sobre a veracidade de alguns conteúdos e também apresenta uma justificativa do porquê determinada informação é apontada como falsa e qual seria a versão correta indicada pela agência de checagem de fatos que analisou o post. O Facebook também passou a tomar algumas medidas, como o envio de uma notificação aos usuários que curtiram ou interagiram com boatos sobre o coronavírus, encaminhando-os um link de acesso a informações oficiais no site da Organização Mundial da Saúde — OMS[11].

Essas ferramentas podem ser consideradas como medidas de educação digital disponibilizadas pelas plataformas, uma vez que conferem ao usuário a possibilidade de ter contato com fontes de informação diversas sobre determinado tema e, principalmente, fontes de instituições públicas oficiais e/ou jornalísticas. A notificação sobre conteúdos enganosos e o convite para que o usuário possa checar a informação são mudanças na arquitetura da plataforma que, embora ainda estejam em uma fase experimental, adquirem o papel de estimular o usuário de rede social a adotar uma perspectiva mais crítica na produção e consumo das informações

online. Isto perpassa, dentre outras práticas, por duvidar da veracidade dos conteúdos circulados, checar fontes, buscar informações diversas e, preferencialmente, aquelas amparadas por fontes oficiais ou jornalísticas. Habilidades como essas são essenciais, sobretudo atualmente, pois, segundo a própria Organização Mundial da Saúde, estaríamos vivendo em um contexto de infodemia[12].

Este cenário suscita questões sobre o espaço que tem sido dado à educação digital também nas iniciativas de combate à desinformação online desenvolvidas pelo Poder Público. Declarações internacionais, frutos de debates multissetoriais sobre o tema, vêm sendo adotadas desde 1982, a partir da crescente preocupação dos países em relação às novas tendências da "sociedade da informação"[13]. A Declaração de Grünwald, fruto do Simpósio Internacional de Educação Midiática de 1982, promovido pela UNESCO, reconheceu, há 38 anos, a necessidade de se promover uma compreensão crítica do fenômeno da comunicação, tendo em vista a onipresença da mídia na sociedade. Posteriormente, no ano de 2005, a Proclamação de Alexandria definiu que "a alfabetização informacional e a aprendizagem ao longo da vida são os faróis da Sociedade da Informação, iluminando os rumos para o desenvolvimento, a prosperidade e a liberdade"[14].

Portanto, pode-se dizer que este cenário informacional, em franca evolução há pelo menos quatro décadas, exige ações positivas do Poder Público, a partir de iniciativas multissetoriais que incluam a sociedade civil e também as plataformas de redes sociais, tendo em vista que, no contexto atual, são elas as administradoras da arquitetura informacional onde circula a maioria dos debates da rede[15]. Apesar disso, o momento atual de pandemia - no qual a desinformação gera um risco real e iminente à saúde das pessoas - parece lançar luz não só sobre a urgência, como também, sobre a provável carência de iniciativas neste sentido no Brasil.

A partir deste cenário, a presente pesquisa se propõe a questionar que tipos de proposições estão sendo consideradas pelo parlamento brasileiro para enfrentar a desinformação, e se as medidas propostas consideram a educação midiática e digital (*media literacy*) como alternativa para o tratamento da questão. As hipóteses levantadas pela pesquisa são as de que: **i)** o tema da desinformação é pautado no debate legislativo, predominantemente através de abordagens criminais, e de que **ii)** há uma insuficiência de abordagens educativas e multissetoriais para o tratamento do problema.

Diante disso, os objetivos específicos do trabalho consistem em: **i)** investigar as iniciativas propostas no parlamento brasileiro para enfrentar o problema da desinformação, a partir de uma análise dos projetos de lei em trâmite no Congresso Nacional, no intuito de **ii)** identificar se a educação midiática e digital dos cidadãos é uma abordagem considerada pelas propostas em andamento.

Para isso, este artigo se encontra dividido em três partes. A primeira parte

conta com uma conceituação dos principais termos desta pesquisa: “desinformação”, “educação midiática” e “abordagem multissetorial”. A segunda apresenta os resultados do levantamento dos projetos de lei em trâmite no Congresso Nacional, no intuito de verificar se a educação é considerada pelas propostas legislativas como uma das alternativas no combate à desinformação. A terceira parte do artigo apresenta considerações finais sobre o tema da educação midiática e digital no contexto legislativo.

1. O papel da educação digital e de uma abordagem multissetorial no combate à desinformação.

Para compreendermos o papel da educação digital e da abordagem multissetorial no combate à desinformação, mostra-se necessário esclarecermos, ainda que brevemente, esses conceitos e suas variações. Esta parte do trabalho tem como objetivo indicar como o conceito de educação digital se relaciona ao contexto da desinformação e qual seria a importância de uma abordagem educativa, combinada à atuação multissetorial de governos, plataformas e sociedade civil para o tratamento deste problema.

1.1 O desafio em conceituar “desinformação”

O problema da desinformação na sociedade e seus impactos negativos na cultura democrática tem adquirido novos contornos com a chegada das redes sociais[16]. No entanto, vale observar, logo de início, que não se trata de um problema novo. Em curioso artigo sobre o tema, *“The True History of Fake News”*[17], o historiador americano Robert Darnton conta como o emprego de “notícias falsas” com impacto público foi uma prática recorrente nos mais diversos períodos da história, especialmente com o objetivo de alcançar resultados políticos. O autor retrata que, no século XVI, por exemplo, o poeta italiano Pietro Aretino, em uma tentativa de manipular as eleições de um novo Papa para a Igreja Católica, em favor da família Médici, escrevia sonetos “perversos”[18] sobre todos os outros candidatos. Esses sonetos eram colados no busto de uma estátua conhecida como “Pasquino”, e ao longo do tempo, essa prática, que ficou conhecida como “pasquinada”[19], tornou-se um hábito em Roma.

Para Darnton, a “pasquinada” seria um gênero comum de divulgação de “notícias maldosas, na maioria das vezes falsas, sobre figuras públicas”[20]. No entanto, é interessante observar que, apesar de Darnton interpretá-las como uma expressão antiga do que hoje são as “fake news”, outros estudiosos do tema compreendem essa tradição como parte de um “ritual cívico” da cultura italiana, seja para a divulgação de “sátiras”[21], criticando a conduta de agentes político-religiosos[22], ou de manifestações livres da “opinião popular” e da “atividade política”[23] da época.

Há quem diga que o Pasquino de Roma é a versão antiga do que hoje são as redes sociais. Mas, se Pietro Aretino publicasse seus sonetos "perversos" no Twitter ou Facebook, será que seus textos seriam considerados como fake news por essas plataformas? Ou seriam uma manifestação legítima da liberdade de expressão? O caso das "pasquinadas" pode ser um exemplo de como a divulgação de conteúdos falsos é uma prática antiga, mas também é um exemplo da dificuldade em se alcançar um conceito objetivo do que seja a "desinformação", e que tipo de práticas de divulgação de "conteúdos falsos" são nocivas e merecem ser combatidas.

No que se refere ao tema da desinformação, especialistas já definiram que o termo "fake news" é um conceito inadequado para capturar a complexidade do problema. Isto porque o cenário da desinformação online vai além da simples disseminação de conteúdos "falsos". O termo desinformação (*lato sensu*) abarca uma série de práticas que podem caracterizar ao menos três tipos de desordem no ambiente informacional, que têm sido compreendidas pelos seguintes termos: *"misinformation"*, *"disinformation"* (*stricto sensu*) e *"mal-information"*.

No primeiro caso, não existe a intenção do propagador da mensagem em espalhar conteúdo falso, mas sim um equívoco da pessoa que o dissemina, ao imaginar que o conteúdo seja verdadeiro[24]. Seria o caso, por exemplo, de uma informação "mal compreendida", ou mal interpretada[25]. Por outro lado, nos casos de *"disinformation"* e *"mal-information"*, existe a intenção de disseminar conteúdo com a finalidade de *enganar* ou de *causar dano*. Desta maneira, o termo *"disinformation" (stricto sensu)* é utilizado para representar aqueles casos em que a pessoa que compartilha o conteúdo sabe de sua falsidade e, portanto, tem a intenção de propagar desinformação[26]. Por sua vez, práticas de *"mal-information"* consistem na criação e/ou distribuição de informações fabricadas, que podem ser verdadeiras ou misturadas com fatos verdadeiros, na intenção de causar dano[27].

Esta diferenciação entre esses três cenários principais é essencial para caracterizarmos a abrangência do fenômeno da desinformação e o dissociarmos do uso indiscriminado da expressão "fake news", que tem sido frequente no meio político. Conforme definido pela Comissão Europeia, em relatório produzido por especialistas[28], além da diferenciação trazida acima, é preciso definir a desinformação como formas de expressão que não sejam abarcadas por discursos que já são tipificados como ilegais, como difamação, discurso de ódio, incitação à violência, entre outros, mas que podem causar prejuízo. Também não deveriam ser consideradas como desinformação aquelas formas de expressão que deliberadamente distorcem os fatos, mas com uma finalidade de crítica artística e/ou política e não com uma intenção enganosa, como seria o caso de sátiras e paródias.

Para além de uma distinção conceitual, também parece fundamental compreender que práticas de *"disinformation"* e *mal-information"* vão muito além da mera

produção de um conteúdo travestido de notícia, mas englobam todo um sistema de disseminação amparado por contas automatizadas, redes de perfis falsos, vídeos manipulados, publicidade de *"microtargeting"*, memes, entre outras estratégias[29]. Essas práticas deliberadas de criação e compartilhamento de conteúdo falso para enganar ou causar dano estão, em grande parte das vezes, inseridas em um verdadeiro "mercado da desinformação"[30]. Esses "mercados" estão constantemente atualizando seu *know-how* sobre o funcionamento dos algoritmos das plataformas, justamente com a finalidade de construir as melhores estratégias para impulsionar conteúdo enganoso e atingir a audiência pretendida.

Além da existência de redes organizadas para o fim de propagar desinformação, esse fenômeno, certas vezes, é aprofundado pela própria arquitetura das plataformas de redes sociais e o funcionamento de seus algoritmos. Já existe uma ampla variedade de estudos científicos que apontam como o *design* das plataformas, ao invés de estimular o debate democrático, pode contribuir com a "radicalização de opiniões"[31], a formação de "filtros bolha" e de "câmaras de eco"[32], nas quais os usuários da rede não têm acesso a opiniões e conteúdos contrários ou alternativos às suas visões políticas. O fenômeno da desinformação envolve, portanto, diversos atores - sejam estatais, não estatais, agindo isoladamente ou coletivamente, bem como as estruturas de circulação e difusão da desinformação, como mídias e plataformas digitais e suas respectivas redes e algoritmos.

1.2. A educação digital, midiática e informacional como alternativa no combate à desinformação

Tendo em vista a difusão massiva e criação exponencial de conteúdos na rede, gerando um tráfego intenso e sem limites territoriais, há anos discute-se medidas, a nível internacional, para adequar o indivíduo a este ecossistema informacional. A Declaração de Grünwald, mencionada anteriormente, incita as autoridades competentes a, entre outros compromissos, criar e apoiar programas abrangentes de educação midiática, desde a pré-escola até a educação de adultos, a fim de desenvolver as habilidades e competências necessárias para o uso e a participação efetiva nos sistemas informacionais de mídias, considerando diversos meios de propagação de informação.

Assim como a desinformação acompanhou o desenvolvimento tecnológico e das mídias, os conceitos que permeiam a educação também sofreram evoluções ao longo do tempo. O termo "alfabetização" é amplamente conhecido como o processo por meio do qual aprendemos a ler e a escrever, ou seja, a utilizar o sistema ortográfico, essencial para a comunicação e o consumo de informação em diferentes meios. Outro conceito relevante neste contexto é o de "letramento", que pode ser definido

"como o estado ou condição de indivíduos ou de grupos sociais de sociedades letradas que exercem efetivamente as práticas sociais de leitura e de escrita", possuindo habilidades e atitudes necessárias para interagir e exercer competências discursivas e cognitivas[33]. Nota-se que, assim como ocorreu com a linguagem escrita, as tecnologias da informação e mídias sociais também inauguraram um novo sistema de comunicação para o qual se exige uma nova linguagem e uma readequação desse processo de "letramento"[34].

No entanto, a adoção dessas novas Tecnologias de Informação e Comunicação (TIC), de forma massiva e repentina, levaram a um uso, a princípio, intuitivo, sem que fosse prestada muita atenção à aprendizagem adequada do sistema digital e midiático e do ecossistema informacional, principalmente para as pessoas que não cresceram diretamente em contato com essa nova linguagem.

Neste cenário, a UNESCO cunhou o conceito de Alfabetização Midiática e Informacional (AMI), que parte da necessidade de se desenvolver habilidades específicas para o exercício da liberdade de expressão e do direito ao acesso à informação nos meios digitais. A AMI surge da conjunção de dois conceitos previamente estabelecidos: i) o conceito de alfabetização informacional, usado para "enfatizar a importância do acesso à informação, a avaliação, a criação e o compartilhamento da informação e do conhecimento"[35], por meio de diferentes ferramentas e canais; e ii) o conceito de alfabetização midiática, que "remonta à inserção de recursos audiovisuais na educação" e pode ser definida como "a habilidade de acessar, analisar, avaliar e criar mensagens através de diversos contextos"[36].

Resumidamente, segundo o marco teórico consolidado pela UNESCO, a AMI pode ser definida pela conjunção das seguintes habilidades: **(i)** compreender o papel e as funções das mídias e de outros provedores de informação nas sociedades democráticas e as condições nas quais essas funções possam ser realizadas; **(ii)** reconhecer e articular sua necessidade informacional para poder localizar, acessar, extrair e organizar informações relevantes; **(iii)** avaliar com senso crítico, em termos de autoria, credibilidade e finalidade, o conteúdo na internet; **(iv)** comunicar sua compreensão sobre o conhecimento criado, com ética e responsabilidade, no meio mais apropriado; **(v)** aplicar as habilidades em TIC[37] para processar informação e produzir conteúdo, engajando-se nas mídias com liberdade de expressão, diálogo intercultural e participação democrática.

A conjunção dessas competências definidas como alfabetização midiática informacional, para a qual utilizamos "educação digital" como sinônimo[38], possibilitaria aos usuários o discernimento em relação ao consumo de informações falsas e o fortalecimento de uma cultura de responsabilidade na circulação das informações nas plataformas de redes sociais.

1.3. A necessidade de uma abordagem multissetorial na promoção da educação digital

Como a desinformação é um fenômeno multifacetado, certamente não existe uma resposta única para o problema. Neste sentido, organismos internacionais têm levantado a necessidade de se implementar uma abordagem multidimensional, quanto às ações a serem empregadas[39], e multissetorial, quanto aos atores que devem fazer parte dessa dinâmica[40]. A abordagem "multidimensional" consiste no emprego de um "conjunto de ações interdependentes"[41] a serem implementadas conjuntamente por governos, plataformas digitais e sociedade civil, como parte de uma atuação também multissetorial.

Neste sentido, mesmo que as plataformas desenvolvam procedimentos autorregulatórios de combate à desinformação - seja para a remoção de conteúdo ou disponibilização de alertas que sinalizem informações não verificáveis - é impossível que se exerça um "controle" absoluto sobre todo o grande volume de conteúdos que circulam pela rede. Sendo assim, é de especial importância que os próprios usuários possuam uma perspectiva crítica no consumo do conteúdo online, sem que dependam das plataformas atuando como "editores", tarefa, inclusive, indesejável, diante dos riscos de censura à liberdade de expressão. Ocorre que a construção de um ambiente informacional saudável depende não apenas dos esforços individuais dos usuários em checar informações ou da autorregulação das plataformas, mas também, de como os governos e as próprias plataformas de redes sociais colaboram para que os cidadãos adquiram as ferramentas necessárias à adoção de uma perspectiva mais crítica na utilização da tecnologia e na interação com os conteúdos online[42]. O cenário exige, portanto, uma abordagem multissetorial, que comporte uma atuação conjunta desses múltiplos atores.

A abordagem multissetorial para a Governança da Internet foi reconhecida como "modelo" no World Summit on Information Society, promovido pelas Nações Unidas, em 2003[43] e 2005[44], e teve destaque na Agenda de Tunis para a Sociedade da Informação[45]. O documento define a abordagem multissetorial como "o desenvolvimento e aplicação por governos, setor privado e sociedade civil, em seus respectivos papéis, de princípios, normas, procedimentos de tomada de decisão e programas conjuntos que moldem a evolução do uso da Internet"[46].

No mesmo sentido, o relatório do Grupo de Trabalho sobre Governança da Internet (WGIG)[47], de 2005, aponta as atribuições de cada setor da sociedade dentro da construção de políticas multissetoriais envolvendo as tecnologias da informação e comunicação, com especial enfoque na governança da internet. Não obstante o protagonismo dos Estados em criar normas e regulações, seja a nível nacional ou internacional, o Relatório sugere que o setor privado contribua para uma construção conjunta, não apenas por meio de sua autorregulação, como também, contribuindo

ativamente no processo legislativo e desenvolvendo propostas de políticas públicas, orientações e ferramentas para gestores públicos, legisladores e outros atores envolvidos nos processos de regulação do ecossistema informacional. O Relatório reconhece, também, a relevância da participação da sociedade civil neste processo, contribuindo para a inclusão e capacitação da população em TIC, agindo para a construção de um processo *bottom-up*, de baixo para cima, inclusivo e focado nos cidadãos, entre outras atribuições.

Um paradigma de abordagem multissetorial no que tange a educação midiática e o combate à desinformação é o Código de Conduta da União Europeia (2018) contra a Desinformação. Ao instituir o "Code of Practice on Disinformation"[48], a Comissão da UE estabeleceu, junto a plataformas como Facebook, Google e Twitter, diversos compromissos, dentre eles o desenvolvimento de ferramentas de alfabetização digital e empoderamento cidadão. Os deveres consistem em:

> **[i]** "(...) investir em produtos, tecnologias e programas para ajudar as pessoas a tomar decisões informadas quando encontrarem notícias online que possam ser falsas"; **[ii]** "(...) desenvolver e implementar indicadores eficazes de confiabilidade, em colaboração com o ecossistema de notícias"; **[iii]** "(...) investir em meios tecnológicos para priorizar informações relevantes, autênticas e oficiais em pesquisas, *feeds* ou outros canais de distribuição classificados automaticamente"; **[iv]** "(...) investir em recursos e ferramentas que facilitam as pessoas a encontrar diversas perspectivas sobre tópicos de interesse público"[49].

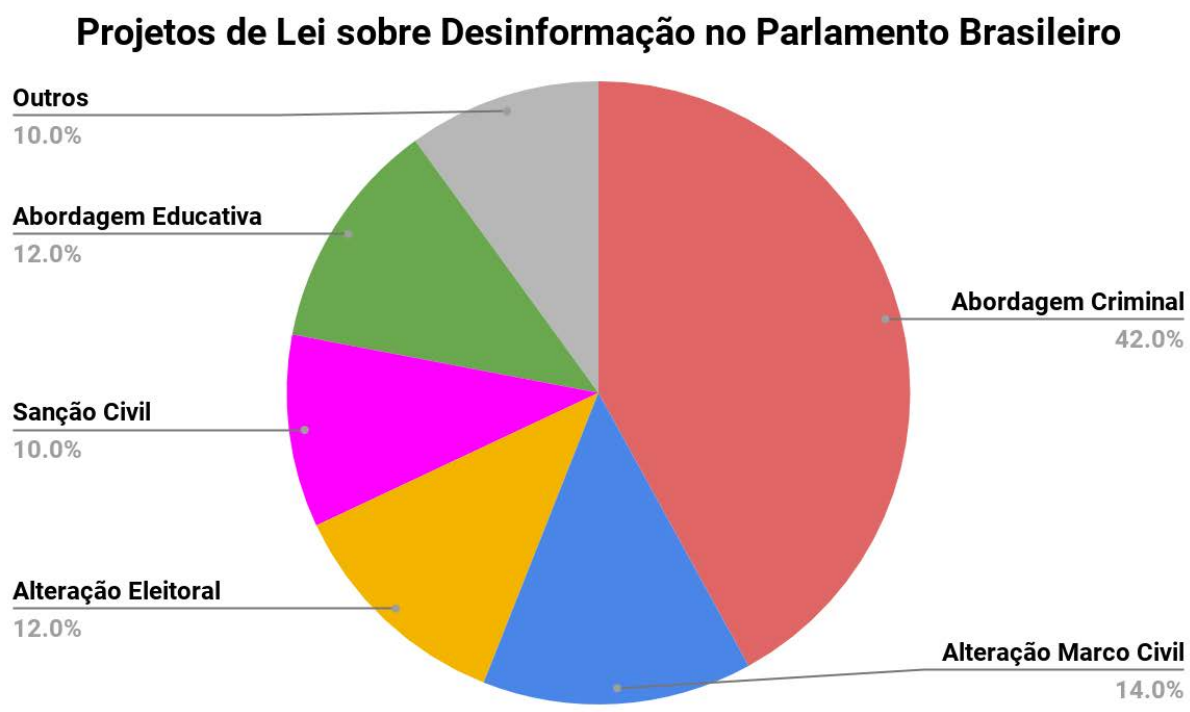
O documento também aponta a necessidade de parcerias entre sociedade civil, governos, instituições educacionais e outras partes interessadas para apoiar os esforços que visam melhorar o pensamento crítico e a alfabetização em mídia digital.

2. O debate legislativo sobre desinformação no Brasil

Iniciativas como o Código de Conduta da União Europeia nos fazem questionar como a questão da educação digital tem sido tratada nos debates sobre desinformação no Brasil. Os parlamentares consideram a educação digital como alternativa no combate à desinformação? Com que frequência esse tema aparece no debate legislativo? Para responder a essas perguntas, foi feito um levantamento dos projetos de lei sobre desinformação, em trâmite no Congresso Nacional, a partir da busca nos sites da Câmara dos Deputados e do Senado Federal[50]. Foram utilizadas as seguintes palavras-chave: "fake news"; "desinformação"; "notícia falsa"; "educação"; "educação digital"; "educação midiática" e "educação informacional"[51].

A partir dessa pesquisa, foram analisados 59 projetos de lei em tramitação, divididos em seis principais abordagens, conforme indicado no gráfico a seguir: **i)** abordagem criminal, consistindo em propostas que tipificam condutas, alteram penas existentes e/ou criam agravantes ou atenuantes em tipos penais; **ii)** abordagem educativa, que consiste na previsão de um ou mais aspectos que compõem a alfabetização midiática e informacional; **iii)** alteração ao Marco Civil da Internet; **iv)** alteração ao Código Eleitoral; **v)** sanção civil e **vi)** outras.

Importa observar que as porcentagens indicadas no gráfico se referem à frequência com que cada uma dessas abordagens aparece no debate legislativo. Não são, portanto, indicativas da porcentagem de projetos encontrados, tendo em vista que um mesmo projeto de lei pode conter mais de uma das abordagens acima referidas.



Conforme esperado, a maior parte das abordagens adotadas nos projetos é classificada como criminal (42%)[52]. Com algumas variações, grande parte das propostas visa alterar o Código Penal, tipificando como crime as condutas de criação, divulgação e compartilhamento de conteúdos falsos online. Alguns projetos têm como objetivo criminalizar a divulgação de conteúdos falsos para assuntos específicos, como, por exemplo, informações inverídicas sobre vacinas[53] ou sobre a atual pandemia do coronavírus[54]. Outros têm por finalidade modificar o Código Eleitoral, a maioria destes propondo alterações ao artigo 323[55], que tipifica como crime eleitoral a divulgação de conteúdos sabidamente inverídicos em relação a candidatos e partidos políticos[56].

Observa-se que, dentre todas as propostas de criminalização encontradas, apenas algumas[57] exigem que o propagador da mensagem saiba que o conteúdo é falso para que a conduta seja caracterizada como crime. Iniciativas neste sentido estariam, ao menos, eximindo de responsabilização criminal aquelas pessoas

que compartilham conteúdo falso de forma equivocada, ou seja, sem que tenham a consciência da falsidade da informação transmitida - casos caracterizados como *"misinformation"*. Por outro lado, outros projetos sequer levam em consideração a intenção do agente para que a conduta seja tipificada como crime[58], de modo que, mesmo sendo um caso de *"misinformation"*, no qual a pessoa compartilha a mensagem sem a intenção de propagar desinformação, ainda assim a pessoa seria penalizada pelo compartilhamento do conteúdo falso.

Chama atenção o perigo que reside no generalismo destes PLs, ao buscar tipificar como crime condutas amplas, que podem atingir direitos fundamentais, abrindo precedente para a repressão de práticas que possam estar legitimamente enquadradas no espectro da liberdade de expressão. Exemplo representativo disso é o caso do PL 6.812/2017[59] que, em seu art. 1º estipula que "constitui crime divulgar ou compartilhar, por qualquer meio, na rede mundial de computadores, informação falsa ou prejudicialmente incompleta em detrimento de pessoa física ou jurídica". Diante da amplitude de condutas que podem ser enquadradas dentro de tipificações abrangentes como esta, é altíssimo o risco de censura e criminalização de manifestações legítimas como, por exemplo, sátiras, paródias e obras artísticas que visam representar releituras ou versões alternativas a fatos da realidade. Além disso, tais iniciativas de criminalização parecem ir na contramão do caráter residual e fragmentário do direito penal, que deve ser considerado apenas como último recurso para a proteção de bens jurídicos[60]. Apesar de todas as críticas e riscos que incidem sobre este tipo de abordagem, a abordagem criminal, como visto, é a mais recorrente no discurso legislativo como forma de tratar o fenômeno da desinformação.

Outra abordagem presente no debate legislativo como alternativa ao combate à desinformação propõe alterações ao Marco Civil da Internet (14%) destinadas, principalmente, a modificar o regime de responsabilização das plataformas pela circulação dos conteúdos postados por terceiros. Outros buscam modificar a legislação eleitoral (12%) propondo alterações ao crime eleitoral de criação e/ou divulgação de informações falsas sobre agentes políticos. Existem, ainda, outros projetos com abordagens genéricas (10%), estabelecendo regras no que concerne, por exemplo, à obrigatoriedade dos provedores de aplicação exigirem o cadastro de documento de identificação oficial dos usuários, para efeito de eventual responsabilização pelo compartilhamento de conteúdo falso (PL 3.389/2019)[61] ou mesmo a identificação de jornalistas responsáveis pela divulgação de matérias (PL 517/2020)[62], bem como regras atinentes a direito de resposta (PL 6.337/2019)[63].

Em contraposição ao cenário criminal, verifica-se que apenas uma pequena parte dos projetos investe em uma abordagem educativa (12%) como forma de lidar com a questão. Neste aspecto, o PL 3.144/2020 indica que a "educação, desenvolvimento do pensamento crítico e alfabetização digital" são pressupostos básicos do combate

à desinformação[64]. Embora também adote uma abordagem criminal para tratar o problema, o projeto estipula que é dever do Estado promover a "alfabetização digital em todos os níveis" e a "educação midiática abrangente, de alta qualidade e sistemática"[65]. Neste sentido, determina que o Poder Público deve realizar a capacitação de cidadãos, servidores públicos e professores para o "uso seguro, consciente e responsável dos meios de comunicação, abrangidas as aplicações de rede", o que incluiria campanhas para "evitar a desinformação e promover a transparência sobre conteúdos patrocinados"[66].

Apesar da menção ao dever do Estado em proporcionar, de forma genérica, o acesso à educação digital, esta proposta não indica ações objetivas a serem adotadas para a efetivação deste direito. Quanto a este aspecto, a determinação que mais se aproxima de algum comando objetivo é a criação de um Comitê de Combate à Desinformação (CCD) integrado por membros do Poder Executivo, o qual, dentre outras atribuições, teria o dever de incentivar "ampla educação digital e conscientização social quanto aos impactos negativos da desinformação", a partir da realização de "palestras e seminários em escolas e órgãos públicos"[67]. Outro projeto, ainda mais genérico, mas com recomendação similar a esta última, é o PL 1.974/2019[68], que propõe a criação de uma "semana nacional de enfrentamento às fake news", na qual órgãos da administração pública e entidades de ensino devem promover ações de conscientização sobre os efeitos danosos da desinformação, bem como iniciativas de estímulo ao seu combate. Como se pode notar, esta proposta também peca ao não trazer recomendações mais específicas sobre essas ações.

Para além destas propostas, existe ainda um grupo de 4 projetos (PLs 1.077/2015, 6.663/2016, 7629/2017, 559/2019 e 1.563/2019) com previsões de modificação da base nacional curricular para incluir as seguintes disciplinas: "utilização ética das redes sociais e mídias digitais, contemplando a abordagem contra a divulgação de notícias falsas (Fake News)"[69]; "educação digital"[70] e "educação e segurança digital"[71]. As propostas indicadas nesse grupo de projetos parecem ter um potencial maior de eficácia quando comparadas às anteriores, tendo em vista que, se implementadas, existiria a obrigatoriedade do Estado em fornecer disciplina específica dentro da grade curricular, o que, se efetivamente cumprido, alcançaria estudantes de escolas públicas e privadas, em nível nacional.

Dentre as propostas concernentes à educação digital, vale destacar, por fim, as recomendações estabelecidas pelo PL 2.630, intitulado "Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet", que ficou popularmente conhecido como "PL das Fake News". O projeto, que foi aprovado pelo Senado e atualmente se encontra em tramitação na Câmara dos Deputados, demonstra alguma consciência quanto à necessidade de se investir em iniciativas de educação digital para tratamento da desinformação online. Inicialmente, indica que o dever do Estado na prestação

da educação "inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet".

Para além desse dever genérico, foram identificadas no projeto duas recomendações específicas que, acredita-se, podem ser interpretadas como caminhos mais objetivos para a concretização da "educação digital". A primeira é o estabelecimento de um dever das plataformas de redes sociais em "identificar" e disponibilizar para os usuários "de maneira destacada", informações sobre os conteúdos "impulsionados", ou seja, aqueles sobre os quais houve pagamento à rede social para que alcançassem uma maior divulgação[72]. Esta previsão contribui, em parte, para duas das competências da AMI, quais sejam: i) compreender o papel e a função das mídias que veiculam a informação e ii) avaliar conteúdo com senso crítico. No entanto, não considera o contexto maior, sobre a arquitetura informacional que seleciona e dispõe os demais conteúdos no *feed* do usuário. Ressalta-se que previsões técnicas como esta necessitam de uma construção multissetorial para que sejam aplicáveis nas plataformas de maneira eficiente e concretizem a intenção do legislador.

A segunda recomendação consiste no direcionamento de recursos para financiar ações de educação digital, seja a partir do direcionamento das multas aplicadas em virtude da lei para o FUNDEB[73], seja por meio da criação de um fundo destinado exclusivamente para financiar ações de educação digital[74]. A segunda opção parece mais eficiente, pois não se limita necessariamente ao público em idade escolar. Não obstante, para uma proposta legislativa que destaca o fortalecimento do processo democrático, a liberdade de expressão e a transparência como objetivos principais[75], há pouco avanço no que tange à educação digital, considerando o conjunto de competências e habilidades elencadas no marco teórico da alfabetização midiática e informacional.

Considerações finais

Apesar da preponderância de abordagens criminais, é possível afirmar que já existe, mesmo que de forma tímida, alguma conscientização no Congresso Nacional sobre o tema da educação digital. É importante ressaltar que, para além dos projetos de lei estudados, o tema já foi introduzido em debates multissetoriais, como a Conferência Legislativa sobre Liberdade de Expressão[76] e o Conselho de Comunicação Social, que trouxeram recomendações relevantes no que tange à educação para o combate à desinformação. Neste aspecto, mostra-se importante que as propostas em tramitação dialoguem com os debates já realizados, rumo a uma evolução construtiva, que se aproveita do conhecimento já produzido acerca do tema.

No ano de 2018, o Conselho de Comunicação Social do Congresso Nacional[77] já havia emitido parecer com algumas orientações baseadas em um estudo de tendências legislativas e "boas práticas" para o combate à desinformação que foram

adotadas ao redor do mundo. Dentre elas: o aumento da transparência sobre as fontes das notícias circuladas e o desenvolvimento de ferramentas destinadas a capacitar os usuários a identificarem desinformação e se adaptarem à rápida evolução dos meios digitais. O parecer do Conselho de Comunicação Social também cita trechos de relevante contribuição para o lugar da educação midiática no debate sobre a desinformação, extraídos de documento apresentado pela Frente Parlamentar pela Liberdade de Expressão e o Direito à Comunicação com Participação Popular (FrenteCom). O parecer conclui que a solução para o problema das *fake news* deve priorizar a implementação de políticas públicas visando à conscientização da população acerca do tema, por meio de uma abordagem multissetorial. Dentre as reflexões neste sentido, destaca-se a seguinte recomendação citada no parecer:

> Políticas públicas de educação para a mídia se fazem urgentes: Políticas públicas de educação para a mídia e a promoção de práticas de empoderamento digital são fundamentais de serem colocadas em curso, incluindo aí o fomento à produção de conteúdos positivos e contranarrativas que engajem a sociedade num debate mais qualificado. Por isso ONU, OEA, OSCE e CADHP defendem "o desenvolvimento de iniciativas participativas e transparentes para uma melhor compreensão do impacto da desinformação e da propaganda na democracia, na liberdade de expressão, no jornalismo e no espaço cívico.[78]

Além dos projetos de lei protocolados nas Casas Legislativas e dos debates multissetoriais citados, desde setembro de 2019 o Congresso Nacional debate a questão da desinformação na Comissão Parlamentar Mista de Inquérito sobre Fake News[79]. A Comissão foi instaurada com os seguintes objetivos: "investigar ataques cibernéticos que atentam contra a democracia e o debate público; a utilização de perfis falsos para influenciar os resultados das eleições de 2018; a prática de cyberbullying sobre os usuários mais vulneráveis da rede de computadores, bem como sobre agentes públicos; e o aliciamento e orientação de crianças para o cometimento de crimes de ódio e suicídio". Em abril de 2020, a comissão teve o seu prazo de funcionamento prorrogado por mais 180 dias. Até o momento, a Comissão teve 23 reuniões, além de audiências públicas. Os projetos de lei apontados no levantamento desta pesquisa também devem ser debatidos na Comissão, o que constituirá mais um espaço para a revisão das perspectivas sobre as medidas mais adequadas para combater a desinformação, no contexto das notícias falsas.

Em que pese o histórico de deliberações sobre educação midiática e digital no combate à desinformação no Legislativo nas ocasiões mencionadas acima, e a relevância do tópico no cenário internacional, não houve um reflexo relevante nas propostas legislativas referentes ao tema no Brasil, conforme observado no

levantamento. Ainda, mesmo as propostas que trouxeram previsões de educação digital, não se aprofundaram no tema. Ressalta-se a relevância de se expandir a perspectiva da educação digital, presente em alguns projetos com enfoque em estudantes, de modo a abranger também o público adulto, grande receptor e propagador de desinformação, público que, como desafio adicional, não é "nativo" da internet e que, além de possíveis obstáculos com a alfabetização literal, carece ainda mais das ferramentas de alfabetização midiática e informacional[80] para que possam adotar uma perspectiva crítica e responsável na produção e consumo de conteúdo online.

Eventuais legislações, elaboradas em consonância com parâmetros internacionais e o contexto brasileiro, poderiam contribuir para avançar políticas públicas baseadas em evidência e lidar com o problema da desinformação de maneira prospectiva e estrutural, construindo um ambiente informacional mais sustentável, em vez de priorizar uma abordagem criminal. A avaliação do cenário atual de alfabetização midiática e informacional no país seria essencial para que se possa dimensionar as necessidades brasileiras e lançar luz sobre possíveis oportunidades legislativas.

Há uma crescente produção científica explorando estratégias para melhorar os espaços online para além de simplesmente sancionar conteúdo problemático ou "maus agentes", cujos resultados sugerem que abordagens educacionais, em vez de punitivas, melhoram o ambiente online[81]. Ainda, se concebidas de maneira multissetorial, tais iniciativas certamente dariam maior visibilidade ao tema e, consequentemente, impulsionariam o desenvolvimento de projetos de educação midiática e informacional também por entes privados e entre a sociedade civil.

Notas

1 BURKHARDT, J. History of Fake News, em: Combating Fake News in the Digital Age. Library Technology Reports, v. 53, n. 8, 2017. Disponível em: https://journals.ala.org/index.php/ltr/issue/viewIssue/662/423

2 ALLCOTT, H.; GENTZKOW, M. Social Media and Fake News in the 2016 Election. Journal of Economic Perspectives, Pittsburgh, American Economic Association, v. 31, n. 2, p. 211-236, 2017. Disponível em: https://web.stanford.edu/~gentzkow/research/fakenews.pdf Acessado em Agosto de 2020.

3 Sobre a disseminação coordenada de notícias falsas no contexto eleitoral em 2018, ver: ITS-Rio. Poder Computacional: Automação no Uso do Whatsapp nas Eleições (2018). Disponível em: https://itsrio.org/wp-content/uploads/2018/10/Poder-Computacional-Relatorio-Whatsapp-Eleicoes-ITS.pdf Acessado em Agosto de 2020.

4 Agência Lupa. Brasil Lidera Desinformação sobre Número de Casos e Mortes por Covid19 no Mundo. Folha de São Paulo, 10 de jun. 2020. Disponível em: https://www1.folha.uol.com.br/equilibrioesaude/2020/06/brasil-lidera-desinformacao-sobre-numero-de-casos-e-mortes-por-covid-19-no-mundo.shtml Acessado em Agosto de 2020.

5 O Instituto Poynter disponibiliza uma base de dados unificada, contendo notícias relativas ao Coronavírus avaliadas por diversas redes de checagem de fatos ligadas à International Fact Checking Agency. A página exibe cerca de 580 reportagens checadas como falsas no Brasil. Disponível em: https://www.poynter.org/ifcn-covid-19-misinformation/?covid_countries=47364&covid_rating=0&covid_fact_checkers=0 Acessado em Agosto de 2020.

6 Facebook e Instagram Removem Vídeo de Jair Bolsonaro por Violação de Regras. G1, 30 de mar. de 2020. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2020/03/30/facebook-e-instagram-removem-video-de-jair-bolsonaro-por-violacao-de-regras.ghtml

7 Bolsonaro foi 2º governante a ter post apagado pelo Twitter; 1º foi Maduro. Veja, 30 de mar. de 2020. Disponível em: https://veja.abril.com.br/mundo/antes-de-bolsonaro-twitter-apagou-post-de-maduro-com-antidoto-caseiro/

8 Facebook and Twitter restrict Trump accounts over 'harmful' virus claim. BBC News, 06 de ago. de 2020. Disponível em: https://www.bbc.com/news/election-us-2020-53673797

9 O Twitter, por exemplo, definiu alguns parâmetros para a remoção de posts que contenham: "Negação das recomendações de autoridades de saúde locais ou globais; [...] Descrição de supostas curas alegadas para COVID-19; [...] Descrição de tratamentos prejudiciais ou medidas de proteção ineficazes [e] [...] Negação de fatos científicos estabelecidos". Uma atualização sobre nossa estratégia contínua durante a COVID-19. Twitter, 16 de mar. de 2020. Disponível em: https://blog.twitter.com/pt_br/topics/company/2019/uma-atualizacao-sobre-nossa-estrategia-continua-durante-o-covid-19.html

10 Sem fake news! Instagram expande medidas de combate à desinformação. Vieira, Nathan, 17 de dez. de 2019. Disponível em: https://canaltech.com.br/redes-sociais/sem-fake-news-instagram-expande-medidas-de-combate-a-desinformacao-158083/

11 Facebook will add anti-misinformation posts to your News Feed if you liked fake coronavirus news. The Verge, 16 de abril de 2020. Disponível em: https://www.theverge.com/2020/4/16/21223456/facebook-coronavirus-misinformation-fake-news-warning-update-who

12 A infodemia é caracterizada pelo excesso de informações sobre determinado tema, "que podem se multiplicar exponencialmente em pouco tempo devido a um evento específico, como a pandemia atual". Neste contexto, existe um desafio adicional em encontrar "fontes idôneas e orientações confiáveis", além de existirem práticas de "manipulação de informações com intenção duvidosa", que, devido às redes sociais, se alastram mais rapidamente, "como um vírus". OPAS (Organização Pan-Americana da Saúde). Entenda a Infodemia e a Desinformação na luta contra a Covid-19, 2020. Disponível em: https://iris.paho.org/bitstream/

handle/10665.2/52054/Factsheet-Infodemic_por.pdf?sequence=14

13 Além da Declaração de Grünwald (1982) e da Proclamação de Alexandria (2005), há, exemplificativamente: a Declaração de Praga para uma Sociedade com Alfabetização Informacional (2003), Agenda de Paris – 12 Recomendações para Educação em Mídia (2007), Declaração de Fez sobre Alfabetização Midiática e Informacional (2011), Declaração de Moscou sobre Alfabetização Midiática e Informacional nas Sociedades do Conhecimento (2012).

14 No original: "Information Literacy and lifelong learning are the beacons of the Information Society, illuminating the courses to development, prosperity and freedom". High-Level Colloquium on Information Literacy and Lifelong Learning, 2006. Disponível em: http://eprints.rclis.org/3829/1/alexfinalreport.pdf Acessado em Agosto de 2020.

15 As plataformas de redes sociais são responsáveis pela governança dos conteúdos e dos processos de interação entre os usuários. São elas que organizam o fluxo informacional, por meio de mecanismos de filtragem, edição e remoção de conteúdo. Neste sentido, ver: GRIMMELMANN, James. The Virtues of Moderation, 17 Yale J.L. & Tech, 2015. Disponível em: https://digitalcommons.law.yale.edu/yjolt/vol17/iss1/2

16 HOFFMANN, Stacie; TAYLOR, Emily & BRADSHAW, Samantha. The Market of Disinformation. Oxford Technology & Elections Commission, 2019. Disponível em: https://comprop.oii.ox.ac.uk/research/oxtec-disinfo-market/

17 DARTON, Robert. The true history of Fake News. The New York Review of Books, fev. 2017. Disponível em: https://www.nybooks.com/daily/2017/02/13/the-true-history-of-fake-news/

18 Segundo Darton (2017) tratavam-se de "wicked sonnets".

19 Segundo o dicionário Michaelis, a "pasquinada" consiste em: "Crítica mordaz escrita em pasquim"; sendo o pasquim: "Folheto satírico afixado em lugar público; [...] de má redação e sem importância; [...] usado para difamar". Disponível em: https://michaelis.uol.com.br/palavra/4b3vQ/pasquinada/ e em https://michaelis.uol.com.br/moderno-portugues/busca/portugues-brasileiro/pasquim/

20 Segundo o original: "The "pasquinade" then developed into a common genre of diffusing nasty news, most of it fake, about public figures". DARTON, Robert. The true history of Fake News. The New York Review of Books, fev. 2017. Disponível em: https://www.nybooks.com/daily/2017/02/13/the-true-history-of-fake-news/

21 Segundo o dicionário Michaelis, a sátira consiste em: "[...] composição poética, livre na forma e na métrica, que censura as instituições, os costumes e as ideias da época, em estilo irônico ou indignado [...] que censura ou ridiculariza de maneira incisiva os defeitos e os vícios". Disponível em: http://michaelis.uol.com.br/busca?id=Xpw5e

22 GILBERT, Christopher J. If This Statue Could Talk: Statuary Satire in the Pasquinade Tradition. Rhetoric and Public Affairs, vol. 18, nº. 1, 2015, pp. 79-112. Disponível em: https://www.jstor.org/stable/10.14321/rhetpublaffa.18.1.0079?seq=1

23 Termos indicados por Gilbert (2015) ao se referir a essa tradição como parte de um "ritual cívico" da cultura italiana.

24 Conforme indicado por Wardle & Derakhshan: "(...) misinformation is information that is false, but the person who is disseminating it believes that it is true". WARDLE, C.; DERAKHSHAN, H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Report to the Council of Europe, 2017, p. 44. Disponível em: https://shorenstein-center.org/information-disorder-framework--for-research-and-policymaking/

25 Usamos o termo "mal-compreendida" por considerar que seria a tradução que mais se aproxima do conceito de "misinformation".

26 Conforme indicado por Wardle & Derakhshan: "Disinformation is information that is false, and the person who is disseminating it knows it is false. It is a deliberate, intentional lie, and points to people being actively disinformed by malicious actors". WARDLE, C.; DERAKHSHAN, H. Op.cit.e, p. 44.

27 Conforme indicado por Wardle & Derakhshan: "(...) those that are true (and those messages with some truth) but which are created, produced

or distributed by “agents” who intend to harm rather than serve the public interest. Such mal--information – like true information that violates a person’s privacy without public interest justification - goes against the standards and ethics of journalism”.WARDLE, C.; DERAKHSHAN, H. Op. cit, p. 44.

28 Independent High Level Group on fake news and online disinformation. A multi-dimensional approach to disinformation. Comissão Europeia, 2018. Disponível em: https://ec.europa.eu/digital--single-market/en/news/final-report-high-level-expert-group-fake-news-and-online-disinformation

29 WARDLE, C.; DERAKHSHAN, H. Op.cit.

30 HOFFMANN, Stacie; TAYLOR, Emily & BRADSHAW, Samantha. The Market of Disinformation. Oxford Technology & Elections Commission, 2019. Disponível em: https://comprop.oii.ox.ac.uk/research/oxtec-disinfo-market/

31 SUNSTEIN, Cass. #Republic; Divided Democracy in the Age ofSocial Media. Princeton University Press, 2017. Disponível em: https://www.amazon.com.br/dp/B079Q4K9TM/ref=dp-kindle-redirect?_encoding=UTF8&btkr=1

32 Neste sentido, ver: FLAXMAN, Seth; GOEL, Sharad; RAO, Justin M. Filter Bubbles, Echo Chambers, and Online News Consumption. Public Opinion Quarterly, vol. 80, issue S1, 2016. Disponível em: https://academic.oup.com/poq/article-abstract/80/S1/298/2223402

33 SOARES, M. Novas práticas de leitura e escrita: letramento na cibercultura. Educ. Soc., Campinas, vol. 23, n. 81, 2002, pp. 143-160. Disponível em: https://www.scielo.br/pdf/es/v23n81/13935.pdf Acessado em Agosto de 2020.

34 UNICEF. The State of the World’s Children 2017: Children in a Digital World, 2017. Disponível em: https://www.unicef.org/uzbekistan/media/711/file/SOWC:%20Children%20in%20a%20Digital%20World.pdf

35 UNESCO, CETIC.BR. Marco de Avaliação Global da Educação Midiática e Informacional, 2016, p. 29. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000246398_por

36 LIVINGSTONE, S. What is media literacy? Intermedia, 32 (3), 2004 pp. 18-20. Disponível em: http://eprints.lse.ac.uk/1027/1/What_is_media_literacy_(LSERO).pdf Acessado em Agosto de 2020.

37 UNESCO. TIC, educação e desenvolvimento social na América Latina e o Caribe, 2017. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000262862_por

38 A escolha pelo uso do termo “educação digital” é devido ao emprego mais decorrente desta expressão no contexto legislativo para exprimir a educação referente aos meios informacionais, midiáticos e digitais.

39 Independent High level Group on fake news and online disinformation (2018), op. cit.

40 Neste sentido, ver: UNESCO. What if we all governed the Internet? Advancing multistakeholder participation in Internet governance, 2017. Disponível em: https://unesdoc.unesco.org/ark:/48223/pf0000259717; INTERNET SOCIETY, Internet Governance: Why the Multistakeholder Approach Works, 2016. Disponível em: https://www.internetsociety.org/wp-content/uploads/2016/04/IG-MultiStakeholderApproach.pdf

41 Segundo o original: “As disinformation is a multifaceted problem, which cannot be addressed by a single measure, the proposed responses should be seen as a set of inter-dependent actions forming part of an overarching, multi-dimensional approach”. Independent High level Group on fake news and online disinformation (2018), op. cit.

42 IOSIFIDIS, P., NICOLI, N. The Battle to End Fake News: a qualitative content analysis of Facebook announcements on how it combats disinformation. The International Communication Gazette, 82, 2019, p. 60-81. Disponível em: https://journals.sagepub.com/doi/abs/10.1177/1748048519880729?journalCode=gazb

43 A primeira fase ocorreu em 2003, na Suíça, e teve por objetivo promover consensos políticos e estabelecer as bases de uma sociedade da informação para todos, refletindo diferentes interesses em questão. Esta etapa do World Summit on Information Society originou dois documentos:

a declaração, disponível em: https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-E.pdf e o plano de ação, disponível em: https://www.itu.int/net/wsis/docs/geneva/official/poa.html

44 A segunda fase do World Summit on Information Society teve por objetivo colocar em prática o plano de ação da fase anterior e estabelecer acordos em tópicos como mecanismos de financiamento e implementação das resoluções. Documentos disponíveis em: https://www.itu.int/net/wsis/documents/index2.htm[1]

45 Tunis Agenda For The Information Society, nov. de 2005. Disponível em: https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.pdf

46 Idem, p. 6.

47 Trata-se de um grupo multissetorial organizado pelas Nações Unidas dentro de seu mandato para o "World Summit on the Information Society", realizado em 2005. Este grupo foi criado após o primeiro "Summit" sobre a Sociedade da Informação, que ocorreu em Genebra, em 2003, com o objetivo de preparar estudos e propor estruturas de trabalho, abrindo caminhos para o consenso entre os países na reunião de Tunis, que resultou na Agenda de Tunis para a Sociedade da Informação.

48 COMISSÃO EUROPEIA. Code of Practice on Disinformation, 2018. Disponível em: https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation

49 COMISSÃO EUROPEIA (2018), op. cit.

50 As buscas foram realizadas no período de 11 de março a 18 de julho de 2020.

51 A pesquisa nos sites da Câmara dos Deputados e do Senado Federal foi realizada em três etapas: (i) pesquisa contínua entre 11/03/2020 e 14/04/2020, sem delimitação temporal no mecanismo de busca; (ii) primeira atualização para inclusão de novos projetos de lei protocolados, em 18/06/2020; (iii) segunda atualização e revisão em 18/07/2020.

52 Do total de 59 projetos encontrados, 34 adotam uma abordagem criminal.

53 Como é o caso do PL 3.842/2019: "Pune quem divulga ou propaga, por qualquer meio, notícias falsas sobre as vacinas do programa nacional de imunização/vacinação de crianças e adolescentes, ou sobre sua ineficiência". Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=0D46B2F0B971E2E543E563D2804EC2AD.proposicoesWebExterno1?codteor=1772934&filename=PL+3842/2019
Também é o caso do PL 5.679/2019: "Torna crime a disseminação de informações falsas sobre vacina, alterando o Decreto-Lei nº 2.848, de 7 de dezembro de 1940, Código Penal". Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=D5C9ACFA936A0F496A947B0B35D06DBA.proposicoesWebExterno1?codteor=1825899&filename=PL+5679/2019

54 Como é o caso dos PLs 2.389/2020, 1258/2020, 1068/2020 e 1416/2020.

55 "Art. 323 do Código Eleitoral: Divulgar, na propaganda, fatos que sabe inverídicos, em relação a partidos ou candidatos e capazes de exercerem influência perante o eleitorado: Pena - detenção de dois meses a um ano, ou pagamento de 120 a 150 dias-multa. Parágrafo único. A pena é agravada se o crime é cometido pela imprensa, rádio ou televisão". Disponível em: http://www.planalto.gov.br/ccivil_03/leis/L4737.htm

56 Como é o caso dos PLs 9.973/2018, 9.626/2018, 10.292/2018, 10.915/2018 e 11.004/2018 (Câmara dos Deputados).

57 É o caso, por exemplo do PL 3.857/2019: "Art. 3º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 – Código Penal, passa a vigorar acrescido do seguinte art. 140-A: Art. 140-A Criar, divulgar, produzir ou compartilhar informação ou notícia que sabe ser falsa por meio da Internet ou outros meios de comunicação em massa: Pena: reclusão um a três anos e multa". (grifo nosso). Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1773418&filename=PL+3857/2019

58 É o caso, por exemplo, do PL 9.884/2018: "Art. 2º Acrescente-se o art. 308-A ao Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. Art. 308-A: Criar, divulgar ou compartilhar, por qualquer meio de comunicação social, a terceiros, informação ou notícia falsa que possa modificar ou desvirtuar a verdade sobre pessoa física e ou

jurídica, que afetem interesse público relevante. Pena - reclusão de dois a quatro anos, e multa". (grifo nosso). Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1647666&filename=PL+9884/2018

59 Dispoinível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1522471&filename=PL+6812/2017

60 Neste sentido, ver: BATISTA, Nilo e ZAFFARONI, Raul. Direito Penal Brasileiro, Editora Revan, 2017.

61 Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1761571&filename=PL+3389/2019

62 Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1862539&filename=PL+517/2020

63 Disponível em:https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1843862&filename=Tramitacao--PL+6337/2019

64 Conforme determina o artigo 1º,. Inciso IV do PL. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1901033&filename=PL+3144/2020

65 Conforme indicado no artigo 21 do projeto. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1901033&filename=PL+3144/2020

66 Conforme indicado no artigo 21 do projeto. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1901033&filename=PL+3144/2020

67 Conforme estabelecido pelo artigo 11, § 1º, inciso X. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1901033&filename=PL+3144/2020

68 Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1727384&filename=PL+1974/2019

69 Conforme disposto no PL 559/2019 (Câmara dos Deputados). Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1708599&filename=PL+559/2019

70 Conforme disposto no PL 6.663/2016, 2.801/2015, 7.629/2017 e 1.563/2019 (Câmara dos Deputados). Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=FEAB009F6F91619DF2FAB56EBDE29BE3.proposicoesWebExterno1?codteor=1515642&-filename=PL+6663/2016; https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1378106&filename=PL+2801/2015; https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1558712&filename=PL+7629/2017 e em https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1720500&filename=PL+1563/2019

71 Conforme disposto nos PLs 1077/2015. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?-codteor=1318745&filename=PL+1077/2015

72 Conforme estipulado pelo inciso II e § 2º do artigo 6º e artigo 16º do projeto, indicados a seguir: "Art. 6º: [...] as redes sociais e os serviços de mensageria privada, no âmbito e nos limites técnicos de seu serviço, devem adotar medidas para: [...] III - identificar todos os conteúdos impulsionados e publicitários cujo pagamento pela distribuição foi realizado ao provedor de redes sociais. [...] § 2º As medidas de identificação de conteúdos impulsionados e publicitários de que trata esse artigo devem ser disponibilizados de maneira destacada aos usuários e mantidos inclusive quando o conteúdo ou mensagem for compartilhado, encaminhado ou repassado de qualquer maneira". (grifo nosso) "Art. 16. Os provedores de redes sociais devem disponibilizar mecanismos para fornecer aos usuários as informações do histórico dos conteúdos impulsionados e publicitários com os quais a conta teve contato nos últimos 6 (seis) meses". (grifo nosso) Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8127649&ts=1597243666825&disposition=inline

73 "Art. 33. Os valores das multas aplicadas com base nesta Lei serão destinados ao Fundo de Manutenção e Desenvolvimento da Educação Básica e de Valorização dos Profissionais da Educação (FUNDEB) e serão empregados em ações de educação e alfabetização digitais". (grifo nosso). Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8127649&ts=1597243666825&disposition=inline

74 "Art. 25. [...] §1º O Conselho de Transparência e Responsabilidade na Internet é órgão responsável pelo acompanhamento das medidas de que trata esta Lei e a ele compete: VII - realizar estudos para a criação de fundo para financiamento da educação digital no Brasil; [...] VII - realizar estudos para a criação de fundo para financiamento da educação digital no Brasil" (grifo nosso). Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=8127649&ts=1597243666825&disposition=inline

75 Ver art. 4º do texto aprovado no Senado Federal, remetido à Câmara dos Deputados. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;jsessionid=82BBD8B041A0A810E3D5C4AEC72677F7.proposicoesWebExterno2?codteor=1909983&filename=Tramitacao-PL+2630/2020

76 A décima segunda edição da Conferência Legislativa sobre Liberdade de Expressão, de maio de 2018, teve por objetivo a discussão da importância da educação midiática na formação da cidadania e no combate a notícias falsas. O evento foi produzido pelo Instituto Palavra Aberta, em parceria com a Câmara dos Deputados e teve maior enfoque na relação da desinformação com crianças e adolescentes, explorando desafios e oportunidades da educação midiática como ferramenta de construção de senso crítico e engajamento cidadão neste público. Gravação da reunião disponível em: https://www.youtube.com/watch?v=P3gIAxdQRTw

77 Órgão multissetorial que tem por atribuição realizar estudos, pareceres e outras atribuições solicitadas que tenham relação com o Título VIII, Capítulo V, "da Comunicação Social", da Constituição Federal.

78 Parecer do Conselho de Comunicação Social nº 1, de 2018. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=7740092&ts=1593906687173&disposition=inline

79 Documentos e histórico disponíveis em: https://legis.senado.leg.br/comissoes/comissao?0&codcol=2292

80 Segundo a UNESCO, os níveis de analfabetismo estão aumentando em razão da exclusão digital, que afeta não apenas os analfabetos, mas também aqueles indivíduos que sejam alfabetizados, na aplicação efetiva de suas competências em diferentes estágios da vida. Ver: UNESCO, CETIC.BR (2016), op. Cit.

81 JHAVER, S.; BRUCKMAN, A.; GILBERT, E. Does Transparency in Moderation Really Matter?: User Behavior After Content Removal Explanations on Reddit. Proc. ACM Hum.-Comput. Interact., vol. 3, nov. de 2019. Disponível em: https://www.cc.gatech.edu/~sjhaver3/Removal_Explanations.pdf Acessado em Agosto de 2020.

Referências Bibliográficas

AGÊNCIA LUPA. Brasil Lidera Desinformação sobre Número de Casos e Mortes por Covid19 no Mundo. **Folha de São Paulo**, 10 Junho 2020. Disponivel em: <https://www1.folha.uol.com.br/equilibrioesaude/2020/06/brasil-lidera-desinformacao-sobre-numero-de-casos-e-mortes-por-covid-19-no-mundo.shtml>. Acesso em: Agosto 2020.

ALLCOTT, H.; GENTZKOW, M. Social Media and Fake News in the 2016 Election. **Journal of Economic Perspectives**, Pittsburgh, EUA, 31, 2017. 211-236. Disponivel em: <https://web.stanford.edu/~gentzkow/research/fakenews.pdf>. Acesso em: Agosto 2020.

BATISTA, N.; ZAFFARONI, R. **Direito Penal Brasileiro**. [S.l.]: Revan, 2017.

BBC. Facebook and Twitter restrict Trump accounts over 'harmful' virus claim. **BBC News**, 06/08/2020. Disponivel em: <https://www.bbc.com/news/election-us-2020-53673797>. Acesso em: Agosto 2020.

BURKHARDT, J. M. History of Fake News, em: Combating Fake News in the Digital Age. **Library Technology Reports**, Chicago, 53, Dezembro 2017. Disponivel em: <https://journals.ala.org/index.php/ltr/issue/viewIssue/662/423>. Acesso em: Agosto 2020.

COMISSÃO EUROPEIA. **Code of Practice on Disinformation**. Comissão Europeia. [S.l.]. 2018.

DARNTON, R. The True History of Fake News. **The New York Review of Books**, 13/02/2017. Disponivel em: <https://www.nybooks.com/daily/2017/02/13/the-true-history-of-fake-news/>. Acesso em: Agosto 2020.

FLAXMAN, S.; GOEL, S.; RAO, J. M. Filter Bubbles, Echo Chambers, and Online News Consumption. **Public Opinion Quarterly**, Oxford, 80, 2016. 298-320.

G1. Facebook e Instagram Removem Vídeo de Jair Bolsonaro por Violação de Regras. **Portal G1, Globo**, 30/03/2020. Disponivel em: <https://g1.globo.com/economia/tecnologia/noticia/2020/03/30/facebook-e-instagram-removem-video-de-jair-bolsonaro-por-violacao-de-regras.ghtml>. Acesso em: Agosto 2020.

GADDE, V.; DERELLA, M. Uma atualização sobre nossa estratégia contínua durante a COVID-19. **Twitter Brasil**, 16/03/2020. Disponivel em: <https://blog.twitter.com/pt_br/topics/company/2019/uma-atualizacao-sobre-nossa-estrategia-continua-durante-o-covid-19.html>. Acesso em: Agosto 2020.

GILBERT, C. J. If This Statute Could Talk: Statutory Satire in the Pasquinade Tradition. **Rhetoric and Public Affairs**, East Lansing, 18, 2015. 79-112. Disponivel em: <https://www.jstor.org/stable/10.14321/rhetpublaffa.18.1.0079?seq=1>. Acesso em: Agosto 2020.

GRIMMELMANN, J. The Virtues of Moderation. **Yale Journal of Law & Technology**, New Haven, EUA, 17, n. 1, 2015. 43-109.

HOFFMANN, S.; TAYLOR, E.; BRADSHAW, S. **The Market of Disinformation**. Oxford Technology & Elections Commission, Universidade de Oxford. Oxford, p. 1-49. 2019.

INDEPENDENT HIGH LEVEL GROUP ON FAKE NEWS AND DISINFORMATION. **A Multi-Dimensional Approach to Disinformation**. Comissão Europeia. Bruxelas, p. 1-44. 2018. (978-92-79-80420-5).

INSTITUTO POYNTER. The CoronaVirusFacts/DatosCoronaVirus Alliance Database. **COVID-19:** Poynter Resources, 2020. Disponivel em: <https://www.poynter.org/ifcn-covid-19-misinformation/?covid_countries=47364&covid_rating=0&covid_fact_checkers=0>. Acesso em: Agosto 2020.

INTERNET SOCIETY. **Internet Governance: Why the Multistakeholder Approach Works**. internetsociety.org. [S.l.].

IOSIFIDIS, P.; NICOLI, N. The Battle to End Fake News: a qualitative content analysis of Facebook announcements on how it combats disinformation. **The International Communication Gazette**, Londres, 82, Outubro 2019. 60-81.

JHAVER, S.; BRUCKMAN, A.; GILBERT, E. Does Transparency in Moderation Really Matter?: User Behavior After Content Removal Explanations on Reddit. **PACM on Human-Computer Interaction**, 3, Novembro 2019. Disponivel em: <https://www.cc.gatech.edu/~sjhaver3/Removal_Explanations.pdf>. Acesso em: Agosto 2020.

LIVINGSTONE, S. What is media literacy? **Intermedia**, Londres, 32, 2004. 18-20. Disponivel em: <http://eprints.lse.ac.uk/1027/1/What_is_media_literacy_(LSERO).pdf>. Acesso em: Agosto 2020.

MACHADO, C.; KONOPACKI, M. **Poder Computacional: Automação no uso do WhatsApp nas Eleições**. Instituto de Tecnologia e Sociedade do Rio de Janeiro. Rio de Janeiro. 2018.

OPAS. **Entenda a Infodemia e a Desinformação na Luta contra a Covid-19**. Organização Panamericana da Saúde. [S.l.], p. 1-5. 2020.

ROBERTSON, A. Facebook will add anti-misinformation posts to your News Feed if you liked fake coronavirus news. **The Verge**, 16/04/2020. Disponivel em: <https://www.theverge.com/2020/4/16/21223456/facebook-coronavirus--misinformation-fake-news-warning-update--who>. Acesso em: Agosto 2020.

SOARES, M. Novas Práticas de leitura e escrita: letramento na cibercultura. **Educação & Sociedade**, Campinas, 23, Dezembro 2002. 143-160.

SUSTEIN, C. R. **#Republic - Divided Democracy in the Age of Social Media**. Princeton: Princeton University Press, 2017.

THE Alexandria Proclamation on Information Literacy and Lifelong Learning, Alexandria, Egito, p. 3-4, 2005. Disponivel em: <http://eprints.rclis.org/3829/1/alexfinalreport.pdf>. Acesso em: Agosto 2020.

UNESCO. **What if we all governed the Internet? Advancing multistakeholder participation in Internet governance**. Organização das Nações Unidas para a Educação, a Ciência e Cultura. [S.l.]. 2017.

UNESCO OFFICE MONTEVIDEO AND REGIONAL BUREAU FOR SCIENCE IN LATIN AMERICA AND THE CARIBBEAN. **TIC, Educação e Desenvolvimento Social na América Latina e o Caribe**. Organização das Nações Unidas para a Educação, a Ciência e a Cultura. Montevidéu, p. 29. 2017.

UNESCO, CETIC.BR. **Marco de Avaliação Global da Educação Midiática e Informacional:** disposição e competências do país. Brasília: [s.n.], 2016. 138 p. ISBN 978-85-7652-215-7. Disponivel em: <https://unesdoc.unesco.org/ark:/48223/pf0000246398>. Acesso em: Agosto 2020.

UNICEF. **Children in a Digital World**. Fundo das Nações Unidas para a Infância. [S.l.]. 2017. (978-92-806-4930-7).

VEJA. Bolsonaro foi 2º governante a ter post apagado pelo Twitter; 1º foi Maduro. **Revista Veja**, 30/03/2020. Disponivel em: <https://veja.abril.com.br/mundo/antes-de-bolsonaro-twitter-apagou-post-de-maduro-com-antidoto-caseiro/>. Acesso em: Agosto 2020.

VIEIRA, N. Sem fake news! Instagram expande medidas de combate à desinformação. **CanalTech**, 17/12/2019. Disponivel em: <https://canaltech.com.br/redes-sociais/sem-fake-news-instagram-expande-medidas-de-combate--a-desinformacao-158083/>. Acesso em: Agosto 2020.

WARDLE, C.; DERAKSHAN, H. **Information Disorder: Toward an interdisciplinary framework for research and policy making**. Conselho Europeu. Estrasburgo, p. 1-109. 2017.

WORLD SUMMIT ON INFORMATION SOCIETY. Declaration of Principles, Genebra, p. 1-9, 2003. Disponivel em: <https://www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!PDF-E.pdf>. Acesso em: Agosto 2020.

WORLD SUMMIT ON THE INFORMATION SOCIETY. Plan of Action, 2003. Disponivel em: <https://www.itu.int/net/wsis/docs/geneva/official/poa.html>. Acesso em: Agosto 2020.

WORLD SUMMIT ON THE INFORMATION SOCIETY. Tunis Agenda for the Information Society, 2005. Disponivel em: <https://www.itu.int/net/wsis/docs2/tunis/off/6rev1.pdf>. Acesso em: Agosto 2020.

Anexo único: projetos de lei no Congresso Nacional sobre desinformação

Abordagem Educativa	Abordagem Eleitoral	Abordagem MCI	Abordagem Criminal	Sanção Civil	Outros	Projeto de Lei
				1		3131/2020
			1			2948/2020
			1			2389/2020
			1			1258/2020
			1			1068/2020
			1			1416/2020
		1	1			808/2020
			1			8592/2017
			1			6812/2017
			1			200/2019
			1			3842/2019
			1			5679/2019
	1		1			5003/2019
			1			2917/2019
		1	1			3857/2019
	1		1	1		9973/2018
	1		1			10915/2018
	1		1			10292/2018
	1		1			11004/2018
	1		1			9626/2018
	1		1			9532/2018
			1			9533/2018
			1			9884/2018
			1			241/2019
			1			9554/2018
			1			9838/2018
			1			9761/2018
		1	1			9931/2018
	1		1			4975/2019
		1				2854/2020
					1	3221/2020
					1	7604/2017
		1				283/2020
		1	1			2601/2019
		1	1			9647/2018
		1		1		246/2018
	1					2149/2019
	1		1			5742/2005
		1			1	3389/2019
					1	6337/2019
		1				517/2020
				1	1	3306/2020
			1			3027/2020

				1	1	3307/2020
1						1974/2019
1	1	1	1	1		3144/2020
1						559/2019
1						1563/2019
1						6663/2016
1						7629/2017
1						2801/2015
1						1077/2015
					1	632/2020 (Senado)
					1	3222/2020
						2844/2020
1		1				7689/2017
1		1	1			2927/2020
						2630/2020
				1		1941/2020
				1		2922/2020 (Senado)

Trabalho final do IV Grupo de Pesquisa ITS Rio

Discriminação tecnológica: desmistificando a neutralidade da Inteligência Artificial em meio à crise de inclusão e de diversidade nas tecnologias emergentes

Paula Guedes

Direito

Atualmente, é impensável e talvez até impossível desassociar o ser humano da tecnologia. Quem não gosta do conforto de receber listas com indicações de conteúdo especialmente preparada para si? Ou da facilidade de desbloqueio de *smartphones* com biometria ou reconhecimento facial? Ou até a otimização de tempo com a utilização de ferramentas de busca, assistentes virtuais e dispositivos inteligentes? Certamente, a Inteligência Artificial (AI) está cada vez mais presente em nossas vidas cotidianas, desde as funções mais simples, como recomendações de produtos ou serviços, às complexas, a exemplo de otimização de processos, auxílio na descoberta de novos medicamentos e até em ferramentas antifraude, o que gera diversos benefícios para o ser humano. [1]

Por isso, a percepção da maioria da sociedade é que os sistemas baseados em Inteligência Artificial tendem a ser naturalmente neutros, objetivos e imparciais, a partir da habilidade de tomar decisões, fazer previsões e otimizar processos de forma automatizada, por meio de uma enorme disponibilização de dados, supostamente neutralizando a subjetividade humana e alcançando resultados (*outputs*) cada vez mais justos e imparciais.[2] Porém, na prática, tal presunção não se mostra verídica, uma vez que esses sistemas podem refletir os preconceitos e vieses humanos já existentes na sociedade, de forma a violar direitos humanos variados, especialmente de grupos historicamente marginalizados[3], como negros, mulheres, deficientes, pobres, membros da comunidade LGBT e até alguns grupos étnicos minoritários.

Hoje, não há mais dúvidas de que a IA, como tecnologia emergente, possui enorme capacidade de reproduzir, reforçar e até exacerbar a desigualdade já existente em diferentes contextos, já que a tecnologia é produto da sociedade, de seus valores, prioridades e, inclusive, desigualdades, o que inclui as relacionadas ao racismo, ódio e intolerância. O *design* e o uso dessas ferramentas podem, direta ou indiretamente, de forma intencional ou não, discriminar determinados grupos sociais[4]. Muitas dessas possíveis violações de direitos humanos não são novas, mas exacerbadas pela escala, volume, rápida (e descuidada) proliferação e impactos reais imediatos facilitados pela IA[5]. A marginalização e discriminação de certas camadas da sociedade são, então, refletidas nos dados e reproduzidas nos resultados que consolidam padrões históricos de preconceitos enraizados[6].

Os Estados Unidos são um exemplo atual de como as tecnologias digitais emergentes, como a IA, sustentam e reproduzem estruturas discriminatórias na justiça criminal, desde o policiamento até o processo de tomada de decisão por juízes. Vários estados do país já utilizam ferramentas de avaliação de risco em todas as etapas do processo criminal para, após processamento inicial de dados, gerar uma pontuação para determinado indivíduo e, com isso, rotular o indivíduo em baixo, médio ou alto risco de reincidência em determinado crime. A partir dessa análise, os resultados são utilizados por juízes no processo de tomada de decisão a respeito de concessão

ou não de fiança e liberdade condicional, delimitação de tempo de sentença e até aplicação de medidas de segurança[7].

Em 2016, um estudo da *ProPublica* demonstrou que uma das ferramentas mais utilizadas nos EUA para avaliação de risco de reincidência criminal, conhecida como COMPAS *(Correctional Offender Management Profiling for Alternative Sanctions)*, apresentava viés racial, classificando pessoas brancas como menos arriscadas e negras como mais arriscadas do que de fato eram, além de identificar afrodescendentes como duas vezes mais propícios do que os brancos ao cometimento de crimes violentos.[8] Tal diferenciação ocorre principalmente em razão da utilização de dados históricos de prisões e condenações anteriores, que acabam por perpetuar práticas policiais e judiciais racistas, exacerbando as disparidades raciais enraizadas na sociedade.[9]

Ainda, mesmo que o sistema não utilize a raça como critério de análise, o uso de padrões sociais para avaliação de risco, como educação, emprego e fatores econômicos, também pode culminar em discriminação racial de forma indireta. Em razão da desigualdade socioeconômica sistêmica presente em algumas sociedades, que afeta mais fortemente indivíduos negros, esse grupo tem mais chances também de ser rotulado desfavoravelmente por critérios socioeconômicos.[10] Desta forma, essas ferramentas permitem que pessoas tenham direitos fundamentais negados por escolhas algorítmicas de que não têm acesso e dados históricos que as colocam sistematicamente em posição de desvantagem.[11]

Para além da utilização de Inteligência Artificial na justiça criminal, outros usos do nosso dia a dia já se provaram igualmente enviesados. Após anos de pesquisa sobre a ferramenta de busca do Google, a pesquisadora Safiya Noble constatou que esses sistemas discriminam meninas e mulheres, principalmente negras, que são comercializadas, sexualizadas e discriminadas em suas identidades. Por exemplo, até 2016, o resultado da busca por "meninas negras" *("black girls")* correspondia a sites pornográficos e anúncios de conteúdo sexual, mesmo sem que fossem incluídos quaisquer indicativos relacionados à pornografia ou sexo na pesquisa.[12]

De forma semelhante, na busca por imagens na plataforma do Google, os resultados para as palavras-chave "penteados não profissionais para o trabalho" traziam referências a mulheres com cabelos cacheados ou penteados afro, enquanto os resultados da pesquisa por "mulher" *("woman")* ou "menina" *("girl")* eram representados majoritariamente por mulheres e meninas brancas. Além de questões de gênero, a ferramenta também se mostrou racialmente enviesada: em 2016, um adolescente afro-americano tornou-se viral ao divulgar um vídeo de sua pesquisa no Google Imagens para "três adolescentes negros". Os resultados encontrados eram imagens associadas à criminalidade, o que não acontecia ao alterar as palavras-chaves para "três adolescentes brancos", associados a cenários felizes e saudáveis.[13]

Esses resultados demonstram as visões de mundo hegemônicas e as narrativas dominantes dos desenvolvedores que construíram tais sistemas. De acordo com o último relatório de diversidade publicado pelo Google, 67,5% da empresa é composta por homens e 43,1% de brancos, enquanto o percentual de mulheres e de negros é de, respectivamente 32,5% e 5,5%[14]. Essa sub-representação de mulheres e negros, principalmente nos níveis mais altos de decisão, é característica comum entre as principais empresas de tecnologia da atualidade, a exemplo de Google, Facebook, Microsoft, Apple e Amazon. A mesma crise de diversidade de gênero e raça é encontrada também em cursos universitários associados à tecnologia que não costumam apresentar disciplinas relacionadas à ética e aos direitos humanos.[15]

Como resultado, os valores culturais, econômicos e políticos existentes nas *big techs*, atualmente concentradas no Vale do Silício, nos Estados Unidos, são repassadas para o código e os recortes de dados utilizados[16]. Desta forma, a lacuna de diversidade é um dos grandes motivos da discriminação algorítmica, pois esses sistemas, mesmo de forma não intencional, herdam vieses e preconceitos dos desenvolvedores, que podem reproduzir *bias* enraizados no contexto da sociedade em que estão inseridos, que tendem a ser ambientes extremamente brancos, masculinos e ricos, com histórico de problemas de discriminação, exclusão e assédio sexual.[17]

Outro exemplo de tecnologia emergente com base em IA e tendência discriminatória é o reconhecimento facial. Um estudo de 2019 do *National Institute of Standards and Technology* (NIST)[18], que avaliou 189 algoritmos de reconhecimento facial pertencentes a 99 desenvolvedores ao redor do mundo, constatou que a maioria tinha de 10 a 100 vezes mais chances de identificar imprecisamente o rosto negro ou asiático em comparação com o branco, o que é agravado quando a análise é feita em mulheres.[19] No mesmo sentido, pesquisa feita pelo *Institute of Electrical and Electronics Engineers* (IEEE) concluiu que, em diferentes grupos demográficos, a ferramenta apresenta menor acurácia em pessoas do sexo feminino, negros e jovens entre 18 a 30 anos.[20] Especificamente em relação aos *softwares* de reconhecimento facial da Microsoft e IBM, análise da pesquisadora Joy Buolamwini do MIT confirmou o melhor desempenho em homens brancos (94-88% de acurácia) e pior em mulheres negras (79,2-65,3% de acurácia).[21]

Além do constrangimento enfrentado pelos indivíduos equivocadamente não reconhecidos (falsos negativos) ou reconhecidos (falso positivo) pelas ferramentas, que comprovadamente discriminam em razão de gênero e raça, as consequências práticas da falta de acurácia podem violar também outros direitos humanos além da não-discriminação. É o caso de Robert-Julian-Borchak Williams, cidadão negro norte-americano, que foi preso após sua identificação como autor do crime de furto

pelo *software* de reconhecimento facial utilizado pela polícia estadual de Michigan. O incidente foi considerado o primeiro caso conhecido de falha no reconhecimento facial que levou à prisão de indivíduo por crime que não cometeu.[22]

Além da utilização prematura das ferramentas de reconhecimento facial, postas à disposição do público antes de serem realizados todas as testagens necessárias para a garantia de segurança e precisão[23], um dos principais motivos da falta de acurácia desses *softwares* está na insuficiência de dados de entrada para os grupos discriminados, o que está em desacordo com a diversidade existente na sociedade. Em outras palavras, há uma enorme disponibilidade de dados para um determinado grupo e falta de dados para outros, especialmente aqueles já marginalizados na sociedade. Considerando que a atividade de seleção de dados para alimentação dos sistemas de Inteligência Artificial, por si só, é uma atividade subjetiva, não há dúvidas de que, apesar da neutralidade alegada por parte da sociedade, essas tecnologias não são neutras e destituídas de valores, podendo reproduzir, perpetuar e agravar padrões discriminatórios existentes.[24]

Desta forma, embora haja enorme necessidade de escrutínio e responsabilização pela qualidade técnica e precisão das ferramentas que utilizam Inteligência Artificial, o cumprimento dos princípios da igualdade e não discriminação, além de outros direitos humanos, deve iniciar com o reconhecimento de que o problema não é meramente técnico ou matemático, mas principalmente uma questão social, política e econômica. A perpetuação de vieses nos sistemas de IA não será curada apenas por modelagens tecnológicas perfeitas, mas com a união de agentes e áreas distintas da sociedade, o que inclui, além dos especialistas em tecnologia, o setor público, empresas privadas, sociedade civil e a academia,[25] em aplicação de soluções técnicas, éticas e voltadas para os direitos humanos.

Em regra, as ferramentas de Inteligência Artificial são desenvolvidas com base em métricas de desempenho, como acurácia, velocidade e eficiência, sem levar em consideração a existência de vieses. Por isso, é fundamental a criação de times heterogêneos e multidisciplinares para conduzir as pesquisas e projetos de IA, de forma a incluir também métricas baseadas em direitos humanos e ética.[26] No mesmo sentido, considerando a crise de diversidade do setor tecnológico, é extremamente necessário o recrutamento de maior pluralidade e diversidade para os cargos de cientistas de dados e demais profissionais relacionados à IA, principalmente de indivíduos de grupos sub-representados, para garantia de convivência de visões de mundo diversas e prevalência do respeito e não discriminação.[27]

Ainda, quando nos referimos à inclusão, é necessário que medidas sejam tomadas não apenas para inserção na sociedade de minorias por categorias isoladas, uma vez que as formas de opressão se cruzam e os esforços de diversidade que visam, por exemplo, mulheres, sem reconhecer o papel da raça e outras formas de identidade,

privilegiam implicitamente as mulheres brancas.[28] Diante dessa premissa, torna-se essencial a aplicação de políticas público-privadas de educação, inclusão interseccional e empoderamento tecnológico para capacitar os indivíduos em geral, mas principalmente os grupos minoritários, a entender melhor a IA, abrindo portas para que ascendam a cursos relacionados (e se mantenham neles) e tenham melhores condições de acesso ao mercado de trabalho.

Portanto, a diversidade e a inclusão desempenham papel fundamental no desenvolvimento dos sistemas de Inteligência Artificial no mundo real. A maioria dos desenvolvedores, na maior parte do tempo, não se considera sexista, racista, homofóbico, xenófobo ou opressor, mas está propenso a excluir ou discriminar grupos marginalizados de forma sistemática pelos sistemas de IA.[29] Por isso, as equipes que concebem, desenvolvem, testam, mantém, implantam e compram a tecnologia devem ser diversificadas, não só em termos de gênero, cultura e idade, mas também no que tange a experiências profissionais e competências no geral, de forma a possibilitar uma reflexão sobre as necessidades múltiplas e diversas dos utilizadores e da sociedade em geral, além do respeito igualitário aos direitos humanos. A Inteligência Artificial deve trabalhar em benefício do ser humano, considerado todas as suas diversidades, e não contra ele.

Notas

1. CORTIZ, Diogo. Inteligência Artificial: equidade, justiça e consequências. Panorama Setorial da Internet: Nº 1, Ano 12, Maio de 2020, pp. 1-5. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/20200626161010/panorama_setorial_ano-xii_n_1_inteligencia_artificial_equidade_justi%C3%A7a.pdf. p. 1.

2. BRAGA, Carolina Henrique da Costa. Decisões Automatizadas e Discriminação: Pesquisa de Propostas Éticas e Regulatórias no Policiamento Preditivo. Dissertação de Mestrado do programa de Pós-Graduação em Princípios Fundamentais e Novos Direitos da Universidade Estácio de Sá (UNESA). Orientação do professor Nilton César da Silva Flores. Rio de Janeiro, 2019. p. 10-11; Human Rights Council. Racial discrimination and emerging digital technologies: a human rights analysis. Report of the Special Rapporteur n contemporary forms of racism, racial discrimination, xenophobia, and related intolerance (Advance Edited Version), 18 jun. 2020, A/HRC/44/57. Disponível em: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Pages/ListReports.aspx. p. 4.

3. BRAGA, Carolina Henrique da Costa. Decisões Automatizadas e Discriminação: Pesquisa de Propostas Éticas e Regulatórias no Policiamento Preditivo. Dissertação de Mestrado do programa de Pós-Graduação em Princípios Fundamentais e Novos Direitos da Universidade Estácio de Sá (UNESA). Orientação do professor Nilton César da Silva Flores. Rio de Janeiro, 2019. p. 10-11.

4. Human Rights Council. Racial discrimination and emerging digital technologies: a human rights analysis. Report of the Special Rapporteur n contemporary forms of racism, racial discrimination, xenophobia, and related intolerance (Advance Edited Version), 18 jun. 2020, A/HRC/44/57. Disponível em: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Pages/ListReports.aspx. p. 4.

5. ANDERSEN, Lindsey. Human Rights in the Age of Artificial Intelligence. Access Now. Nov. 2018. Disponível em: https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf. p. 08.

6. Ibid. p. 18.

7. YAVUZ, Can. Machine Bias: Artificial Intelligence and Discrimination. Faculty of Law, Lund University, Spring term 2019. JAMM07 Master Thesis – International Human Rights Law. Supervisor: Karol Nowak. p. 58 e 59.

8. ANGWIN, Julia; KIRCHNER, Lauren; LARSON, Jeff; MATTU, Surya. Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks. ProPublica, 23 mar. 2016. Disponível em: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing. Acesso em 22 jul. 2020.

9. YAVUZ, Can. Machine Bias: Artificial Intelligence and Discrimination. Faculty of Law, Lund University, Spring term 2019. JAMM07 Master Thesis – International Human Rights Law. Supervisor: Karol Nowak. p. 60.

American Civil Liberties Union (ACLU). *A Tele of Two Countries: Racially Targed Arrests in the Era of Marijuana Reform*. ACLU Research Report, 2020. Disponível em: https://www.aclu.org/sites/default/files/field_document/042020-marijuana-report.pdf.

10. YAVUZ, *Can. Machine Bias: Artificial Intelligence and Discrimination*. Faculty of Law, Lund University, Spring term 2019. JAMM07 Master Thesis – International Human Rights Law. Supervisor: Karol Nowak. p. 61.

11. BRAGA, Carolina Henrique da Costa. *Decisões Automatizadas e Discriminação: Pesquisa de Propostas Éticas e Regulatórias no Policiamento Preditivo*. Dissertação de Mestrado do programa de Pós-Graduação em Princípios Fundamentais e Novos Direitos da Universidade Estácio de Sá (UNESA). Orientação do professor Nilton César da Silva Flores. Rio de Janeiro, 2019. p. 56.

12. À título de exemplo, os resultados da pesquisa levavam à sites que incluíam palavras como "sexo" ("sex"), "estrela pornô" ("porn star"), "quente" ("hot"), "hardcore", "bunda" ("ass") e "adolescentes" ("teenagers"); NOBLE, Safiya. Google Has a Striking History of Bias Against Black Girls. Time, 26 mar. 2018. Disponível em: https://time.com/5209144/google-search-engine-algorithm-bias-racism/. Acesso em 22 jul. 2020.

13. NOBLE, Safiya. Google Has a Striking History of Bias Against Black Girls. Time, 26 mar. 2018. Disponível em: https://time.com/5209144/google--search-engine-algorithm-bias-racism/. Acesso em 22 jul. 2020.

14. Google. Google Diversity Annual Report 2020. Disponível em: https://diversity.google/.

15. NOBLE, Safiya. Google Has a Striking History of Bias Against Black Girls. Time, 26 mar. 2018. Disponível em: https://time.com/5209144/google--search-engine-algorithm-bias-racism/. Acesso em 20 mai. 2020.

16. Human Rights Council. Racial discrimination and emerging digital technologies: a human rights analysis. Report of the Special Rapporteur n contemporary forms of racism, racial discrimination, xenophobia, and related intolerance (Advance Edited Version), 18 jun. 2020, A/HRC/44/57. Disponível em: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Pages/ListReports.aspx. p. 4.

17, CRAWFORD, Kate. Artificial Intelligence's White Guy Problem. The New York Times, 25 jun. 2016. Disponível em: https://www.nytimes.com/2016/06/26/opinion/sunday/artificial-intelligences-white-guy-problem.html. Acesso em 27 mai. 2020.

18. GROTHER, Patrick; NGAN, Mei; HANAOKA, Kayee. Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects. National Institute of Standards and Technology (NIST), NISTIR 8280, dez. 2019. Disponível em: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf.

19. BUSHWICK, Sophie. How NIST Tested Facial Recognition Algorithms for Racial Bias. Scientific American, dez. 2019. Disponível em: https://www.scientificamerican.com/article/how-nist-tested--facial-recognition-algorithms-for-racial-bias/. Acesso em 31 jul. 2020.

20. BRUEGGE, Richard W. Vorder; BURGE, Mark J; JJAIN, Anil K; KLARE, Brendan F.; KLONTZ, Joshua C. Face Recognition Performance: Role of Demographic Information. IEEE Transactions on Information Forensics and Security. Disponível em: https://www.openbiometrics.org/publications/klare2012demographics.pdf.

21. BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. Proceedings of Machine Learning Research 81:1–15, 2018 Conference on Fairness, Accountability, and Transparency. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

22. The New York Times. Wrongfully Accused by an Algorithm. 24 jun. 2020. Disponível em: https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html. Acesso em 16 jul. 2020; American Civil Liberties Union (ACLU). Wrongfully Arrested Because Face Recognition Can't Tell Black People Apart. 24 jun. 2020. Disponível em: https://www.aclu.org/news/privacy-technology/wrongfully-arrested-because--face-recognition-cant-tell-black-people-apart. Acesso em 16 jul. 2020.

23. YAVUZ, Can. Machine Bias: Artificial Intelligence and Discrimination. Faculty of Law, Lund University, Spring term 2019. JAMM07 Master Thesis – International Human Rights Law. Supervisor: Karol Nowak. p. 48.

24. BRAGA, Carolina Henrique da Costa. Decisões Automatizadas e Discriminação: Pesquisa de Propostas Éticas e Regulatórias no Policiamento Preditivo. Dissertação de Mestrado do programa de Pós-Graduação em Princípios Fundamentais e Novos Direitos da Universidade Estácio de Sá (UNESA). Orientação do professor Nilton César da Silva Flores. Rio de Janeiro, 2019. p. 53.

25. Human Rights Council. Racial discrimination and emerging digital technologies: a human rights analysis. Report of the Special Rapporteur n contemporary forms of racism, racial discrimination, xenophobia, and related intolerance (Advance Edited Version), 18 jun. 2020, A/HRC/44/57. Disponível em: https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session44/Pages/ListReports.aspx. p. 5.

26. CORTIZ, Diogo. Inteligência Artificial: equidade, justiça e consequências. Panorama Setorial da Internet: Nº 1, Ano 12, Maio de 2020, pp. 1-5. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/20200626161010/panorama_setorial_ano-xii_n_1_inteligencia_artificial_equidade_justi%C3%A7a.pdf. p. 3.

27. CRAWFORD, Kate; WEST, Sarah Myers; WHIIAKER, Meredith. Discriminating Systems: Gender, Race, and Power in AI. AI Now Institute, April 2019. Disponível em: https://ainowinstitute.org/discriminatingsystems.html. p. 17.

28. JOY, Erica. #FFFFFF Diversity. 7 out. 2015. Disponível em: https://medium.com/this-is-hard/ffffff-diversity-1bd2b3421e8a.

29. COSTANZA-CHOCK, Sasha. Design Justice: Community-Led Practices to Build the Worlds We Need. The MIT Press, 3 mar. 2020, 360 p. Design Values: Hard-Coding Liberation? p. 9.

30. Grupo Independente de Peritos de Alto Nível sobre Inteligência Artificial da Comissão Europeia (High-Level Expert Group on Artificial Intelligence – European Commission). Orientações Éticas para uma IA de Confiança (Guidelines on Trustworthy AI). Abril de 2019. Disponível em: https://ec.europa.eu/futurium/en/ai-alliance-consultation/guidelines#Top. p. 29.

Trabalho final do IV Grupo de Pesquisa ITS Rio

Tratamento de dados de adolescentes no Brasil e a necessária proteção de direitos por *design*

Elora Raad Fernandes

Direito

Introdução

O contexto hiperconectividade atual, no qual um número crescente de indivíduos e objetos vêm sendo continuamente conectados por meio de tecnologias digitais em rede, tem favorecido a chamada datificação da infância. Crianças e adolescentes passam a ser vistos não como pessoas, mas como um conjunto de dados, que pode ser explorado.

Os "nativos digitais", ao contrário das gerações anteriores, têm seus dados tratados desde a concepção, por meio de exames de ultrassom digital, babás eletrônicas, objetos e brinquedos conectados, o que pode significar modificações profundas na vida dessas pessoas no futuro. A datificação possibilita desde a propaganda direcionada e a recusa a uma vaga de trabalho até a manipulação de sistemas políticos e a vigilância por parte de governos e empresas.

Diante desse contexto, a Lei Geral de Proteção de Dados Pessoais (LGPD — Lei 13.709/2020) dedicou às crianças e aos adolescentes um artigo próprio. O art. 14, da LGPD, determina que seus dados devem ser tratados segundo seu melhor interesse e que o consentimento em relação ao tratamento desses dados poderá ser realizado, sem representação ou assistência dos pais, pelos maiores de 12 anos.

Todavia, deve-se ter em mente que o comportamento humano, principalmente no ambiente digital, é balizado não somente pelo direito, mas também por estruturas sociais, tecnológicas e mercadológicas[1]. Nesse sentido, será que as estruturas nas quais os adolescentes estão imersos favorecem esse consentimento?

Interessante é a teoria de Livingstone, Stoilova e Nandagiri, que busca analisar a temática a partir da "natureza das relações e dos contextos, nos quais crianças agem em ambientes digitais e em como eles entendem as implicações para a sua privacidade[2]". Assim, as autoras distinguem os três principais tipos de relações, nas quais a privacidade é importante para as pessoas.

Primeiramente, elas descrevem a privacidade interpessoal, dimensão que está diretamente relacionada à identidade de cada indivíduo, a como ele se vê e a como ele é visto pela sociedade. Importa destacar, nesse sentido, que adolescentes buscam privacidade, de maneira geral, em relação àqueles que têm poder imediato sobre eles[3]. Assim, a vigilância por parte de governos e empresas não é o seu foco de preocupação, mas, sim aquela por parte de seus pais, professores ou outras autoridades presentes em suas vidas.

Em segundo lugar, a privacidade institucional está ligada às relações entre o adolescente e outras organizações públicas ou do terceiro setor. Essa discussão já se torna mais complexa, já que o tratamento de dados por essas entidades é frequentemente visto como legítimo, muitas vezes devido ao potencial interesse público que o subjaz. Apesar disso, os governos são atores importantes na criação do rastro digital, o que tem sido bastante discutido no cenário atual de uso de tecnologias para combater a Covid-19.[4]

Por fim, há também a privacidade comercial, que está diretamente relacionada ao tratamento dos dados por empresas, com o objetivo principal de traçar perfis para a publicidade direcionada. As táticas de *marketing* utilizadas na Internet, muitas vezes baseadas em localização, *cookies* e comportamento *online* têm ocorrido indiscriminadamente, mesmo no Brasil, em que a publicidade direcionada a crianças é considerada abusiva.

As dimensões apresentadas pelas autoras são bastante interessantes, não para subsidiar a defesa de uma tutela diferenciada dos dados tratados por cada um desses atores, mas para compreender a visão dos adolescentes, no que se refere à sua privacidade e à proteção de seus dados na Internet. Esse entendimento, a partir da ótica dessas pessoas é essencial, principalmente em relação aos adolescentes, que poderão consentir para o tratamento de seus dados sem a ajuda dos responsáveis.

O contexto brasileiro

A partir das diferentes dimensões apresentadas acima, percebe-se que a temática não dá azo a soluções simplistas e isso é ainda intensificado quando se leva em consideração o contexto brasileiro. A pesquisa Tic Kids Online, realizada pelo Núcleo de Informação e Comunicação do Ponto BR (NIC.br), traz informações valiosas nesse sentido. Segundo a publicação,

> *classes mais altas possuíam melhores condições de acesso à rede, a utilizavam com mais frequência, por meio de uma pluralidade maior de dispositivos e em uma maior variedade de locais. Além disso, sob a perspectiva geográfica, é possível observar que crianças e adolescentes de diferentes regiões não têm o mesmo acesso ao ambiente online*[5].

A existência de desigualdades socioeconômicas entre os adolescentes brasileiros reflete diretamente nas oportunidades que as Tecnologias da Informação e Comunicação (TIC) podem proporcionar. Destaca-se, por exemplo, que o uso da Internet para consumo de notícias é expressivamente menor em áreas rurais (24%) em relação a áreas urbanas (38%). Da mesma forma, adolescentes de áreas urbanas utilizaram mais a Internet para conversar sobre política ou problemas de sua cidade ou país (22%) do que usuários de áreas rurais (12%). Essa distorção também pode ser observada na comparação entre as classes AB (31%), C (18%) e DE (17%)[6].

Os dados apresentados pela pesquisa também revelam que muito foco tem sido dado ao desenvolvimento de habilidades para que crianças e adolescentes lidem com a privacidade interpessoal[7], mas pouca atenção têm sido dispensada as outras dimensões. Isso pode ocorrer tanto em razão da falta de conhecimento acerca do tratamento de dados por esses atores, pela dificuldade de controle dos dados nessas esferas atualmente[8].

Proteção de dados de adolescentes por *design*: o caso do Reino Unido

A situação apresentada demonstra que o Brasil possui discrepâncias consideráveis no que diz respeito a habilidades e uso da Internet, tanto em relação a classes sociais quanto a questões territoriais. O acesso à rede com qualidade, porém, é fundamental para o desenvolvimento de uma educação digital de qualidade. Da mesma forma, se o adolescente possui apenas habilidades para lidar com a privacidade interpessoal, faltam-lhe informações necessárias para compreender o processo que está por trás do tratamento de dados por parte de instituições e empresas[9].

Assim, quando se trata de proteger os dados de adolescentes na Internet, não basta considerar apenas a idade de consentimento para o tratamento de dados. Isso, pois a capacidade de tomada de decisões não é algo desenvolvido individualmente. Assume-se aqui que a capacidade é um conceito relacional, moldado pelas interações sociais. Por essa perspectiva, os adultos (não só os pais ou responsáveis, mas a sociedade e também o Estado) devem assumir sua instância de responsabilidade nesse processo, devendo criar um ambiente adequado e prover assistência no desenvolvimento e exercício dessa capacidade[10].

A fim de criar esse ambiente adequado e concretizar o melhor interesse, o Reino Unido, de maneira pioneira, em sua lei geral de proteção de dados (*Data Protection Act*), criou a necessidade específica de se respeitar os direitos de crianças e adolescentes por *design*.

Apesar de determinar que adolescentes, a partir dos 13 anos, podem consentir para o tratamento de seus dados, a lei estabeleceu que o *Information Commissioner's Office* (ICO), sua autoridade de proteção de dados, criaria um código de práticas que contivesse orientações sobre padrões de *design* adequados à idade em relação a qualquer serviço que possa ser acessado por menores. Destaca-se, então, que ele é direcionado não somente àqueles serviços desenvolvidos especificamente para eles, de maneira que o fato de o serviço não ser voltado a esse grupo não pode ser desculpa para descumprir o seu melhor interesse.

Esse código, lançado em janeiro de 2020, dita 15 padrões de *design* que fornecem proteção integrada, sendo eles cumulativos e interligados. As configurações dos serviços *online* devem ter "alta privacidade" por padrão, de forma que

> *somente a quantidade mínima de dados pessoais deve ser coletada e retida; os dados das crianças de maneira geral não devem ser compartilhados; serviços de geolocalização devem estar desativados por padrão. Técnicas de nudge não devem ser usadas para incentivar as crianças a fornecer dados pessoais*

> *desnecessários, enfraquecer ou desativar suas configurações de privacidade. O código também aborda questões de controle pelos pais e profiling*[11].

Essa dupla regulação, por meio da idade para consentimento e da definição de uma alta privacidade por padrão é extremamente importante. A discussão acerca do aumento da idade de consentimento, com o objetivo de proteger melhor os menores, ignora a necessidade de um espaço de privacidade interpessoal, principalmente em relação a seus pais ou responsáveis. Da mesma forma, não resolve o problema do desenvolvimento de habilidades digitais por parte do adolescente, uma vez que cada indivíduo possui um processo único de amadurecimento. E, por fim, também não abarca as situações em que o consentimento não é utilizado como base legal para tratar os dados de adolescentes.

Em síntese, ao se adotar padrões de *design* para proteger os dados, utilizando-se da tecnologia para regular comportamentos humanos, os adolescentes poderão experimentar consentir e aprender por meio de erros e acertos, sem que isso gere problemas em relação a formação de suas personalidades ou os prejudique no futuro. Da mesma forma, garante-se que o tratamento de dados através de outras bases legais esteja também adequado ao melhor interesse. No caso do Brasil, isso é ainda mais necessário, uma vez que suas complexidades socioeconômicas fazem com que diferentes realidades coexistam em um mesmo território.

Nesse sentido, a fim de fazer valer o princípio do melhor interesse, presente no *caput* do art. 14, da LGPD, bem como todo o arcabouço normativo de proteção às crianças e aos adolescentes no país, é essencial que Autoridade Nacional de Proteção de Dados brasileira (ANPD), ainda a ser criada, adote um código semelhante. Esse direcionamento para a incorporação de padrões de privacidade específicos para os menores nas tecnologias, além de trazer maior segurança jurídica para os provedores de aplicações, possibilitará que a datificação da infância seja mitigada no Brasil.

Notas

1. LESSIG, Lawrence. Code: version 2.0. Nova York: Basic Books, 2006.

2. LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. Children's data and privacy online: Growing up in a digital age. An evidence review. London: London School Of Economics And Political Science, 2019, p. 13, tradução nossa.

3. BOYD, Danah. It's complicated: the social lives of networked teens. New Haven: Yale University Press, 2014.

4. Cf. FERNANDES, Elora Raad; CANTANHEDE, Cindyneia Ramos. Proteção de crianças e adolescentes por design: um debate necessário em meio à pandemia de covid-19. In: BIONI, Bruno R.; ZANATTA, Rafael A. F.; RIELLI, Mariana; VERGILI, Gabriela; FAVARO, Iasmine. Os dados e o vírus: pandemia, proteção de dados e democracia. pandemia, proteção de dados e democracia. São Paulo: Data Privacy Brasil, 2020. p. 73-81. Disponível em: <https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F108127%2F1595880339E-BOOK_OS_DADOS_E_O_VRUS_PANDEMIA_PROTEO_DE_DADOS_E_DEMOCRACIA_-_CAPA_ESPECIAL.pdf>. Acesso em: 01 ago. 2020.

5. NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. TIC Kids Online Brasil 2018: pesquisa sobre o uso da Internet por crianças e adolescentes no Brasil. São Paulo: Comitê Gestor da Internet no Brasil (CGI.BR), 2019. Disponível em: <https://www.cetic.br/media/docs/publicacoes/216370220191105/tic_kids_online_2018_livro_eletronico.pdf>. Acesso em: 14 mai. 2020.

6. NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. TIC Kids Online Brasil 2018, cit.

7. Nesse sentido, destaca-se que 69% dos usuários entrevistados afirma saber como verificar se uma informação encontrada online está correta; 88% considera saber definir o que deve ou não ser compartilhado na Internet; 73% afirma saber muitas coisas sobre como usar a Internet e o mesmo número sustenta saber mais sobre a Internet que seus pais. Por fim, 63% afirma saber como modificar as configurações de privacidade em redes sociais (NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. TIC Kids Online Brasil 2018, cit.).

8. No que diz respeito à privacidade comercial, destaca-se que 52% dos usuários entrevistados reportou ter tido contato com publicidade em redes sociais. Apesar de eles considerarem a publicidade na Internet irritante (68%) ou chata (76%), o efeito que ela gera não pode passar despercebido: 80% dos usuários reportou ficar com vontade de ter o produto depois de assistir à publicidade e 71% enunciou que pessoas da sua idade ficam chateadas por não poderem comprar o produto (NIC.BR - NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. TIC Kids Online Brasil 2018, cit.). Já em relação à privacidade institucional, pode-se dizer que não há ainda dados suficientes sobre o tratamento de dados de crianças e adolecentes nesse âmbito no Brasil.

9. Livingstone, Stoilova e Nandagiri demonstram como esses adolescentes, ao serem apresentados às práticas de profiling e targeting, não compreendem por que seus dados estão sendo utilizados com essas finalidades e, por isso, essa não é uma preocupação genuína por parte dessas pessoas (LIVINGSTONE, Sonia; STOILOVA, Mariya; NANDAGIRI, Rishita. Children's data and privacy online, cit.).

10. RUHE, Katharina M.; CLERCQ, Eva de; WANGMO, Tenzin; ELGER, Bernice S.. Relational Capacity: broadening the notion of decision-making capacity in paediatric healthcare. Journal Of Bioethical Inquiry, [s.l.], v. 13, n. 4, p. 515-524, 30 jun. 2016. Springer Science and Business Media LLC. http://dx.doi.org/10.1007/s11673-016-9735-z.

11. REINO UNIDO. INFORMATION COMMISSIONER'S OFFICE. Age appropriate design: [s.l.], 2020. Disponível em: https://ico.org.uk/for-organisations/guide-to-data-protection/key-data-protection-themes/age-appropriate-design-a-code-of-practice-for-online-services/. Acesso em: 24 abr. 2020, p. 4, tradução nossa.

Trabalho final do IV Grupo de Pesquisa ITS Rio

Responsabilidade civil dos provedores de aplicações de internet e os direitos dos usuários: o que deve prevalecer?

Juliana Medeiros

Direito

Responder a essa pergunta não é uma tarefa fácil e em uma simples reflexão sobre o funcionamento das plataformas digitais, mídias sociais e relações entre usuários, conseguimos perceber que escolher apenas um lado parece uma análise muito simples para um tema um tanto complexo.

Fato é que após a entrada em vigor do Marco Civil da Internet – MCI (lei 12.965/14) parecia que nunca mais precisaríamos voltar a discutir a responsabilidade civil dos provedores de aplicação de internet por conteúdos postados por terceiros em suas plataformas online. Isso porque, o artigo 19 do MCI trouxe em sua redação o momento em que o provedor de aplicações de internet poderia ser responsabilizado civilmente:

> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet **somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências** para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

É, portanto, após a ordem judicial específica descumprida pelo provedor de aplicações de internet, que este se veria responsável civilmente a indenizar por danos morais o usuário que teve seu direito violado por terceiro na plataforma.

Contudo, o tema da responsabilidade civil do provedor de aplicação retomou à pauta de discussão após o *Leading Case* RE 1.037.396/SP chegar ao Supremo Tribunal Federal - STF em sede de repercussão geral, questionando a constitucionalidade do artigo 19 do MCI.

Assim, o artigo 19 que antes trazia uma redação clara a respeito da responsabilidade civil dos provedores de aplicações de internet, hoje retoma a um lugar de incerteza e insegurança sobre seu futuro.

Todavia, cabe destacar que a hipótese de responsabilidade civil trazida pelo artigo 19 do MCI não priva o provedor de aplicação - por seu livre convencimento - de remover o conteúdo violador quando notificado extrajudicialmente pelo usuário.

> O provedor de aplicações, como uma rede social ou um provedor de hospedagem, pode então decidir remover um conteúdo caso ele ofenda os termos de uso que regem a sua atuação. Nesse sentido, a notificação privada ou a denúncia de conteúdos potencialmente abusivos ou ilícitos serve de sinalização para o provedor, embora não seja ele, em regra, obrigado a remover apenas pelo recebimento dessas notificações extrajudiciais.

> Esse é o entendimento que decorre do Marco Civil da Internet em seu artigo 19 e atende mais uma vez a posição de destaque que a liberdade de expressão ocupa no ordenamento jurídico. Se a notificação privada tivesse o condão de obrigar um provedor a remover qualquer conteúdo que fosse indicado, não restariam críticas a qualquer produto na Internet brasileira.[1]

Nesse sentido, entende-se que "o provedor de aplicações de internet teria a possibilidade e o dever de contribuir com os usuários da rede, evitando danos, auxiliando na identificação de ofensores e retirando de seus domínios conteúdos lesivos à dignidade da pessoa humana"[2].

É exatamente em virtude desse entendimento sobre o dever de cuidado que deveria ser imputada ao provedor de aplicações por aquilo que é postado na rede, que hoje se discute a constitucionalidade do artigo 19 no STF.

No entanto, não se pode olvidar que o princípio basilar do Marco Civil da Internet (MCI) é a liberdade de expressão e qualquer atribuição de responsabilidade civil aos provedores de aplicações de internet diversa da hoje prevista no texto legal - como a responsabilidade objetiva ou a subjetiva após mera notificação extrajudicial -, poderia comprometer a magnitude desse princípio, além de comprometer o livre discurso na rede e proporcionar a censura, o que não parece ser a solução.

Assim, ainda que se concorde com o necessário dever de cuidado a ser atribuído às plataformas, é preciso estar atento aos perigos de se definir uma responsabilidade civil prévia à ordem judicial aos provedores de aplicações, pois atribuindo a estes o dever de fiscalizar, remover e retirar conteúdos sem a prévia análise legal, é que o mesmo se torne promotor de um discurso viciado no ambiente digital.

Por isso, dar conta dessas peculiaridades não é uma tarefa fácil e embora o jogo de "tudo ou nada" em tentar se definir a responsabilidade do provedor de aplicações de internet, o assunto deveria ser tratado com mais cautela e compreensão, a fim de que se compreenda que as regras do jogo devem mudar.

A opção pela declaração da inconstitucionalidade do artigo 19 do MCI não parece solucionar o problema de proteção dos direitos dos usuários, e por si só, traria mais problemas do que soluções, como o vácuo legislativo, limites à liberdade de expressão e a limitação do discurso na rede.

O cenário é, portanto, aquele em que entendemos que a declaração da inconstitucionalidade do artigo 19 do MCI, assim como a sua manutenção sem quaisquer outras medidas, não é a solução e por essa razão, há a necessidade de se encontrar um ponto de interseção comum entre os dois caminhos, de modo a proteger o discurso da rede, ao mesmo tempo em que se impõe aos provedores de aplicação de internet o dever de ser agente atuante na promoção de direitos e prevenção de atos ilícitos na sua plataforma digital.

É nesse ensejo que se compreende que uma vez que se muda o foco para políticas que visam uma mudança de comportamento, estabelecendo, por exemplo, obrigações de infraestrutura para as plataformas digitais, estar-se-ia mudando também o resultado, isto é, como o conteúdo estará sendo compartilhado.

O foco deve ser então nos comportamentos, a fim de que se estabeleçam medidas do que é ou não aceitável no ambiente digital - por exemplo, compartilhamento de mensagens em massa, perfis falsos, automatização de contas - e não no conteúdo, pois se assim fosse, poderia se gerar uma análise subjetiva de remoção sobre o que é um conteúdo aceito pelas políticas e os termos de uso da plataforma ou o que não é.

O cenário brasileiro ainda anda a passos pequenos no entendimento de que políticas de transparências e segurança poderiam alterar o resultado de como o conteúdo é compartilhado, mas após a pandemia provocada pelo novo coronavírus (COVID-19), as principais plataformas digitais uniram forças para intensificar comportamentos preventivos de disseminação de notícias falsas envolvendo desinformação a respeito do vírus.

> Essas iniciativas parecem seguir o "caminho do meio", privilegiando tanto a liberdade de expressão, quanto o interesse público em se manter um ambiente informacional saudável nas redes. De quebra, investem em um terceiro direito: a educação digital dos envolvidos na cadeia de compartilhamento de informação, desde o autor até os usuários que compartilham e disseminam a informação e todos os que consumiram este conteúdo. E evitam os riscos de censura, inevitavelmente presentes quando se opta pela remoção do conteúdo[3].

Foi num momento de extrema necessidade como o da pandemia da Covid-19 que plataformas como Twitter[4], Instagram[5] e Facebook[6] passaram a adotar comportamentos que visavam um maior combate aos conteúdos geradores pela desinformação. É nessa conjuntura que colocar a discussão sobre infraestrutura das plataformas em pauta parece um caminho bom, viável e adequado.

Uma iniciativa paradigmática neste sentido está sendo implementada pela União Europeia – UE, ao instituírem um código de conduta para combate à desinformação, o "Code of Practice on Disinformation".[7]

A Comissão da UE estabeleceu juntamente a plataformas como Facebook, Google e Twitter, diversos compromissos, dentre eles, o desenvolvimento de ferramentas de alfabetização digital e empoderamento do cidadão e, apesar do Código de Conduta voltar-se para medidas que visem impedir a desinformação, as propostas de deveres são amplamente possíveis de serem aplicadas de maneira mais abrangente para também servir de norte às medidas ao combate de violação de direitos no ambiente digital.

Perpassando por medidas, como investimento em produtos e tecnologias de apoio a decisões informadas e implementação de indicadores eficazes de confiabilidade, o que se deve aproveitar como objeto a ser aplicado no cenário de proteção dos direitos dos usuários a conteúdos violadores na internet é a imperiosa necessidade das plataformas se comprometerem com obrigações de infraestrutura.

Além disso, uma das mais palpáveis iniciativas que se depreende com esses objetivos também são os Princípios de Santa Clara. Tais princípios, definidos em ocasião de uma conferência de Moderação de Conteúdo na Scale, em Santa Clara, Califórnia, em 2 de fevereiro de 2018, advogados e especialistas acadêmicos que apoiam o direito à liberdade de expressão online discutiram métodos para considerar a melhor forma de obter transparência e responsabilidade significativas em torno da moderação cada vez mais agressiva das plataformas da internet de conteúdo gerado por usuários.[8]

Na perspectiva brasileira, a adoção dos princípios de Santa Clara serviriam como ponto de partida, descrevendo níveis mínimos de transparência e responsabilidade que esperamos que possam servir de base para um diálogo mais aprofundado no futuro.[9]

A fim de garantir maior transparência e prestação de contas na atividade moderação de conteúdos produzidos pelos internautas por parte dos provedores de aplicação os princípios de Santa Clara são divididos em três, sendo eles: números, notificações e recursos:

> **Números:** As empresas devem publicar o número de postagens removidas e contas permanentemente ou temporariamente suspensas devido a violações de suas diretrizes de conteúdo;
>
> **Notificações:** As empresas devem fornecer um aviso a cada usuário cujo conteúdo seja retirado ou a conta seja suspensa sobre o motivo da remoção ou suspensão.
>
> **Recursos:** As empresas devem possibilitar que os usuários recorram de todas as decisões de remoção de conteúdo ou suspensão de contas.

Percebe-se que a transparência na execução das diretrizes de conteúdo é essencial para que se dê o mínimo de credibilidade ao discurso de defesa intransigente da liberdade de expressão, que vem sendo empregado pelos provedores de aplicação, como a exemplo a ação que discute a constitucionalidade do artigo 19 do MCI.[10]

Outra política digna de destaque nesse sentido é a que vem aplicando a UNESCO, no que tange a educação digital[11], apresentando alfabetização midiática também como uma alternativa eficiente. O conceito de alfabetização midiática e informacional (AMI)

cunhado pela UNESCO, visa desenvolver habilidades específicas para o exercício da liberdade de expressão e do direito ao acesso à informação nos meios digitais.

A conjuntura dessas competências definidas como alfabetização midiática informacional (ou educação digital), seria mais uma medida que possibilitaria a fortificação de uma cultura de responsabilidade na circulação das informações nas plataformas, apresentando-se como mecanismo de mudança de infraestrutura do conteúdo circulante na rede.

Dessa forma, compreende-se que talvez seja a hora de aproveitar e ampliar as políticas de infraestruturas estudadas e recém-aplicadas ao conteúdo de combate à desinformação, como um norte para a mudança de paradigma na interpretação da relação estabelecida entre usuários e provedores de aplicações internet quando da violação de direito dos primeiros nas plataformas digitais. [12]

As plataformas devem se voltar ao atendimento de políticas de uso da rede que abarquem dentre outras coisas, deveres de transparência abrangendo, por exemplo, a fundamentação direta dos motivos que levam a remoção de um conteúdo por violação de direitos, assim como a emissão de relatórios periódicos contendo número de postagens removidas, o motivo das remoções, relatório em números da quantidade de conteúdos violadores de direitos notificados à plataforma, dentre outras hipóteses que visem a segurança e clareza da relação envolvendo provedores de internet e usuários. Além disso, as plataformas devem adotar mecanismos eficazes de reclamação e identificação de contas, além do incentivo à educação digital.

Esta parece se apresentar como a melhor maneira de minimizar a violação de direitos entre usuários na rede, ao tempo em que provedores de aplicações de internet aplicam ferramentas de infraestrutura que conferem maior transparência no tocante à circulação do conteúdo e de modo que se preserve o amplo discurso e a liberdade de expressão.

É certo que não se pode garantir uma real mudança sem que a mesma seja aplicada, até porque a internet desde sua existência se mostra como uma verdadeira "caixinha de surpresas". Assim, não se pode prever se a aplicação dessas obrigações de infraestrutura irá de fato mudar em grande medida o comportamento dos usuários quanto ao modo como interagem nas plataformas e compartilham conteúdo, ou seja, se essas mudanças de infraestrutura minimizariam de modo amplo a violação de direitos entre os usuários.

Todavia, certo é que a aplicações de tais ferramentas estruturais garantem um acesso à rede mais transparente e conferem um sentimento de maior segurança para o usuário, o que por si só já se apresenta um relevante benefício.

Assim, ainda que se acredite firmemente que mudanças estruturais nas plataformas mudam a forma como conteúdo é compartilhado pelos usuários, ainda que isso potencialmente não ocorra de forma significativa, não há como negar os

benefícios de uma rede que propicia maior transparência no tocante à circulação do conteúdo, e que preserva o amplo discurso e a liberdade de expressão. Portanto, essa é atualmente a forma mais adequada de se solucionar o conflito envolvendo as violações de direitos dos usuários na internet e a necessária responsabilidade dos provedores de aplicações por esses conteúdos violadores de direitos.

Notas

1. SOUZA, Carlos Affonso e TEFFÉ, Chiara Spadaccini. Liberdade de Expressão e o Marco Civil da Internet. Pesquisa Tic Domicílios. 2016, p. 43. Disponível em: https://www.academia.edu/36006753/LIBERDADE_DE_EXPRESS%C3%83O_E_O_MARCO_CIVIL_DA_INTERNET Acesso em: 09/12/2019

2. TEFFÉ, Chiara Antonia Spadaccini de. A responsabilidade civil do provedor de aplicações de internet pelos danos decorrentes do conteúdo gerado por terceiros, de acordo com o Marco Civil da Internet . Revista Fórum de Direito Civil RFDC. Belo Horizonte, ano 4, n. 10, set. / dez. 2015. Disponível em: https://www.editoraforum.com.br/noticias/a-responsabilidade-civil-do-provedor-de-aplicacoes-de-internet-pelos-danos--decorrentes-do-conteudo-gerado-por-terceiros-de-acordo-com-o-marco-civil-da-internet/ Acesso em: 18/06/2020

3. Disponível em: https://feed.itsrio.org/remover--ou-n%C3%A3o-remover-conte%C3%BAdo-falso-eis-a-quest%C3%A3o-73399efcd6cf Acesso em: 18/06/2020.

4. Disponível em: https://blog.twitter.com/pt_br/topics/company/2019/uma-atualizacao-sobre--nossa-estrategia-continua-durante-o-covid-19.html Acesso em: 18/06/2020.

5. Disponível em: https://canaltech.com.br/redes-sociais/sem-fake-news-instagram-expande-medidas-de-combate-a-desinformacao-158083/ Acesso em: 18/06/2020.

6. Disponível em: https://www1.folha.uol.com.br/poder/2020/04/combate-a-fake-news-requer-criterios-democraticamente-legitimos.shtml?pwgt=l8dwudzcavpr9dfltflfpx5ptozru-9q9botz4j41xut6vncy&utm_source=whatsapp&utm_medium=social&utm_campaign=compwagift Acesso em: 18/06/2020.

7. Os deveres consistem em: i) investir em produtos, tecnologias e programas para ajudar as pessoas a tomar decisões informadas quando encontrarem notícias online que possam ser falsas; ii) desenvolver e implementar indicadores eficazes de confiabilidade, em colaboração com o ecossistema de notícias; iii) investir em meios tecnológicos para priorizar informações relevantes, autênticas e oficiais em pesquisas, feeds ou outros canais de distribuição classificados automaticamente; iv) investir em recursos e ferramentas que facilitam as pessoas a encontrar diversas perspectivas sobre tópicos de interesse público.

8. Disponível em: https://santaclaraprinciples.org/ Acesso em: 18/06/2020.

9. Disponível em: https://santaclaraprinciples.org/ Acesso em: 18/06/2020.

10. Disponível em: https://medium.com/contrarraz%C3%B5es/modera%C3%A7%C3%A3o-de-conte%C3%BAdo-princ%C3%ADpios-de-santa-clara-e-marco-civil-da-internet--4183891b2976 Acesso em: 18/06/2020.

11. O termo “alfabetização” é amplamente conhecido como o processo por meio do qual aprendemos a ler e a escrever, ou seja, a utilizar o sistema ortográfico, tão essencial para a comunicação moderna. Nota-se que, assim como a linguagem escrita foi um divisor de águas na história da humanidade, as tecnologias da informação e mídias sociais também podem ser consideradas como um novo sistema de comunicação para o qual, inclusive, se exige igualmente um processo específico de aprendizagem.
No entanto, o uso intuitivo dessas ferramentas permitiu a adoção dessa nova linguagem de forma massiva e repentina, sem que nos déssemos conta da importância de se investir em uma aprendizagem adequada do sistema digital, principalmente para as pessoas que não cresceram diretamente em contato com essa nova linguagem.
Disponível em: https://feed.itsrio.org/remover--ou-n%C3%A3o-remover-conte%C3%BAdo-falso-eis-a-quest%C3%A3o-73399efcd6cf Acesso em: 18/06/2020.

12.
1. Compreender o papel e as funções das mídias e de outros provedores de informação nas sociedades democráticas e as condições nas quais essas funções possam ser realizadas;
2. Reconhecer e articular sua necessidade informacional para poder localizar, acessar, extrair e organizar informações relevantes;
3. Avaliar com senso crítico, em termos de autoria, credibilidade e finalidade, o conteúdo na internet;
4.Comunicar sua compreensão sobre o conhecimento criado, com ética e responsabilidade, no meio mais apropriado;
5.Aplicar as habilidades em tecnologia da informação e comunicação (TIC) para processar informação e produzir conteúdo, engajando-se nas mídias com liberdade de expressão, diálogo intercultural e participação democrática

Disponível em: https://feed.itsrio.org/remover--ou-n%C3%A3o-remover-conte%C3%BAdo-falso-eis-a-quest%C3%A3o-73399efcd6cf Acesso em: 18/06/2020.

Trabalho final do IV Grupo de Pesquisa ITS Rio

Desafios na contratação de *startups* pela administração pública

Rafael Ribeiro Neto

Inovação

Introdução

A contratação de *startups* e soluções ligadas à inovação pela administração pública é um tema extremamente relevante hoje. O avanço tecnológico proporcionado pela revolução 4.0, trouxe desafios para o Estado, não só para sua função regulatória, mas também administrativamente e na prestação de serviços. Contratar *startups* e incorporá-las à administração pública e, ainda, possibilitar uma entrega de serviços mais eficientes aos cidadãos, é hoje um desafio para o setor público. A inflexibilidade legislativa e o controle excessivo são algumas das críticas. Apesar disso, há saídas e os gestores públicos estão olhando atentamente tudo isso e analisando as melhores formas não só alterar as legislações vigentes, como também criar maneiras para atingir o que o processo legislativo tradicional não permite.

Nesse contexto, o presente artigo visa apresentar um panorama do processo licitatório, seus desafios e soluções viáveis para contratação de startups pela administração pública.

Revolução industrial 4.0

Em 2011 surgiu na Alemanha a denominação "Indústria 4.0", a fim de dar vida ao projeto alemão de promover um salto de competitividade nunca visto antes no país por meio do uso de novas tecnologias, como sistemas ciber-físicos (CPS), *big data analytics*, computação em nuvem, internet das coisas (*IoT*) e internet dos serviços (*IoS)*, impressão 3D, outras formas de manufatura aditiva, inteligência artificial, digitalização, colheita de energia (*energy harvesting*) e realidade aumentada.

Em paralelo às mudanças ocasionadas pela indústria 4.0, várias outras importantes mudanças em outros ambientes modificaram as economias, como por exemplo, o avanço de novas fontes de energia renovável, veículos autônomos, utilização de robôs e uso de inteligência artificial para eliminar tarefas repetitivas, uso de *blockchain* em estruturas conservadoras (bancos, cartórios, dentre outras) e tantas outras que impactaram diretamente a economia no mundo. O avanço de novas fontes de energia renováveis a maneira com a qual países industrializados se relacionam com países como o Brasil, que é polo mundial na produção de energia renovável. Robôs e inteligência artificial impactaram diretamente nos postos de trabalho e causam transformações na maneira como trabalhamos e a existência das nossas profissões passa a ser questiona se seremos essenciais ou não. A *blockchain* impacta diretamente o sistema financeiro com transações transparentes, reconhecimento de documentos e outras transações, que se tornam instantâneas, remodelam o conceito de moeda e tantas outras aplicações ainda inexploradas. Diante dessas mudanças, é cada vez mais difícil prever quais serão as consequências sobre nossas vidas, na economia, nas empresas, nos mercados, etc.

A revolução industrial 4.0 foi precedida pela 1ª revolução industrial que fazia uso de motores a vapor e equipamentos mecânicos nas fábricas do século XVIII. Já na 2ª revolução industrial, uso de linhas de produção e ampla aplicação da eletricidade na manufatura na segunda metade do século XIX. Na 3ª revolução industrial, era aplicada à eletrônica, tecnologia da informação e automação dos processos de produção nas últimas três décadas do século XX. Todas elas têm algo em comum: a chegada de novas tecnologias, que, quando empregadas de forma ampla na indústria, transformaram de forma muito rápida a produção e prestação de serviços.

Porém, há diferenças extremamente importantes entre a revolução industrial 4.0 e as outras que a antecederam: antes o impacto causado, a direção de desenvolvimento tecnológico, econômico, público e, ainda, a velocidade de implementação de tecnologia com que ela acontece. O impacto da revolução 4.0 é de transformações ainda maior do que as outras revoluções, a direção de desenvolvimento nas diversas áreas demonstra um potencial de aplicação dessas tecnologias nas mais diversas áreas, fato que nas outras revoluções os impactos eram muito mais relacionados ao terceiro setor e na revolução 4.0, o impacto é a multidisciplinaridade, a escala de aplicações tecnológicas e a metrificação, extração e utilização de dados de qualquer pessoa, atividade, máquina, etc., tendo aplicação, por exemplo, na administração pública com a utilização de *big data* e análise de dados para mapeamento, controle, diagnóstico e monitoramento de localização de *smartphones*, visando o combate de uma eventual pandemia, possibilitando que a administração pública tome decisões com base nesses dados para mitigar ou controlar a pandemia em determinada localidade.

Em um mundo extremamente conectado, readequado a utilização de dados e com uma nova concepção de manufatura e prestação de serviços, a indústria 4.0 possibilitou a criação de pequenas fábricas modulares, flexíveis e ultraconectadas possibilitando reduzir drasticamente o custo de produção e aumentando a escala, além de possibilitar inovações nunca antes vistas, fazendo com que a previsibilidade que havia há 50 anos atrás, não seja mais possível.

Startups, as empresas do século XXI

Com um crescimento exponencial nos últimos anos e a sua popularização no fim do século passado, o mundo corporativo foi tomado pelas empresas deste século, as chamadas *startups*.

O *Oxford English Dictionary* aponta que o primeiro uso da palavra "*startup*" para definir empresas inovadoras foi feito em um artigo publicado pela Forbes em 1976: "*The unfashionable business of investing in startups in the electronic data processing field*".

Com base na atuação de pessoas do segmento das *startups*, Alex Payne[1], ex-engenheiro do Twitter e fundador da Simple (uma *fintech*[2]), ele conceitua como *tech companies* aquelas cuja atuação envolve vender um produto ou fornecer algum serviço relacionado à tecnologia. Assim, se o cliente consome a própria tecnologia da empresa, pode-se dizer que esta é uma *tech company*.

Outro conceito muito bem aceito é o do Eric Ries[3] (2011):

> *"É uma instituição humana designada a entregar um novo produto ou serviço sob condições de extrema incerteza, algo que se pode reproduzir repetidamente em grande quantidade com grande ganho de produtividade, também conhecido como produção em massa."*

Segundo dados[4] da Associação Brasileira de Startups – Abstartups, já são mais de 12 mil *startups* de diversos setores mapeadas no Brasil e com grande potencial crescimento.

Como o Brasil define startups?

A lei complementar nº 123[5] em seu art. 65-A diz que:

> Art. 65-A. É criado o Inova Simples, regime especial simplificado que concede às iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem como startups ou empresas de inovação tratamento diferenciado com vistas a estimular sua criação, formalização, desenvolvimento e consolidação como agentes indutores de avanços tecnológicos e da geração de emprego e renda.
> § 1º - Para os fins desta Lei Complementar, considera-se startup a empresa de caráter inovador que visa a aperfeiçoar sistemas, métodos ou modelos de negócio, de produção, de serviços ou de produtos, os quais, quando já existentes, caracterizam startups de natureza incremental, ou, quando relacionados à criação de algo totalmente novo, caracterizam startups de natureza disruptiva.
> E
> § 2º - As startups caracterizam-se por desenvolver suas inovações em condições de incerteza que requerem experimentos e validações constantes, inclusive mediante comercialização experimental provisória, antes de procederem à comercialização plena e à obtenção de receita.

Mesmo com a lei complementar, o Brasil ainda não possui um conceito formal de startups. Sabendo desse *gap* e buscando conceituar e possibilitar o desenvolvimento das startups, desburocratizar e propiciar um ambiente mais seguro e favorável aos negócios, há um projeto de lei – PLP nº 146[6] de 2019, chamado de "Marco Legal das Startups" em trâmite no Congresso Nacional que conceitua startup como:

> "A pessoa jurídica constituída em quaisquer das formas legalmente previstas, cujo objeto social principal seja o desenvolvimento de produtos ou serviços inovadores de base tecnológica com potencial de rápido crescimento de forma repetível e escalável."

Como outros países definem *startups*?

Em alguns países já existe o conceito legal de *startup*, é importante entender que cada país busca classificar o termo de maneira diferente, mas sempre com o objetivo de desenvolvimento das *startups* e de seus ecossistemas. A lei italiana[7] tem como requisitos que a *startup* tenha no máximo cinco anos de vida, seja sediada na Itália, não distribua lucro, fature anualmente no máximo cinco milhões de euros, comercialize produtos ou serviços com alto valor tecnológico e outros aspectos básicos.

Na Letônia[8], para ser caracterizada como uma *startup* a empresa deve ter no máximo cinco anos de vida, o faturamento nos dois primeiros anos de vida não pode ser maior que duzentos mil euros, 50% dos gastos da *startups* devem ser gastos com pesquisa e desenvolvimento, e pelo menos 70% dos colaboradores devem possuir mestrado ou doutorado, além de outros requisitos para preencherem o status de *startup*.

A legislação francesa[9] requer que a *startup* seja constituída em até oito anos, tenha a qualificação de microempresa ou empresa de pequeno porte conforme as leis francesas, tenha em sua composição societária pelo menos 50% das suas ações ou quotas com empreendedores ou fundos de *venture capital*[10] e outros requisitos.

Importante notar que o conceito de *startup* para fins legislativos varia de acordo com a política adotada pela administração pública de cada país e sua finalidade. Geralmente *startups* possuem apelo de desenvolvimento tecnológico e diversos países passaram a criar conceitos e políticas públicas para estimular o desenvolvimento delas, de tecnologia, pesquisas e claro de negócios.

Govtechs, as *startups* que levam inovação para a administração pública

Com a crescente onda das *startups* e a possibilidade de atuação delas em diversos setores, o termo *startups* foi direcionado para outros setores como o financeiro, em que temos as chamadas *fintechs* que são *startups* que oferecem soluções para o mercado financeiro. A administração pública também é alvo das *startups* chamadas de *govtechs*, que nada mais são do que *startups* que oferecem produtos e serviços com tecnologia e inovação para o setor público e para uso interno de seus colaboradores e na prestação de serviços externos, direcionados a seus clientes, no caso, os cidadãos.

Segundo o BrazilLab[11], hub de inovação que acelera ideias e conecta empreendedores com o poder público, pode se destacar três pontos em comuns as tradicionais *startups* e as *govtechs*:

i- O uso de ferramentas digitais;
ii- Análise de dados e utilização de novas tecnologias, e;
iii- Pessoas que transitaram entre esfera pública e privada que podem oferecer com um olhar diferente, serviços melhores do que o prestado atualmente à população.

As *govtechs* não definem os cidadãos como seu público-alvo, mas sim a administração pública, que por meio de políticas públicas e em conjunto *govtechs* conseguem desenvolver, testar, implementar seu produto ou serviço de acordo com o seu objetivo e, então, atingir o maior número possível de cidadãos.

Um dos principais benefícios que as *govtechs* oferecem à administração pública é o aumento de eficiência do Estado e, consequentemente, impacto positivo para a sociedade como um todo. Metodologias ágeis para reorganização de processos internos conseguem trazer agilidade, eficiência, qualidade de serviços internos, clareza das atividades e outros benefícios para os colaboradores da administração pública.

O uso de *big data*, inteligência artificial, *machine learning* oferecem escala, diminuição dos gastos, economia com pessoal, assertividade na tomada de decisões. Por exemplo, já há *govtechs* que utilizam dados públicos disponíveis em portais de transparência para padronização e cruzamento de dados, gerando relatórios para tomada de decisões mais assertivas e controle fiscal das contas públicas. As ouvidorias do Supremo Tribunal Federal e do Superior Tribunal de Justiça já utilizam inteligência artificial para funções que antes eram realizadas apenas por pessoas e agora serão pelas máquinas.

No Reino Unido, um estudo realizado pela PWC[12], demonstrou um crescimento em investimentos nas *govtechs* de 198% em 2017. A ideia de uma *govtech* é incorporar tecnologias e inovação no setor público, possibilitando melhorias, modernizações, eficiências, diminuição de gastos, transparência e, principalmente, qualidade de serviços públicos prestados.

Alguns países traçaram planos para se transformar por meio de tecnologias, fomento ao empreendedorismo e desenvolvimento de *startups*, *govtechs* e todos os outros nichos de atuação. A Estônia, por exemplo, tem o inovador projeto governamental de digitalização da sua sociedade chamado "e-Estônia", esse projeto possibilita economizar 2% do seu Produto Interno Bruto – PIB, traz comodidade e facilidade para sua sociedade e, ainda, facilita o acesso a serviços públicos[13].

O Uruguai, por meio de sua agência governamental *Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento* – AGESIC, produziu diversas iniciativas voltadas para inovação e digitalização, buscando desburocratizar o país e, ainda, aumentar a conectividade. Um exemplo de iniciativa é o plano de ação de governo aberto[14], distribuído em 11 eixos temáticos que combinados firmam um total de 39 compromissos para inovar e desenvolver o Uruguai.

No Brasil, mais precisamente no estado do Amapá, a administração pública estadual, criou o Programa de Inovação com Tecnologia da Informação (PITI)[15], que surgiu da vontade de conectar o movimento de criação de *startups* com os desafios enfrentados pelo setor público. O programa se tornou parte da estratégia da administração pública para fortalecer o empreendedorismo no Amapá ao fomentar a criação de *startups* digitais. O estado já investiu mais de R$ 250 mil reais no desenvolvimento de projetos e a tendência é que esse número cresça. Diferente de outros estados em que o número de *startups* são maiores, como Santa Catarina, São Paulo e Minas Gerais, a administração pública criou um programa para fomentar a criação de *startups* e fortalecer isso no estado do Amapá. De 2017 para cá, 10 *startups* foram impactadas pelo programa, desenvolvendo protótipos para as soluções dos desafios enfrentados pela administração pública, sendo que das 10 *startups*, 4 estão operando seu modelo de negócios.

Licitações

A administração pública exerce uma pluralidade de atividades complexas, visando o interesse público. Para que isso aconteça, ela precisa valer-se de serviços, bens, produtos fornecidos por terceiros, motivo este em que a administração pública é obrigada a firmar contratos para realização de obras, prestação de serviços, fornecimento de bens, execução de serviços públicos, etc. com empresas, *startups* e outras pessoas jurídicas.

O processo de contratação de terceiros para realização dessas atividades é chamado de licitação. A licitação é um procedimento administrativo, por meio do qual a administração pública e aqueles vinculados a ela, selecionam a melhor proposta dentre as oferecidas, por meio de parâmetros pré-estabelecidos e firmam contrato com a empresa interessada que preenche esses parâmetros. O processo licitatório e os contratos administrativos da licitação são regulados pela lei nº 8.666 de 1993, a chamada lei de licitações.

Esses parâmetros são descritos em editais[16] e são os protagonistas dos processos licitatórios, sendo necessário constante o aprimoramento para que as licitações sejam efetivamente capazes de satisfazer o escopo, que motivou a realização do processo licitatório. A lei das licitações sempre exigiu a especificação do produto, bem ou serviço pretendido pela administração pública, determinando, ainda, que ela deveria ser certa e discriminada. Essa é a lógica prevista na Lei 8.666/93, notadamente na definição de projeto básico prevista no inciso IX do art. 6º[17].

Os principais objetivos do processo licitatório são satisfazer a uma necessidade da administração pública e da sociedade em geral.

As licitações possuem modalidades em que serão determinadas segundo o objeto licitado (se é um bem ou serviço específico e o valor da compra). As licitações possuem também tipos, que serão definidos de acordo com a escolha da melhor proposta.

A concorrência é uma modalidade de licitação aberta a qualquer interessado, desde que comprove que sua empresa atenda aos requisitos mínimos previsto no edital para execução do objeto.

A tomada de preço é outra modalidade de licitação aberta a interessados cadastrados ou que já atendam às condições exigidas no cadastramento dentro do prazo antes do recebimento das propostas.

O convite é uma modalidade em que a administração pública convida empresas do segmento do objeto licitado para participar do processo de licitação.

O pregão é a opção mais utilizada para aquisição de bens e serviços comuns, podendo ser realizado de forma presencial ou digital.

Os tipos de licitação são divididos em 3: o primeiro trata do menor preço, em que ganha a proposta que for mais vantajosa para a administração pública em relação a valores (quem preencher os requisitos e apresentar o menor valor será o vencedor). O segundo tipo é o de melhor técnica, no qual a administração pública leva em conta a proposta que for mais vantajosa em termos técnicos e, por fim, por preço e técnica, quando é apresentado pela empresa sua proposta e documentação em 3 envelopes (um para habilitação, um para a proposta técnica e por último, um com preço), que são avaliados seguindo essa ordem.

Desafios na contratação pública de *startups*

A contratação de *startups* pela administração pública é algo que vai ao encontro aos desafios do século XXI, enquanto administração pública e de como exercer a sua função administrativa, regulatória e executiva, promover a entrega para a sociedade de forma mais eficiente, com maior assertividade e acessibilidade de informações. O avanço tecnológico dos últimos anos possibilita que isso seja feito, mas requer uma nova forma de se fazer negócios entre *startups* e administração pública para

superar os desafios comuns ao processo de contratação pública.

As *startups* também passam pelo processo licitatório e os principais desafios são: o processo é caro, burocrático, lento e muito arriscado devido à insegurança jurídica dos órgãos de controle[18] sobre o processo de licitação.

Outro desafio frequentemente citado pelos empreendedores é a exigência de garantia contratual, o que é discricionário do gestor, segundo a lei e que é muito comum nos editais de licitação. Em se tratando de *startups*, esse costume pode limitar a competitividade e não possibilitar que a administração pública conquiste a melhor solução para seu problema, uma vez que, *startups* no geral não possuem equilíbrio financeiro para dispor de um crédito como garantia.

As especificações técnicas previstas nos editais são as partes mais importantes de um processo licitatório, sendo essencial o aprimoramento dessas, uma vez que é necessário satisfazer a necessidade motivada na realização do processo. É exigência legal a especificação da solução pretendida pela administração pública.

Em se tratando da área de inovação e tecnológica, a exaustão e objetividade de qualquer projeto relacionado a contratação de soluções para a administração pública, esse processo é muito sensível e, geralmente, leva a administração pública a dois caminhos: um grande investimento de recursos financeiros público com pesquisas, consultorias, servidores e outros para realização de um mapeamento e especificações de soluções de TI ou ineficiência administrativa para mapear e especificar o que o mercado pode oferecer.

Isso acontece devido à complexidade e ao dinamismo das *startups* e suas soluções não são tangíveis pelo processo licitatório e as ferramentas previstas no ordenamento jurídico não são suficientes para lidar com essas situações tão comuns às *startups*, necessitando que a administração pública atualize seus processos e ordenamento jurídico para se relacionar melhor com as *startups*, a tecnologia e a inovação.

É evidente que a lei das licitações não foi feita para integrar as *startups*, novas tecnologias e inovação com a administração pública, ela foi feita para aquisição de bens, realização de serviços, principalmente, voltados para obras públicas. Mesmo assim, a licitação passou por várias mudanças ao longo do tempo para possibilitar a inovação e o desenvolvimento tecnológico junto à administração pública.

Esse argumento é um consenso entre os administradores públicos e os atores do mercado de inovação, que tem alguma relação com a administração pública e os que desejam ter. Outro ponto relevante é a inflexibilidade a ferramentas, atuações entre todos os interessados e a adoção da tentativa e erro, algo muito comum entre as *startups* é que, ao desenvolverem uma solução, a *startup* realiza uma medição da aceitabilidade dos seus usuários frente ao que foi desenvolvido, colhido o *feedback*, acontece os ajustes de acordo com o *feedback* dos usuários para tornar a solução melhor, algo incomum com os atores da administração pública.

Dispensa de licitação e contratação de *startups* por empresas estatais

Geralmente os contratos com a administração pública devem passar pelo processo licitatório, mas há duas possibilidades em que isso não, necessariamente, tem que acontecer: a dispensa de licitação ou a sua inexigibilidade.

A dispensa da licitação está prevista no art. 24 da lei 8.666 de 1993[19] e acontece em situações em que, mesmo havendo a possibilidade de competição entre empresas particulares, o processo de licitação não é utilizado para a contratação pela administração pública, podendo essa, contratar diretamente.

A lei nº 10.973 de 2004 prevê a possibilidade de incentivos à inovação e à pesquisa científica e tecnológica em ambientes produtivos, criando uma hipótese de dispensa de processo licitatório.

O decreto nº 9.283 de 2018[20] implementa uma série de mudanças legislativas com o objetivo de facilitar o desenvolvimento de projetos de inovação tecnológica e que sejam de interesse público e beneficie a cadeia produtiva nacional. Consta nele, a possibilidade de dispensa de processo licitatório de serviços e obras de engenharia que são essenciais para o desenvolvimento de projetos de inovação tecnológica e aumenta as possibilidades de contratação direta pela administração pública de inovações tecnológicas com objetividade e eficiência:

> Art. 31. O fornecimento, em escala ou não, do produto, do serviço ou do processo inovador resultante das atividades de pesquisa, desenvolvimento e inovação encomendadas na forma estabelecida neste Decreto poderá ser contratada com dispensa de licitação, inclusive com o próprio desenvolvedor da encomenda.

A lei 13.303 de 2016 (Estatuto das Empresas Estatais)[21] prevê a dispensa de licitação em casos em que empresas estatais estejam executando atividades previstas no seu objeto social ou que possa materializar oportunidades de negócio, assim dispõe a lei:

> Art. 28. Os contratos com terceiros destinados à prestação de serviços às empresas públicas e às sociedades de economia mista, inclusive de engenharia e de publicidade, à aquisição e à locação de bens, à alienação de bens e ativos integrantes do respectivo patrimônio ou à execução de obras a serem integradas a esse patrimônio, bem como à implementação de ônus real sobre tais bens, serão precedidos de licitação nos termos desta Lei, ressalvadas as hipóteses previstas nos arts. 29 e 30.
> (...)

> § 3º São as empresas públicas e as sociedades de economia mista dispensadas da observância dos dispositivos deste Capítulo nas seguintes situações:
> I – Comercialização, prestação ou execução, de forma direta, pelas empresas mencionadas no caput, de produtos, serviços ou obras especificamente relacionados com seus respectivos objetos sociais;
> II – Nos casos em que a escolha do parceiro esteja associada a suas características particulares, vinculada a oportunidades de negócio definidas e específicas, justificada a inviabilidade de procedimento competitivo.

Portanto, as contratações realizadas com base no parágrafo deste artigo são dispensadas do processo licitatório e essa contratação direta possui uma relação jurídica de direito privado, uma vez que, não estão inseridas no regime jurídico de contratação via licitação, mas sim no que regula as relações de mercado no qual uma estatal está inserida.

Diante disso, uma estatal poderá em seu edital definir o seu problema segundo critérios em que se avalie soluções inovadoras que de fato resolvam aquele problema, o que não acontece no processo licitatório tradicional. A estatal ainda poderá destacar as especificações necessárias e os resultados esperados, possibilitando no processo seletivo com esses e outros critérios definidos anteriormente, tornar a contratação de soluções inovadoras para seus problemas mais assertiva e eficiente.

Um exemplo dado por Pedro Ivo Peixoto[22]:

> (...) uma estatal do setor bancário pretende valer-se de solução digital para maximizar a oferta de crédito a potenciais clientes por meio de fintechs que se remunerem por comissões nas operações que realizar. Enquadrada possivelmente nos dois incisos do § 3º do art. 28 da Lei 13.303/2016, a estatal poderia lançar edital de chamada pública para selecionar a solução que se mostrar mais eficiente segundo os critérios expostos, e firmar com um ou mais concorrentes contratos privados.

O processo a ser realizado nos moldes do art. 28 da lei 13.303 de 2016 são feitos de forma livre pela empresa estatal, mas deve respeitar os princípios que regulam a administração pública, além de adotarem critérios e regulamentos bem estabelecidos.

Parcerias público privadas - PPPs

A parceria público privada ou PPP são acordos entre os setores público e privado para a realização conjunta de determinado serviço ou obra de interesse da população.

As parcerias público privadas (PPPs) são regulamentadas pela lei nº 11.079 de 2004 e subsidiariamente pela lei 8.987 de 1995 (lei geral das concessões), também pela lei 9.074 de 1995 e os contratos administrativos que não são classificados como contratos de concessão (por exemplo, concessão de estrada rodoviária) estão sujeitos à lei 8.666 de 1993.

O setor de *govtechs* cresce na Europa oferecendo soluções inteligentes para infraestrutura social nos segmentos de iluminação pública, gestão de resíduos sólidos, mobilidade urbana, saúde e segurança, entre outros. E um importante mecanismo de crescimento é a PPP.

Amsterdam possui um programa de desenvolvimento de inovação urbana baseado em um concurso público de inovação com vários desafios que a cidade possui e que está sendo replicado em várias outras cidades. Se valendo de parcerias público privadas, Amsterdam vai combatendo os seus problemas urbanos por meio do programa "*Amsterdam´s Startup-in-Residence Programme* (SiR)" com inovação e envolvimento de todos os atores locais, desde a administração pública municipal até os ecossistemas empresariais locais.[23]

Os contratos públicos de Amsterdam com o programa são baseados no orçamento público e nas demandas do governo que visam criar e difundir estrategicamente inovações buscadas pela sociedade dos problemas que elas e o governo apontam. Além disso, o programa se vale das parcerias público privadas que beneficiam e promovem o desenvolvimento econômico impulsionado pela inovação.

O Bay Area Council Economic Institute em um dos seus reports cita que que há uma lacuna de investimentos em infraestruturas e uma falta de capacidade dos órgãos públicos em desenvolver e gerenciar compras complexas. Por meio do projeto chamado P3[24], o governo incentiva o setor privado a entrar em projetos, principalmente voltados para área de infraestrutura, que é um aspecto fundamental na utilização de métodos inovadores na entrega de projetos.

No Brasil, há o Iguá Lab[25,] que atua no gerenciamento e na operação de sistemas de abastecimento de água e esgotamento sanitário, por intermédio de concessões e de parcerias público-privadas. Há também, o programa Energy Future[26] da ANEEL[27] e todo o setor de energia elétrica que busca, assim com o Iguá Lab, projetos e soluções inovadoras voltados para o mercado de energia no Brasil.

É importante destacar que um dos principais pontos relacionados à PPP's no mundo inteiro é a possibilidade de desenvolvimento local, da economia do país, além do desenvolvimento tecnológico e da administração pública que cria estratégias

para que todo o ambiente de inovação se desenvolva, seja como em Amsterdam ou na Califórnia. As PPP's têm papel fundamental para desenvolvimento de políticas de inovação no mundo inteiro.

Marco legal das startups

O Marco Legal das Startups[28] é um projeto de lei (PLP nº 146/2019) que visa regulamentar as *startups* enquanto negócios no Brasil, visando uma simplificação de processos e desburocratização para que o ecossistema empreendedor brasileiro se desenvolva.

A importância do marco legal não é só definir o conceito de *startups*, mas também permitir que o ecossistema brasileiro se desenvolva, tenha processos formais bem definidos, permita o acesso ao crédito e, principalmente, dê segurança jurídica para os empreendedores e seus negócios.

Um dos pontos mais relevantes e de grandes discussões do marco legal das *startups* está relacionado a contratação destas pela administração pública e como encontrar uma forma para que isso aconteça, dada suas características.

Alguns pontos a serem observados na criação do marco legal está relacionado a contratação pública de *startups*. É importante entender que elas não são semelhantes a empresas tradicionais. É necessário mudança de cultura e de pensamento para criar soluções para que as *startups* possam de fato ser incluidas na da administração pública.

Nos trabalhos de criação do marco legal, e mais especificamente o grupo responsável[29] pelo tema da contratação de *startups* pela administração pública, foi destacado pelos redatores que uma mudança legislativa não é suficiente, é necessário uma mudança de cultura para atualizar o processo de compras públicas, visando contratar *startups* e essas se tornarem fornecedoras do poder público como também levar inovação aos órgãos públicos.

Apesar da nossa legislação ter avançado muito e já haver mecanismos para contratação de *startups* e inovação pela administração pública, o alto nível de burocracia e a alta interferência jurídica dos nossos órgãos de controle são grandes desafios a serem superados, o marco legal é importante para possibilitar a mudança cultural, principalmente, nos níveis estaduais e municipais.

É importante que por um lado, a administração pública faça testes, lance processos e programas pilotos em todas as esferas que ela visa contratar serviços, produtos e soluções inovadores que foram ou estão em desenvolvimento por *startups*. E por outro lado, é essencial que as empresas que aceitem correr os riscos do insucesso desses testes e os programas possam de fato ser contratados de forma direta, caso sejam bem-sucedidas, alinhando seus objetivos com a administração pública.

Um processo licitatório simplificado beneficiaria bastante a validação e os testes das soluções das *startups*, e ainda evitaria problemas, como a definição da modalidade e do tipo da licitação a ser seguida e a redação dos termos de referência que são vistos como genéricas demais ou são comparadas com soluções já testadas, não direcionando muito bem no momento de contratação.

Baseado em experiências prévias, que trouxeram resultados positivos e que necessitavam aprimoramento como o PitchGov SP[30] e o Pitch Sabesp[31], uma das soluções encontradas é a utilização de *"termo de colaboração para teste de inovação (TCTI)[32]"*, que possibilita que a administração pública faça testes e, posteriormente, realize a contratação das startups, usando o seu poder de compra para o desenvolvimento das startups.

A criação do TCTI tem o objetivo de que *startups* e empresas de base tecnológica possam estabelecer relações de cooperação e colaboração com entidades e, principalmente, para com a administração pública, isso somente foi possível com uma série de mecanismos advindos da lei nº 13.019 de 2014. Administrações, nas esferas estadual e municipal, costumeiramente adotam um termo de colaboração envolvendo entidades, prefeitura/estado e as *startups* ou ainda uma eventual edição de lei, seja ela municipal ou estadual tratando de inovação e possibilidade de testes.

O estado do Espírito Santo é um exemplo claro da criação desse tipo de mecanismo, o seu projeto de lei complementar nº 48 de 2019[33] foi aprovado e institui procedimentos e fomento entre a administração pública estadual e as *startups*.

É importante destacar que a lei nacional de inovação (nº 10.973 de 2014) já prevê a autorização para que a União, estados, Distrito Federal e os municípios possam realizar compras para fomento e desenvolvimento de *startups* e inovação.

O artigo 19, § 2º-A, inciso VII, elenca a possibilidade do poder de compra do Estado como um mecanismo de fomento à inovação pela administração pública. Ele também é corroborado no § 6º, incisos IX e XII, que dispõe da extensão desses mecanismos previstos em lei para "*indução de inovação por meio de compras públicas*" e "*implantação de solução de inovação para apoio e incentivo a atividades tecnológicas ou de inovação em microempresas e em empresas de pequeno porte*"[34] o que na grande maioria dos casos, abrange as *startups*.

Além dessas previsões, o artigo 20-A, também da lei nacional de inovação, diz o seu § 3º que *"Outras hipóteses de contratação de prestação de serviços ou fornecimento de bens elaborados com aplicação sistemática de conhecimentos científicos e tecnológicos poderão ser previstas em regulamento"*.

É notório que o legislador ao redigir a lei da inovação possibilitou liberdade maior para que se criasse e desenvolvesse soluções inovadoras na contratação de bens, produtos ou serviços pela administração pública.

Dito isso, dentro da possibilidade de se validar rapidamente da contratação ou não de qualquer *startup*, a contratação realizada seguindo os moldes do TCTI pode ser considerada uma abordagem mais lógica para desenvolvimento das *startups*, incorporação delas à administração pública, mais transparência, além de aproximar a administração pública de uma administração e governo aberto, possibilitando que essa possa realizar desafios para a sociedade ou *startups* possam apresentar soluções para a administração pública, seguindo o que é feito em Amsterdam.

A minuta do TCTI prevê a necessidade de definição prévia de objetivos que se pretendem atingir com o teste, estabelece métricas para avaliação e, ainda, o prazo máximo de 1 ano para conclusão dos testes. É necessário também, uma comissão para avaliar com pelo menos 3 pessoas, uma de fora da administração e que tenha conhecimento técnico para avaliar o teste. O apoio financeiro às *startups* também é levado em conta, mas com o objetivo de dar suporte financeiro para expansão dos testes de acordo com os resultados, portanto, pode ocorrer em situações específicas e com valores limitados. Há também, a previsão de que obtido sucesso no teste ou fim do período, a contratação é garantida. Caso os testes não sejam positivos ou surjam novas empresas com soluções semelhantes ao objeto inicial do TCTI, deve-se realizar nova licitação.

O TCTI não tem o objetivo de ser a única forma de contratação de *startups*, até porque o seu procedimento não é obrigatório e há situações em que *startups* já possuem seu produto ou serviço validado e não necessitam da fase de testes. Somente o caso concreto é que poderá determinar a melhor forma de contratação das *startups*.

Considerações Finais

Em vez de se focar na solução, foque no problema e no seu usuário para então encontrar soluções. Esse é um conselho muito dado por empreendedores a pessoas que desejam empreender. Seguir esse conselho é essencial para a administração pública realizar e implementar soluções trazidas pelas *startups*, além de superar gargalos impostos por ela mesma ou por questões legislativas.

A legislação atual e as que virão (vide marco legal das *startups*), já possui mecanismos que permitem a contratação de *startups* pela administração pública. O que é necessário é que a administração pública saiba usar os mecanismos, que as barreiras sejam diminuídas, foque em sua experiência e claro entenda e aprenda com as características dos ecossistemas de *startups* e inovação, e com cases nacionais e internacionais, internalizando tudo que possa beneficiar seus colaboradores e também os cidadãos.

Outro detalhe relevante é que ao não se conectar com os ecossistemas de inovação, a administração pública fica obsoleta, perde a oportunidade de construir políticas públicas para se tornar mais competitiva e relevante (vide Estônia) e caminhar para não só um governo digital, mas também para uma administração pública altamente eficiente, escalável e, claro, transparente.

Notas

1. PAYNE, Alex. What Is and Is Not A Technology Company. Disponível em: <https://goo.gl/9bmrNd> Acesso em 28 jan. 2020.

2. *Fintechs*: são startups que desenvolvem produtos e serviços voltados para o mercado financeiro, por exemplo, o Nubank é uma *fintech*.

3. RIES, Eric. Startup Enxuta. São Paulo: Ed. Leya, 2012.

4. Estudo do número de startups mapeadas pelo Brasil. Abstartups, 2020. Disponível em: <https://startupbase.com.br/home>. Acesso em 28 jan. 2020.

5. Lei complementar nº 123 de 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/lcp/lcp123.htm>. Acesso em 28 jan. 2020.

6. Proposta do Marco Legal das Startups. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1757419>. Acesso em 28 de jan. 2020.

7. Conceito de startup segundo legislação italiana. Rio jrc. Disponível em: <https://rio.jrc.ec.europa.eu/en/library/law-17-december-2012-n221-innovative-start-ups> Acesso em 28 de jan. 2020.

8. Conceito de startup segundo legislação da Letônia. Labsoflatvia. Disponível em: <www.labsoflatvia.com/news/latvvian-startup-law-finally-translated-into-english>. Acesso em 28 jan. 2020.

9. Conceito de startup segundo legislação da França. Impots. disponível em: <www.impots.gouv.fr/portail/international-professionnel/tax-incentives#ISU>. Acesso em 28 jan. 2020.

10. *Venture capital*: conhecido como capital de risco, é uma atividade exercida pelos investidores, através de um fundo de investimento ou veículos próprios de investimento, injetam capital nas empresas em troca de participação societária

11. Conceito de govtech. BrazilLab. Disponível em: <Link> Acesso em 29 jan. 2020.

12. Estudo da PWC sobre transformações públicas no setor público e potencial de investimento. PWC. Disponível em: <https://www.pwc.com/gx/en/psrc/united-kingdom/assets/govtech-report.pdf> Acesso em 29 jan. 2020.

13. HELLER, Nathan. Estonia, the digital republic. The New Yorker. Disponível em: <https://www.newyorker.com/magazine/2017/12/18/estonia-the-digital-republic>. Acesso em 03 fev. 2020.

14. Plano de governo aberto do Uruguai. Disponível em: <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/nuevo-informe-seguimiento-del-4deg-plan-accion-nacional-gobierno-abierto>. Acesso em 03 fev. 2020.

15. Pesquisa feita pelo BrazilLab sobre o PITI. BrazilLab. Disponível em: < https://d335luupugsy2.cloudfront.net/cms/files/53545/1575321270LO_Casesdeinovacao_Amapa_rev_2_2.pdf>. Acesso em 03 fev. 2020.

16. Edital: é um ato escrito em que são apresentadas determinações, características, avisos, citações e demais comunicados de ordem oficial.

17. Art. 6o Para os fins desta Lei, considera-se:
(...)
IX - Projeto Básico - conjunto de elementos necessários e suficientes, com nível de precisão adequado, para caracterizar a obra ou serviço, ou complexo de obras ou serviços objeto da licitação, elaborado com base nas indicações dos estudos técnicos preliminares, que assegurem a viabilidade técnica e o adequado tratamento do impacto ambiental do empreendimento, e que possibilite a avaliação do custo da obra e a definição dos métodos e do prazo de execução, devendo conter os seguintes elementos:
(...)

18. Órgãos de controle: realizam a fiscalização de toda a licitação.

19. Art. 24. É dispensável a licitação:

XXXI - nas contratações visando ao cumprimento do disposto nos arts. 3º, 4º, 5º e 20 da Lei no 10.973, de 2 de dezembro de 2004, observados os princípios gerais de contratação dela constantes.

20. Decreto nº 9.283 de 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9283.htm>. Acesso em 07 fev. 2020.

21. Lei 13.303 de 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/lei/l13303.htm>. Acesso em 07 fev. 2020.

22. PEIXOTO, Pedro Ivo. Contratação de Soluções Inovadoras pela administração pública: desafios e caminhos. Disponível em: <https://web.bndes.gov.br/bib/jspui/bitstream/1408/18641/1/PRArt214894_Contratacao%20de%20solucoes%20inovadoras%20administracao%20publica_P.pdf>. Acesso em 07 fev. 2020.

23. WINDEN, Willem Van. Intermediation in public procurement of innovation: How Amsterdam's startup-in-residence programme connects startups to urban challenges. Disponível em: < https://doi.org/10.1016/j.respol.2019.04.013> Acesso em: 08 fev. 2020.

24. Public-private partnerships in california - how governments can innovate, attract investment and improve infrastructure performance. Disponível em: <http://www.bayareaeconomy.org/files/pdf/P3inCaliforniaWeb.pdf>. Acesso em: 10 fev. 2020.

25. guá Lab. Disponível em: <https://igualab.com.br/>. Acesso em: 10 fev. 2020.

26. Energy Future. Disponível em: <https://www.energyfuture.com.br/>. Acesso em 10 fev. 2020.

27. Agência Nacional de Energia Elétrica.

28. Proposta do Marco Legal das Startups. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1757419>. Acesso em 28 de jan. 2020.

29. Como é possível estimular a contratação de inovação e de startups pelo poder público. Disponível em: <https://www.jota.info/coberturas-especiais/inova-e-acao/como-e-possivel-estimular-a-contratacao-de-inovacao--e-de-startups-pelo-poder-publico-18062019> Acesso em: 28 jan. 2020.

30. O que é o PitGov SP. Disponível em: <http://www.pitchgov.sp.gov.br/>. Acesso em 13 fev. 2020.

31. O que é o Pitch Sabesp. Disponível em: <http://www.sabesp.com.br/pitchsabesp/>. Acesso em 13 fev. 2020.

32. Como é possível estimular a contratação de inovação e de startups pelo poder público. Disponível em: <https://www.jota.info/coberturas-especiais/inova-e-acao/como-e-possivel-estimular-a-contratacao-de-inovacao-e-de-startups-pelo-poder-publico-18062019> Acesso em: 28 jan. 2020.

33. PLC nº 48 de 2019. Disponível em: <https://pge.es.gov.br/Media/pge/docs/PL%20startups.pdf>. Acesso em 11 fev. 2019.

34. Art. 19. A União, os Estados, o Distrito Federal, os Municípios, as ICTs e suas agências de fomento promoverão e incentivarão a pesquisa e o desenvolvimento de produtos, serviços e processos inovadores em empresas brasileiras e em entidades brasileiras de direito privado sem fins lucrativos, mediante a concessão de recursos financeiros, humanos, materiais ou de infraestrutura a serem ajustados em instrumentos específicos e destinados a apoiar atividades de pesquisa, desenvolvimento e inovação, para atender às prioridades das políticas industrial e tecnológica nacional.
§ 2º-A. São instrumentos de estímulo à inovação nas empresas, quando aplicáveis, entre outros:
(...)
VIII – uso do poder de compra do Estado; (...)
§ 6º As iniciativas de que trata este artigo poderão ser estendidas a ações visando a: (Incluído pela lei nº 13.243 de 2016)
(...)
IX – indução de inovação por meio de compras públicas; (Incluído pela lei nº 13.243 de 2016)
(...)
XII – implantação de solução de inovação para apoio e incentivo a atividades tecnológicas ou de inovação em microempresas e em empresas de pequeno porte. (Incluído pela lei nº 13.243 de 2016).

Trabalho final do IV Grupo de Pesquisa ITS Rio

Identidade autossoberana para além do hype

Beatriz Souza Costa

Inovação

Introdução

Os atributos que caracterizam uma pessoa é o que define o termo "identidade". Esses caracteres podem ser aspectos biométricos, nomenclatura e, até mesmo, posicionamentos adotados durante a vida civil. Por ser inerente à pessoa humana, integra os direitos da personalidade. De acordo com a renomada civilista Maria Helena Diniz, "o direito da personalidade é o direito da pessoa defender o que lhe é próprio, como a vida, a identidade, a liberdade, a imagem, a privacidade, a honra, etc."[1]. Esse direito da personalidade se traduz, em uma de suas extensões, no mundo físico e digital através da identidade física e digital, sejam elas emitidas por órgãos governamentais ou não.

Os documentos de identidade fundacionais, como as certidões de nascimento e de casamento, são a identidade legal. A partir deles, é possível gerar os documentos de identidade funcionais, como a Carteira Nacional de Habilitação e o passaporte. Com a desmaterialização das informações, as interações passaram a ser executadas por meio de sistemas de informação interconectados e da internet, resultando no surgimento da identidade digital. Está é conceituada como "os elementos de *hardware* ou *software* que permitem que uma pessoa se identifique e seja autenticada, obtenha as permissões para acessar determinados recursos de informação ou físicos (por exemplo, o acesso a uma área) e realizar transações pela Internet ou redes privadas".[2]

Devido à própria estrutura da Internet, tema que abordaremos ao longo deste artigo, hodiernamente, o usuário fornece seus dados para obter acesso ao serviço a cada *site* acessado. Por conseguinte, diversos *players* do mercado possuem um vasto banco de dados que passam a estar automaticamente suscetíveis a ataques cibernéticos. A "gestão da identidade traz, por um lado, desafios em termos de privacidade, proteção de dados e novos riscos de fraude e, por outro lado, a necessidade de revisar e ajustar os esquemas de governança, os marcos legais e as tecnologias que podem estar se tornando obsoletas".[3]

É nesse cenário que a identidade autossoberana (também conhecida como self-sovereign identity ou SSI, ambos termos em inglês), que, assim como os outros sistemas identitários, se encaixa na discussão atemporal da extensão do direito à privacidade, à proteção de dados e da autodeterminação informativa. O modelo de identidade autossoberana prima permitir o gerenciamento da identidade pelos próprios usuários, sem depender de qualquer tipo tradicional de autoridade centralizada.

Do ponto de vista dos cidadãos, estes experimentarão benefícios econômicos e ganhos de eficiência de serviços, além da alteração do equilíbrio de poder, aumentando a propriedade e o controle sobre seus dados. Uma solução de identidade autossoberana reduz a necessidade de manter repositórios centralizados de informações

de identificação. Uma vez que a propriedade e o atestado de identidade são transferidos para os cidadãos, não há necessidade de hospedar servidores e bancos de dados com dados pessoais. Além disso, com o uso da tecnologia *blockchain*, serão experimentados benefícios econômicos, ganhos de eficiência e um menor risco de vazamentos de dados pessoais.[4]

Considerando a fase inicial da tecnologia *blockchain* no funcionamento da SSI, é notório alguns desafios que precisam ser superados. São eles: (i) interoperabilidade; (ii) proteção de dados, com foco no direito ao esquecimento quando falamos de *on-chain records*; (iii) adesão popular; e (iv) fator humano, principalmente quando falamos de *off-chain records*. Pensando nesses gargalos, elaboramos o presente artigo.

1. Premissa Constitucional

Para demonstrar a importância temática, é de suma importância fixarmos parâmetros sobre o direito à privacidade. A Constituição Federal assegura a privacidade (gênero) ao reconhecer o direito à indenização pelo dano material ou moral decorrente da violação à intimidade, à vida privada, à honra e à imagem das pessoas (espécies), conforme o inciso X do artigo 5º. Portanto, o direito à privacidade é um direito fundamental.

O direito à privacidade sofreu diversas mutações interpretativas ao longo dos anos, indo do *right to be left alone*[5] até o estado atual, onde o ordenamento resguarda a faculdade que cada indivíduo possui de obstar a intromissão de estranhos, assim como de impedir o acesso e a divulgação de informações privadas, sejam elas hábitos, convicções, relacionamentos afetivos, liberdade sexual, convicção política e afins.

Nas palavras de Celso Lafer em "A Reconstrução dos Direitos Humanos",

> *"[a] construção doutrinária e pretoriana em torno do direito à intimidade, que tem como ponto de partida o tema clássico da inviolabilidade de domicílio, passa pelo sigilo da correspondência, o segredo profissional, o direito à honra e à reputação, e acabou adquirindo projeção autônoma em relação aos demais direitos da personalidade, que têm como objeto a integridade moral do ser humano".*[6]

Neste diapasão, Gustavo Tepedino, Heloisa Helena Barboza e Maria Celina Bodin de Moraes recordam,

> *"Como leciona Stefano Rodotà, na atual sociedade de informação tendem a prevalecer definições mais funcionais do conceito, as quais, em diversos modo, fazem referência à possibilidade de um sujeito conhecer, controlar, direcionar ou mesmo interromper o fluxo de informações que lhe dizem respeito (Tecnologie e Diritti,*

> *p. 101, original não grifado). Na doutrina brasileira, Celso Lafer, procurou ampliar o conceito, tomando-o não apenas como "o direito do indivíduo estar só", mas ainda como a "possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo que a ela só refere, e que diz respeito ao seu modo de ser no âmbito da vida privada" (A reconstrução dos Direitos Humanos, p. 239). (...).*
>
> *Sustenta-se na atualidade que o controle das informações pessoais leva também ao direito de determinar o modo de construção da própria esfera privada (Stefano Rodotà, Tecnologie e Diritti, p. 122) – conceito que se encontra em crescente expansão, incluindo cada vez maior número de setores da vida humana e compreendendo, assim, toda uma gama de escolhas existenciais relacionadas à política, ao sexo e à religião, à guisa de exemplo".* [7]

Nas palavras de Caio Mário Pereira da Silva, o direito à privacidade "oferece caráter dúplice: o direito de estar só, de não se comunicar; e simultaneamente de não ser molestado por outrem, como também pela autoridade pública, salvo quando um imperativo de ordem pública venha a determiná-lo".[8] Conclui-se que a finalidade do direito à privacidade é, a grosso modo, defender a esfera privada da pessoa de toda intromissão de terceiros.

Analisando este direito fundamental aplicado a dados, em 1983, o Tribunal Constitucional Alemão inaugurou uma nova linha doutrinária ao afirmar que "não existem mais dados insignificantes". Nas palavras de Marcus Vinicius Furtado Coêlho, ex-presidente da Ordem Brasileira de Advogados:

> *"O livre desenvolvimento da personalidade impõe o asseguramento de uma série de garantias fundamentais no plano constitucional, entre as quais destaca-se o* ***direito à autodeterminação de dados e informações pessoais****. Essas informações podem ser definidas, na compreensão de Schertel, como sinais utilizados na comunicação, que servem para identificar uma pessoa e, quando assumem a forma impressa, transformam-se em dados pessoais".*[9] *(grifos nossos)*

Ingo Sarlet identifica o direito à autodeterminação como a face subjetiva do direito à privacidade, isto porque, neste aspecto, a privacidade opera como "direito de defesa, portanto, como direito à não intervenção por parte do Estado e de terceiros no respectivo âmbito de proteção do direito e, como expressão também da liberdade pessoal, como direito a não ser impedido de levar sua vida privada conforme seu projeto existencial pessoal e de dispor livremente das informações sobre os aspectos que dizem respeito ao domínio da vida pessoal, e que não interferem em direitos de

terceiros".[10] Conclui-se que a autodeterminação informativa é a faculdade do titular dos dados determinar e controlar os seus próprios dados.

Recentemente, o Supremo Tribunal Federal, em decisão histórica, reconheceu a existência da autodeterminação informativa no julgamento da medida cautelar na Ação Direta de Inconstitucionalidade nº 6387[11] contra a Medida Provisória nº 954/2020.[12] A MP determinava que as empresas de telecomunicações compartilhassem os dados como nome, telefone e endereço, de todos os seus usuários com a Fundação Instituto Brasileiro de Geografia e Estatística — IBGE, para fins de pesquisas estatísticas, tendo em vista a situação de emergência de saúde pública decorrente do novo coronavírus.

A ministra Rosa Weber, ao fazer menção ao artigo de Warren e Brandeis, determinou que desde então reconhecia-se que "as mudanças políticas, sociais e econômicas demandam incessantemente o reconhecimento de novos direitos, razão pela qual é necessário, de tempos em tempos, redefinir a exata natureza e extensão da proteção à privacidade do indivíduo". Em sua decisão, a ministra afirmou ainda que "decorrências dos direitos da personalidade, o respeito à privacidade e à autodeterminação informativa foram positivados, no art. 2º, I e II, da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), como fundamentos específicos da disciplina da proteção de dados pessoais". Afastando a constitucionalidade da referida MP, o Tribunal Pleno do STF proferiu decisão histórica ao reconhecer expressamente que a Constituição Federal de 1988 assegura aos brasileiros o direito à autodeterminação informativa, devendo o uso dos dados e informações pessoais ser controlado pelo próprio indivíduo, salvo quando a legislação estritamente determinar.

Paralelamente, ainda temos o direito à proteção de dados que é a possibilidade de cada titular de dados determinar de forma autônoma a utilização que é feita de seus próprios dados pessoais, em conjunto com diversas garantias, para evitar que os dados sejam utilizados de forma prejudicial ao titular ou à coletividade. Tal direito já existia em nosso ordenamento jurídico, mas foi consolidado com a promulgação da Lei Geral de Proteção de Dados (Lei nº 13.709/2018[13])

Inclusive, está em tramitação o Projeto de Emenda Constitucional nº 17/2019[14], cujo objetivo é incluir a proteção de dados pessoais no rol das cláusulas pétreas. Caso a PEC seja aprovada, com a alteração do 5º da Constituição Federal, qualquer outra proposta que tenta abolir a proteção de dados pessoais não será possível, proteção conferida graças à elevação de seu status à cláusula pétrea. Ademais, a proposta fixa competência privativa da União para legislar sobre a proteção e o tratamento de dados pessoais. Tendo o exposto como premissa, passamos a analisar a trajetória da identidade digital.

2. Breve histórico sobre a identidade digital

A internet foi criada em 1969, nos Estados Unidos. Inicialmente conhecida como Arpanet – rede de titularidade do Departamento de Defesa norte-americano -, sua função era interligar laboratórios de pesquisa. A partir de 1982, o uso da Arpanet tornou-se maior no âmbito acadêmico e, com a expansão, começou a ser utilizado o nome "internet". Por quase duas décadas, apenas os meios acadêmico e científico tiveram acesso à rede. Em 1987, pela primeira vez, foi liberado seu uso comercial nos EUA.

Kim Cameron, chefe de arquitetura de identidade e acesso da Microsoft, no artigo *The Laws of Identity*[15], publicado em 2005, afirma em sua introdução que "a internet foi criada sem uma forma para saber a quem ou a que você está se conectando" (tradução livre). Para ele, a internet foi criada sem uma camada de identificação, assim, o sistema de endereçamento da Internet é baseado na identificação de máquinas em uma rede e não de pessoas, e, portanto, não tem como identificar pessoas de forma única.

No mundo físico, os governos emitem e validam a identificação civil através da emissão de documentos físicos, como a carteira de identidade. Assim, o Estado se perpetua, através de suas instituições, como uma figura centralizada e historicamente considerada como confiável, que garante a identidade de cada cidadão. Por outro lado, no mundo digital, mesmo com os avanços obtidos desde 1987, ainda não existe uma forma fácil, segura e aceita pela maioria da população, capaz de provar quem são seus usuários.

O relatório *Picture perfect: A blueprint for digital identity*, publicado em 2016 pela Deloitte, atesta que os sistemas de identidade compartilham aspectos básicos, são eles: "(i) usuários – aqueles que obtêm uma identidade para conseguir realizar transações; (ii) fornecedores de identidade – aqueles que capturam e armazenam os atributos da identidade dos usuários, asseguram a veracidade e chegam a concluir as transações em nome deles; e (iii) os terceiros de confiança – aqueles que atendem aos usuários após a obtenção da identidade com os fornecedores" (tradução livre).

Ademais, a evolução da identidade digital tenta resolver três problemas centrais no âmbito da governança de dados. O primeiro é a segurança, uma vez que a informação precisa ser protegida contra divulgação não intencional. O segundo é o controle, onde objetiva-se que o proprietário da identidade tenha gerência de quem pode ver e acessar seus dados e para que fins. Por último, temos a portabilidade, que permitirá a utilização de dados onde o usuário quiser, sem vinculação a qualquer provedor.

O artigo "A gestão da identidade e seu impacto na economia digital", publicado em 2017 pelo Banco Interamericano de Desenvolvimento, afirma que a "gestão de sistemas de identidade requer um modelo de governança e um modelo de negócio;

um marco legal apropriado e atualizado; a simplificação e padronização de processos e sistemas; o estabelecimento de mecanismos de interoperabilidade que facilitem a coordenação entre os diferentes organismos, e a promoção e coordenação do ecossistema de uso da identidade".[16]

Cristopher Allen[17], em seu artigo *The path to self-sovereign identity*, divide a história da identificação digital em quatro momentos. O autor inicia sua dissertação no modelo centralizado, em que a identidade pertence e é controlada por uma única entidade. Dentro do domínio desta entidade, a identificação funciona perfeitamente, mas não pode ser utilizada em domínio distinto. Desta forma, o usuário deverá criar uma identidade para cada site ou aplicativo que utilizar. A principal característica desse modelo é que os dados de cada usuário são de propriedade da própria entidade. Como consequência, a remoção dos dados da sua base apaga por completo a identidade digital do usuário.

O segundo modelo explicitado por Allen é o federado, que confere um nível de portabilidade quando comparado com o centralizado. Nele, é possível usar a identificação criada em uma entidade em outra. Em um nível mais avançado, os sites e aplicativos poderiam até compartilhar a informação de usuários. Como exemplo, temos o Facebook Login, que permite que usuários utilizem o login e senha criados na rede Facebook para ingresso em outras redes. Por mais que esse modelo permita a portabilidade, os dados continuam sendo titularidade da entidade que o usuário se inscreveu. Com isso, ser desconectado desta entidade inicial acarretará a impossibilidade de uso da rede de terceiros.

Em seguida temos o modelo *user-centric*, onde o usuário controla os seus dados na rede, inclusive, para quem eles serão disponibilizados. O indivíduo cria o seu próprio "armazém de dados" com informações que ele poderá dar permissão de acesso a outras organizações, mantendo um registo à medida que o faz. A identidade centrada no usuário é mais frequentemente manifestada na forma de armazenamento, independente de dados pessoais em um extremo do espectro, e de grandes redes sociais, no outro extremo. No entanto, todo o espectro ainda depende da seleção de um provedor de identidade individual pelo usuário e da concordância com seus contratos de adesão, muitas vezes unilaterais.

Antes de adentrarmos no último modelo, objeto deste trabalho, importante frisar que a quantidade de relações travadas no âmbito digital e a complexidade das mesmas é exponencial. Inclusive, há diversas legislações setoriais que regulam tanto a identificação quanto a relação digital, com fim de conferir segurança da mesma maneira que o mercado confia nos documentos físicos emitidos pelas autoridades públicas. Enquanto na internet criamos uma identidade digital em cada site ou aplicativo que acessamos ou optamos por utilizar serviço de identificação de outros provedores, no mundo físico, a depender do órgão público que teremos

contato, diferentes documentos nacionais nos são solicitados. Assim, possuímos cada vez mais diferentes tipos de identidade e oferecemos os nossos dados a uma quantidade considerável de *players* do mercado.

Isto posto, apresentamos o último modelo: a identificação autossoberana. O surgimento de novas soluções criptográficas mais seguras desencadeou uma nova visão sobre o tema "identidade digital", que, em última análise, poderá solucionar problemas existentes nos ambientes digital e tradicional.

Neste modelo, assim como no *user-centric,* o usuário decide quando e como as informações são compartilhadas. Contudo, ele supera os três elementos acima mencionados, pois permite o controle individual, é seguro e permite total portabilidade. O indivíduo, a quem a identidade pertence por completo, controla e gerencia sua identidade. A existência digital do indivíduo é independente de qualquer organização individual.

A melhor maneira de pensar em identidade autossoberana, é como um registro digital ou recipiente de transações de identidade, que o próprio usuário controla. O fundamento central é o controle pessoal dos dados pelos seus titulares. Para a identidade digital ser realmente autossoberana, a infraestrutura precisa ser um ambiente confiável, e que não pertença ou seja controlada por qualquer organização, mesmo que seja um pequeno grupo de organizações. Por isso, esse modelo, ainda incipiente, encontrou guarida na tecnologia *blockchain*, embora, não necessariamente, limitado a ela. Para uma melhor compreensão do tema, cumpre estabelecer alguns parâmetros sobre a tecnologia *blockchain*.

3. Premissas básicas sobre a tecnologia *Blockchain*

O termo *blockchain* se refere a uma das hipóteses de "tecnologia de registro distribuído" (ou *Distributed Ledger Technology* - DLT, na expressão em inglês). Assim, existem diversas formas de DLT, entre elas a tecnologia *blockchain*. Contudo, é comum que se utilize o termo *"blockchain"* para toda e qualquer DLT, mesmo que ela não envolva, necessariamente, "blocos" *(block)* ou seu encadeamento *("chain").*

A forma mais simples de se entender *blockchain*[18] é imaginar um banco de dados organizado como um livro registro, em que os dados são agrupados em blocos e estes, por sua, vez são encadeados em uma sequência cronológica. Os dados são inseridos na *blockchain* através de técnicas de criptografia, como funções de *hashing*[19]. Tanto os blocos quanto seu encadeamento são construídos utilizando criptografia de dados, sendo que cada bloco contém, em geral: (i) o número do bloco; (ii) os dados armazenados no bloco; (iii) o *hash* do bloco anterior; (ii) o *hash* do próprio bloco.

Por conta deste conteúdo dos blocos, e tendo em vista o modo de funcionamento dos *hashes*, qualquer tentativa de alteração no *hash* de um bloco "b", teria impacto imediato no bloco "b+1", tendo em vista que este último traz nele a informação do

hash anterior e o seu próprio *hash*, o qual é gerado, tomando por base todas as informações nele contidas. Isto leva a concluir que, quanto mais antigo o bloco, mais difícil seria sua alteração, pois todos os blocos sequenciais teriam que ser alterados.

Assim, a estrutura de encadeamento dos blocos, em que cada um deles traz o *hash* do anterior, é um dos principais elementos que assegura a confiabilidade/imutabilidade dos dados, e que tornou a tecnologia tão difundida. Porém, tal segurança somente é possível graças a uma outra característica, esta considerada um dos marcos da tecnologia: a descentralização (ou distribuição, para ser mais abrangente conceitualmente) do processo de consenso/validação das transações registradas.

Todos os nodes[20] que rodam o *software* da *blockchain* mantém uma versão igual da *blockchain* entre si, e mesmo que não tenham "resolvido" o problema matemático e criado um bloco, funcionam como validadores das "soluções" encontradas por terceiros, confirmando, assim, que o novo bloco deve ser mantido na *blockchain*. Tal método de consenso, conhecido como mineração[21], gera uma dificuldade prática enorme para violação da *blockchain*, tendo em vista que seria necessário reunir, em tese, 50%+1 da capacidade computacional dos mineradores para "vencer" a batalha contra os remanescentes e acrescentar um bloco "violado". Isto para alterar apenas o último bloco.

Para alterar um bloco mais antigo, seria ainda mais complicado, pois, como visto, a alteração de um bloco mudaria seu *hash*, com consequências em todos os blocos seguintes. Como a *blockchain* cresce sempre a partir da sua maior ramificação e todas as menores são descartadas neste processo, uma tentativa de alteração, por exemplo, do antepenúltimo bloco, teria que construir um novo penúltimo e um novo último de forma mais "rápida" do que o acréscimo de um novo bloco na *blockchain* original. Este mecanismo previne, entre outros eventos, a ocorrência do *double-spending*[22], dando mais segurança às transações registradas na *blockchain*[23].

De forma didática, as características mais marcantes da *blockchain* são as seguintes: (i) descentralização – já mencionada acima; (ii) eliminação de intermediários –a confiança que antes era depositada no intermediário passa à tecnologia, "eliminando", assim, a sua necessidade; (iii) imutabilidade – informações inseridas na *blockchain* não podem ser modificadas; (iv) irreversibilidade – por ser imutável, uma vez gravada na *blockchain*, a informação é irreversível; (v) segurança – ainda devido à imutabilidade e à descentralização, temos um alto nível de segurança, pois toda informação é gravada de forma definitiva; (vi) transparência – qualquer pessoa pode fazer transações e consultar o histórico de transações da rede sem pedir autorização a ninguém; logo, é facilmente auditável.

Mencionado acima, as informações são inseridas na *blockchain* através da criptografia, de forma que qualquer documento pode ser convertido em um *hash* – longa sequência de letras e números – similar a uma impressão digital. A validação das

informações e a transformação em *hash* possibilitam que as informações ali inseridas sejam compartilhadas e autenticadas sem a revelação das mesmas. Portanto, embora tenha sido criada para dar apoio a um criptoativo, a utilização da tecnologia no setor da identificação permite a criação de uma impressão digital confiável e auditável do documento de identificação.

Para o presente artigo, cumpre ainda diferenciar o que seria o registro *on-chain* do *off-chain*. A *blockchain* usualmente possui um limite sobre o tamanho e quantidade de dados que podem ser armazenados em um único bloco. Além disso, o custo de cada transação na rede pode ser muito custoso. Por fim, existem diversos dados que são confidenciais e sigilosos; logo, registrá-los na *blockchain* pode gerar danos irreversíveis.

Considerando o exposto, há uma divisão entre os dados que são gravados na *blockchain (on-chain records)* e aqueles que são grandes demais para serem armazenados na *blockchain* de modo eficiente, ou que requer a capacidade de ser alterado ou excluído *(off-chain records)*. Portanto, para alguns dados identitários, pode ser interessante fazer o registro fora da rede, e nesta registrar, apenas, a tradução criptográfica do que foi registrado *off-chain*, garantindo a validade e confiabilidade na informação registrada fora da *blockchain*.

A tecnologia *blockchain* proporciona uma maneira transparente, imutável, confiável e auditável de lidar com a identificação de forma transparente e segura. A tecnologia garantirá fundamentos que a identidade autossoberana precisava para sair do mundo teórico, quais sejam: (i) descentralização, ou seja, não pertencer a qualquer organização, governo ou terceiro interessado; (ii) existência por maior tempo que os usuários; (iii) garantia do direito ao esquecimento; e (iv) inclusão.

4. Benefícios da identidade autossoberana

De pronto, cumpre ressaltar que existem ferramentas de identidade do mundo físico no mundo digital, como os certificados digitais emitidos pelas autoridades certificadoras, todavia, estas ainda dependem de um intermediário que atribui confiança ao certificado usado por um indivíduo. Ademais, o serviço não é gratuito e existem, somente, 80 organizações ao redor do mundo que controlam a emissão desses certificados.[24] No Brasil, por exemplo, temos a Infraestrutura de Chaves Públicas Brasileira – ICP-Brasil, que é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão brasileiro através do credenciamento centralizado de autoridades certificadoras, conferido pela Autoridade Certificadora Raiz – AC-Raiz.

O caminho para um modelo de identificação digital sem a dependência de um terceiro intermediário, atualmente, traduz-se na construção de redes distribuídas de confiança, que possam validar as informações produzidas por indivíduos em meios

físicos e digitais. "O conceito de identidade autossoberana refere-se a um modelo em que cada usuário tem total controle sobre seus dados, que podem ser armazenados em carteiras pessoais (semelhantes a carteiras de criptomoedas). Neste contexto, pode-se decidir quando e como as informações são compartilhadas."[25]

Nas palavras de Emily Fry[26] e Elizabeth M. Renieris[27],

> *"a ideia básica por trás da identidade autossoberana é permitir um modelo de gerenciamento de identidade que coloque os indivíduos no centro de suas transações relacionadas à identidade, permitindo-lhes gerenciar uma série de identificadores e informações pessoais, sem depender de qualquer tipo tradicional de autoridade centralizada. Uma escola emergente de SSI se baseia na combinação da tecnologia de registro distribuído e uso de identificadores descentralizados, bem como outros padrões técnicos em desenvolvimento pelo World Wide Web Consortium (WCʒ), e às vezes, também, é conhecida como "identidade descentralizada". [28]*

A identidade digital possui cinco fragilidades centrais: (i) o problema da proximidade – relações a distância possuem um alto risco de fraude identitária; (ii) escalabilidade – sistemas de identificação digitais são baseados em relações comerciais e integrações técnicas para enraizar as autoridades de confiança; (iii) flexibilidade - os sistemas de identidade atuais são rígidos, com esquemas e casos de uso fixos; (iv) privacidade - identificadores compartilhados, como *cookies*, permitem que informações pessoais sejam acumuladas e correlacionadas sem o consentimento qualificado do usuário; (v) consentimento - os sistemas de identidade dependem de identificadores universais, como endereços de e-mail, números de telefone que tornam fácil para terceiros correlacionar o comportamento e manter o controle das pessoas sem sua permissão.[29]

Em teoria, a descentralização e a criptografia resolveriam esses problemas. Ao oferecer mais segurança contra ataques *hackers*, visto a dificuldade para quebrar a criptografia da *blockchain*, supera-se o problema da privacidade e da proximidade. Por sua vez, o usuário, ao ter controle dos seus dados, aplicativos e serviços, somente terão acesso aos dados mínimos e necessários[30], resolvendo o problema do consentimento. Caso o sistema seja adotado por diversas instituições, soluciona-se os problemas da flexibilidade e da escalabilidade.

Ademais, como a tecnologia torna a informação nela gravada imutável, inquestionável e segura, por meio de assinaturas digitais baseadas em criptografia de chave pública. Outra vantagem é a redução dos custos envolvidos no modelo centralizado tradicional de identificação, uma vez que o registro de uma informação só precisará ser feito uma única vez e será válido em todas as instituições. Em adendo, a

identidade digital única, baseada em *blockchain*, também possibilita que os dados sejam sempre atualizados com as informações mais recentes do usuário.

Somente a título de exemplificação, podem ser citados alguns casos que declaram ser uma identidade autossoberana, como a Sovrin, rede de identidade de código aberto pública e permissionada, em que a fundação sem fins lucrativos Sovrin Foundation supervisiona o consenso das transações. Outro exemplo é a uPort, sistema de identidade de código aberto desenvolvido pela ConsenSys, o qual permite o gerenciamento de dados pelos usuários através da plataforma de *blockchain* Ethereum.

Ainda temos a Veres One, *blockchain* pública otimizada para fins de identidade digital, em que o sistema da rede foi projetado para ser autossuficiente com a finalidade de evitar ataques contra a rede e recompensar financeiramente os usuários para garantir sua segurança. No Brasil temos o BlockIoT, é o projeto CPqD (Centro de Pesquisa e Desenvolvimento em Telecomunicações)[32] que tem como objetivo a criação de identificação digital de pessoas e coisas com o uso da *blockchain*[33].

Outro projeto do CPqD, em conjunto com o LIFT — Laboratório de Inovações Financeiras e Tecnológicas, é o FinID — Sistema de Identidade Digital Descentralizada. Além desses, está em curso alguns projetos feitos pela Microsoft, IBM e Deloitte, em conjunto com o governo brasileiro.

Para alguns pesquisadores, "a identidade digital única já é realidade em alguns países como Estônia, Cazaquistão e Índia. Na Estônia, por exemplo, esta identidade unifica o acesso a diversos serviços, como transações bancárias, solicitação de benefícios estatais, declaração de impostos, registros escolares, etc. (Thompson e Yu, 2017)". Importante mencionar que os sistemas desses países não são, necessariamente, baseados em *blockchain* e/ou utilizam tecnologias descentralizadas. Contudo, o uso da tecnologia será viável ao controle pessoal de dados e servirá como prova oficial identitária.

5. Atuais desafios da identidade autossoberana

Por mais que a identidade autossoberana traga inúmeros benefícios, existem gargalos que precisam ser superados. Discutiremos aqui os quatro principais desafios a serem superados, iniciando pela interoperabilidade. A interoperabilidade é "a capacidade de diversos sistemas e organizações trabalharem em conjunto, de modo a garantir que pessoas, organizações e sistemas computacionais interajam para trocar informações de maneira eficaz e eficiente".[34] Enquanto a integração é o processo de conectar dois ou mais sistemas através do uso de uma tecnologia, a interoperabilidade é a comunicação de diferentes redes sem a necessidade de outra tecnologia.

Quando acessamos uma rede utilizando os dados do Facebook, por exemplo, não estamos tratando de uma interoperabilidade e sim de uma integração. Para que a

identidade seja autossoberana é necessário que haja a interoperabilidade entre os sistemas, caso contrário, permanecerá o cenário em que o usuário fornece os mesmos dados múltiplas vezes para diferentes *players*.

Vimos acima que existem diversos projetos em *blockchain* para viabilizar a identidade autossoberana. Para que a interoperabilidade aconteça, é necessário que todos estejam de acordo sobre como a mesma ocorrerá. Dever-se-á ter uma padronização tecnológica ampla, para que o menor esforço seja demandado no momento da elaboração de interfaces, culminando em uma comunicação mais rápida e ágil. Defende-se aqui a adoção de "padrões abertos, ou seja, aqueles que estão publicamente disponíveis e não são controlados por nenhum governo ou corporação, que tornam possível que quaisquer empresas, cidadãos e países se conectem e troquem informações com autonomia".[35]

O segundo aspecto a ser superado é a adesão popular. A tecnologia *blockchain* existe desde 2008; logo, a mesma é nova se comparada com as tradicionais. Mesmo com 12 anos em circulação, é ínfima a parcela da população mundial que possui acesso à tecnologia. Afinal, ainda 46,4% (quarenta e seis vírgula quatro por cento)[36] da população mundial não possui acesso à internet. Portanto, o caminho ainda é longo para a disseminação dessa tecnologia.

Tornar a identidade autossoberana, significa dar ao público o controle de suas informações, porém, ao mesmo tempo, é aumentar a responsabilidade pessoal dos titulares para a atualização e pertinência de seus dados. Para que uma tecnologia seja aceita e utilizada, esta tem que provar para o usuário que o seu uso melhorará a sua performance em uma função específica, e a sua interface precisa ser fácil. Além disso, fatores externos, como a adesão em massa, gera um efeito comportamental positivo para a consolidação de uma tecnologia. Assim, por mais que o sistema seja interessante, esses fatores poderão afastar a sua real aplicabilidade.

Neste sentido, Adrian Doerk, no texto *The growth factors of self-sovereign identity*, afirma que um dos aspectos críticos a serem considerados é que "se não houver uma educação massiva e prestadores de serviços disponíveis para sanar dúvidas, educar e assegurar a identidade digital, não veremos nenhum grau significativo de adoção por parte do usuário".[37] Outro ponto levantado pelo autor é a obtenção de confiança do público na tecnologia, afinal, como toda tecnologia, é possível que a identidade seja abusada para fins de vigilância.

Pode levar muitos anos para que ocorra a adoção da identidade autossoberana e, quando a população passar a confiar e a usá-la, poderá ter surgido uma nova tecnologia que deixará a SSI baseada em *blockchain* defasada.[38] Por fim, a tecnologia deverá assegurar que pessoas com deficiência consigam utilizá-la, afinal, o direito à identidade é um direito constitucional de todo cidadão, tanto no Brasil quanto em outros países.

Em seguida, temos a portabilidade, desafio que emerge da proteção de dados. Nos termos do artigo 18, inciso V, da LGPD, o titular de dados tem o direito a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa. Por mais que os defensores da SSI indiquem a possibilidade técnica da portabilidade, ainda é incipiente o debate sobre a mitigação de riscos, alocação de responsabilidade ou mecanismos de aplicação ou reparação.

Outro aspecto da proteção de dados é o direito ao esquecimento, direito de eliminação de dados e direito de retificação. Acima, vimos a diferença do registro *on-chain* e *off-chain*. Quando as informações identitárias são registradas diretamente na *blockchain*, devido a sua característica de imutabilidade, o titular dos dados não conseguirá retificar ou eliminar os dados registrados.

Por mais que existam plataformas *blockchain* que aleguem ser possível a modificação, isso sugere um afastamento da plataforma do ideal criado acerca da própria tecnologia, em que o mecanismo de encadeamento de blocos garantiria imutabilidade e, por consequência, confiabilidade. O que é possível tecnicamente é o registro da informação atualizada no bloco posterior, informando que o registro do bloco "X" foi de um dado errado. O problema poderá ser superado, caso exista um sistema de governança *on-chain* que permita a modificação segura do bloco questionado.

Note que a responsabilidade da veracidade e do registro dos dados é transferido ao titular, portanto, a cobertura conferida pelas leis de proteção de dados existentes poderá ser questionada. Afinal, quem será o responsável pela plataforma ou pela demora da retificação ou remoção? Questões ainda em aberto neste modelo.

Por fim, também há problemas quando o registro das informações é feito *off-chain*. Isto porque, por mais que os problemas de eliminação e modificação sejam superados com mais facilidade, voltamos ao fator humano. Portanto, os problemas atuais da identificação no mundo físico transportar-se-ão para o digital. Os grandes bancos de dados *off-chain* continuarão suscetíveis a ataques cibernéticos, fraudes e todos os problemas que a própria teoria de identidade digital tenta superar.

Conclusão

É notório que a evolução do debate sobre o modelo identitário ideal é necessário e atemporal, visto que as inovações tecnológicas tendem a modificar a visão que a sociedade constrói acerca de um conceito. Com a atualização do conceito de privacidade e a sobressalência da autodeterminação informativa, o debate sobre a identidade autossoberana não poderia ser mais pertinente.

As características inerentes da tecnologia *blockchain* – descentralização, eliminação de intermediários, imutabilidade, irreversibilidade, segurança e transparência – retiram da teoria a SSI, na medida em que, ao eliminar o intermediário de modo seguro e auditável, transfere ao titular dos dados a capacidade de autodeterminar-se.

Vimos, ao longo do presente artigo, que as cinco fragilidades centrais da identidade digital – proximidade, escalabilidade, flexibilidade, privacidade e consentimento – podem ser superadas com a adesão da SSI.

Contudo, é necessário solucionar aspectos pendentes, quais sejam: interoperabilidade; proteção de dados, com foco no direito ao esquecimento quando falamos de *on-chain records*; fator humano, e, principalmente, a adesão popular para que o modelo funcione. O debate acerca da identidade autossoberana não podia ser mais contemporâneo e necessário no contexto brasileiro, principalmente com a promulgação de atos normativos que permeiam o assunto - como a Lei Geral de Proteção de Dados e o Decreto nº 10.278, de 18 de março de 2020. Contudo, precisamos ultrapassar a exposição dos benefícios e adentrar na discussão sobre os pontos em aberto para melhorar a construção do sistema.

Notas

1. DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro*. São Paulo: Saraiva, 2007, p. 119-120.

2. PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital*. Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A3o-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020.

3. PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital*. Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A3o-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020.

4. Para os fins deste artigo, consideramos que ainda não há tecnologia que viole a criptografia da *blockchain*.

5. WARREN, Samuel D.; BRANDEIS, L. D., "The Right to Privacy". Harvard Law Review ,vol. IV, 15 de dezembro de 1890.

6. LAFER, Celso. *A reconstrução dos direitos humanos*. São Paulo: Companhia das Letras, 2003, p. 240.

7. TEPEDINO, Gustavo; BARBOZA, Heloisa Helena; MORAES, Maria Celina Bodin de. *Código Civil Interpretado: Conforme a Constituição da República*. Rio de Janeiro: Renovar, 2014, 3.ed. p. 60-61.

8. PEREIRA, Caio Mario da Silva. *Instituições de Direito Civil - Volume I*. 30ª Edição. Rio de Janeiro: Forense, 2017. p. 216.

9. COÊLHO, Marcus Vinicius Furtado. *O direito à proteção de dados e a tutela da autodeterminação informativa*. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa#_ftnref3>. Acesso em: 03.07.2020.

10. SARLET, Info Wolfgang; MARINONI, Luis Guilherme; MITIDIERO, Daniel. Curso de Direito Constitucional. 8ª Edição. São Paulo: Saraiva Educação, 2019, p. 576.

11. BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.387/DF – Distrito Federal. Relatora: Ministra Rosa Weber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf> Acesso em: 15.07.2020.

12. BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Diário Oficial da União, Atos do Poder Executivo, Brasília, DF, 17.04.2020. Seção 1 - Extra, p. 1.Disponível em: <http://www.in.gov.br/web/dou/-/medida-provisoria-n-954-de-17-de-abril-de-2020-253004955> Acesso em: 15.07.2020.

13. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Atos do Poder Legislativo, Brasília, DF, 15.08.2018. Seção 1, p. 59.Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/KujrwoTZC2Mb/content/id/36849373/do-1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337> Acesso em: 15.07.2020.

14. BRASIL. Proposta de Emenda à Constituição nº 17, de 2019. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757> Acesso em: 15.07.2020.

15. CAMERON, Kim. *The Laws of Identity*. 2005. Disponível em: <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>. Último acesso em: 03.06.2020.

16. PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital*. Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A3o-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020

17. Christopher Allen é um desenvolvedor em blockchain e de identidade digital, pioneiro na criptografia da internet e co-autor do "TLS Security Standard".

18. Para esta explicação, consideramos a blockchain do Bitcoin.

19. A função Hash (Resumo) é qualquer algoritmo que mapeie dados grandes e de tamanho variável para pequenos dados de tamanho fixo. Por esse motivo, as funções Hash são conhecidas por resumirem o dado.

20. Na infraestrutura da *blockchain*, os nodes (ou nós) são os computadores responsáveis pelo consenso sobre uma transação em tempo real, contendo cópias dos registros autenticados distribuídos entre eles.

21. A depender a *blockchain* utilizada a forma de validação pode ser diferente.

22. O *double-spending* refere-se a um cenário em que alguém consegue utilizar os mesmos fundos mais de uma vez.

23. Consideramos a *blockchain* pública.

24. KONOPACKI, Marco. *Blockchain e identidades digitais: caminhos para uma nova democracia.* ITS Rio. 2018. Disponível em: <https://feed.itsrio.org/blockchain-e-identidades-digitais-caminhos-para-uma-nova-democracia-7719b8ae-5doe> Último acesso em: 01.07.2020.

25. Binance Academy. *Casos de Uso Blockchain:* Identidade Digital. 2020. Disponível em: <https://academy.binance.com/pt/blockchain/blockchain--use-cases-digital-identity> Último acesso em: 01.07.2020.

26. CEO da Digital Trust na MATTR, empresa sediada na Nova Zelândia que desenvolve padrões abertos, infra-estrutura técnica e software voltado a identificação digital.

27. Fundadora e CEO da HACKYLAWYER, especializada em direito e engenharia de políticas. Advogada especialista em privacidade (CIPP/E, CIPP/US), em identidade e pesquisadora do Berkman Klein Center for Internet & Society da Universidade de Harvard, onde pesquisa estruturas de governança de dados para a era digital.

28. FRY, REINIERIS. *SSI? What we really need is full data portability*. 2020. Disponível em: <https://womeninidentity.org/2020/03/31/data-portability/> Último acesso em: 07.07.2020.

29. WINDLEY, Philip. *How blockchain makes self-sovereign identities possible.* Computer World. 2018. Disponível em: <https://www.computerworld.com/article/3244128/how-blockchain-makes-self-sovereign-identities-possible.html> Último acesso em: 07.07.2020.

30. LGPD. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;

VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

31. Na criptografia de chave pública ou criptografia assimétrica é formada por uma chave pública utilizada para cifrar o conteúdo e por uma chave privada utilizada para decifrar o texto cifrado. Nas assinaturas digitais, a criptografia assimétrica ocorre quando a chave privada é utilizada para codificar o conteúdo e a respectiva chave pública para decifrar a mensagem criptografada, obtendo, assim, a autenticidade.

32. Centro de pesquisa brasileiro focado na inovação em tecnologias da informação e comunicação. Ele atua na pesquisa, desenvolvimento e suporte de diversos setores, como o da administração pública e financeiro

33. AUGUSTO, Thaís. *CPqD quer utilizar o block-chain para dar mais segurança à identidade digital.* Canal Tech. 2019. Disponível em: <https://canaltech.com.br/blockchain/cpqd-quer-utilizar-o-blockchain-para-dar-mais-seguranca-a--identidade-digital-136101/I> Último acesso em: 08.07.2020.

34. MELLO, Ana Paula Pessoa; MESQUITA, Hudson; VIEIRA, Carlos Eduardo. *Introdução à Interoperabilidade.* Escola Nacional de Administração Pública. 2015. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/2399/1/M%C3%B3dulo_1_EPING.pdf> Último acesso em: 15.07.2020.

35. MELLO, Ana Paula Pessoa; MESQUITA, Hudson; VIEIRA, Carlos Eduardo. Introdução à Interoperabilidade. Escola Nacional de Administração Pública. 2015. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/2399/1/M%C3%B3dulo_1_EPING.pdf> Último acesso em: 15.07.2020.

36. *Estudo da ONU revela que mundo tem abismo digital de gênero.* ONU News. 2019. Disponível em: <https://news.un.org/pt/story/2019/11/1693711#:~:-text=O%20uso%20da%20Internet%20continua,popula%C3%A7%C3%A3o%20de%20todos%200%20mundo.> Último acesso em: 15.07.2020.

37. DOERK, Adrian. *The growth factors of self--sovereign identity*. Medium. 2020. Disponível em: <https://medium.com/@SSI_Ambassador/the-growth-factors-of-self-sovereign-identity--33aa3cc17ce7> Último acesso em: 15.07.2020.

38. WILSON, Chuck. *O papel do blockchain em um ecossistema de identificação em franca evolução.* Valid. 2018. Disponível em: <https://valid.com/pt-br/blockchainid_por/> Último acesso em: 15.07.2020.

Bibiografia

ALLEN, Christopher. *The path to self-sovereign identity*. Publicado em 25.04.2016. Disponível em: <http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.> Último acesso em: 04.02.2020.

ALLESSIE, David; SOBOLEWSKI, Maciej; VACCARI, Lorenzino. *Blockchain for digital government.* 2019. Disponível em: https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/blockchain-digital-government. Último acesso em: 10.03.2020.

AUGUSTO, Thaís. *CPqD quer utilizar o blockchain para dar mais segurança à identidade digital.* Canal Tech. 2019. Disponível em: <https://canaltech.com.br/blockchain/cpqd-quer-utilizar-o-blockchain-para-dar-mais-seguranca-a-identidade-digital-136101/I> Último acesso em: 08.07.2020.

Berryhill, J., T. Bourgery and A. Hanson (2018), *"Blockchains Unchained: Blockchain Technology and its Use in the Public Sector"*, OECD Working Papers on Public Governance, No. 28, OECD Publishing, Paris. Disponível em: <https://doi.org/10.1787/3c32c429-en.>

Binance Academy. *Casos de Uso Blockchain: Identidade Digital.* 2020. Disponível em: <https://academy.binance.com/pt/blockchain/blockchain-use-cases-digital-identity> Último acesso em: 01.07.2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Atos do Poder Legislativo, Brasília, DF, 15.08.2018. Seção 1, p. 59. Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/KujrwoTZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-agosto-de-2018-36849337> Último acesso em: 15.07.2020.

BRASIL. Medida Provisória nº 954, de 17 de abril de 2020. Diário Oficial da União, Atos do Poder Executivo, Brasília, DF, 17.04.2020. Seção 1 - Extra, p. 1.Disponível em: <http://www.in.gov.br/web/dou/-/medida-provisoria-n-954-de-17-de-abril-de-2020-253004955> Último acesso em: 15.07.2020.

BRASIL. Proposta de Emenda à Constituição nº 17, de 2019. Câmara dos Deputados. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2210757> Último acesso em: 15.07.2020.

BRASIL. Supremo Tribunal Federal. Ação direta de inconstitucionalidade nº 6.387/DF – Distrito Federal. Relatora: Ministra Rosa Weber. Disponível em: <http://www.stf.jus.br/arquivo/cms/noticiaNoticiaStf/anexo/ADI6387MC.pdf> Último acesso em: 15.07.2020.

CAMERON, Kim. *The Laws of Identity*. 2005. Disponível em: <https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf>. Último acesso em: 03.06.2020.

COÊLHO, Marcus Vinicius Furtado. *O direito à proteção de dados e a tutela da autodeterminação informativa*. 2020. Disponível em: <https://www.conjur.com.br/2020-jun-28/constituicao-direito-protecao-dados-tutela-autodeterminacao-informativa#_ftnref3>. Último acesso em: 03.07.2020.

DINIZ, Maria Helena. *Curso de Direito Civil Brasileiro*. São Paulo: Saraiva, 2007, p. 119-120.

DOERK, Adrian. *The growth factors of self-sovereign identity*. Medium. 2020. Disponível em: <https://medium.com/@SSI_Ambassador/the-growth-factors-of-self-sovereign-identity-33aa3cc17ce7> Último acesso em: 15.07.2020.

DONEDA, Danilo; KANASHIRO Marta. *O novo sistema brasileiro de identificação - traços exclusivos de uma transformação geral.* Politics. Setembro 2012. Disponível em: <https://politics.org.br/edicoes/o-novo-sistema-brasileiro-de-identifica%C3%A7%C3%A3o-tra%C3%A7os-exclusivos-de-uma-transforma%C3%A7%C3%A3o-geral>. Acesso em 15 out. 2019.

Estudo da ONU revela que mundo tem abismo digital de gênero. ONU News. 2019. Disponível em: <https://news.un.org/pt/story/2019/11/1693711#:~:text=O%20uso%20da%20Internet%20continua,popula%C3%A7%C3%A3o%20de%20todos%200%20mundo.> Último acesso em: 15.07.2020.

FAFT, *Public consultation on FATF draft guidance on digital identity.* 2019. Disponível em: <https://www.fatf-gafi.org/publications/fatfrecommendations/documents/consultation-digital-id-guidance.html.>

FRY, REINIERIS. *SSI? What we really need is full data portability.* 2020. Disponível em: <https://womeninidentity.org/2020/03/31/data-portability/> Último acesso em: 07.07.2020.

KANG, Margareth; DOS SANTOS, Maike Wille; DONEDA, Danilo. *Políticas de Identidade na era digital e o registro civil nacional.* 2016. Disponível em <http://opiniaopublica.ufmg.br/site/files/artigo/4-Margareth-Kang.pdf>. Último acesso em 15.10.2019.

KONOPACKI, Marco. *Blockchain e identidades digitais: caminhos para uma nova democracia.* ITS Rio. 2018. Disponível em: <https://feed.itsrio.org/blockchain-e-identidades-digitais-caminhos--para-uma-nova-democracia-7719b8ae5doe> Último acesso em: 01.07.2020.

LAFER, Celso. *A reconstrução dos direitos humanos.* São Paulo: Companhia das Letras, 2003, p. 240.

Learning Machine. *Digital Identity.* Disponível em: <https://www.learningmachine.com/digital-identity/> Último acesso em 15.10.2019.

MELEIRO, Juan. *Identidade Auto-Soberana.* 2018. Disponível em: <https://medium.com/mosaicouniversity/identidade-auto-soberana-parte--1-35f3013da8e7> Último acesso em 15.10.2019.

MELLO, Ana Paula Pessoa; MESQUITA, Hudson; VIEIRA, Carlos Eduardo. *Introdução à Interoperabilidade.* Escola Nacional de Administração Pública. 2015. Disponível em: <https://repositorio.enap.gov.br/bitstream/1/2399/1/M%C3%B3dulo_1_EPING.pdf> Último acesso em: 15.07.2020.

PAREJA, Alejandro; PEDAK, Mari; GÓMEZ, Carlos; BARROS, Alejandro. *A gestão da identidade e seu impacto na economia digital.* Banco Interamericano de Desenvolvimento. 2017. Disponível em: <https://publications.iadb.org/publications/portuguese/document/A-gest%C3%A30-da-identidade-e-seu-impacto-na-economia-digital.pdf> Último acesso em: 26.06.2020.

PEREIRA, Caio Mario da Silva. *Instituições de Direito Civil - Volume I.* 30ª Edição. Rio de Janeiro: Forense, 2017. p. 216.

SARLET, Info Wolfgang; MARINONI, Luis Guilherme; MITIDIERO, Daniel. *Curso de Direito Constitucional. 8ª Edição.* São Paulo: Saraiva Educação, 2019, p. 576.

SOVRIN FOUNDATION (2017). *The inevitable Rise of Self-Sovereign Identity.* Disponível em: <https://sovrin.org/wp-content/uploads/2018/03/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.> Acesso em: 10.04.2020.

SOVRIN FOUNDATION (2018). *Sovrin: A Protocol and Token for Self-Sovereign Identity and Decentralized Trus.* Disponível em: <https://sovrin.org/wp-content/uploads/2018/03/Sovrin-Protocol-and-Token-White-Paper.pdf>. Acesso em: 1.04.2020

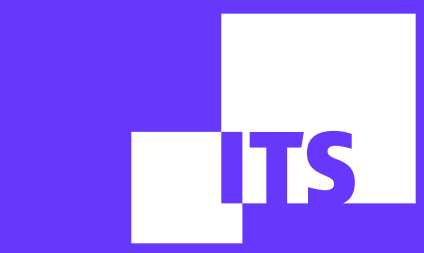
TEPEDINO, Gustavo; BARBOZA, Heloisa Helena; MORAES, Maria Celina Bodin de. *Código Civil Interpretado: Conforme a Constituição da República.* Rio de Janeiro: Renovar, 2014, 3.ed. p. 60-61.

Wang F and De Filippi P (2020). *Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion.* Disponível em <https://www.frontiersin.org/articles/10.3389/fbloc.2019.00028/full> Último acesso em: 15.07.2020.

WARREN, Samuel D.; BRANDEIS, L. D., *"The Right to Privacy"*. Harvard Law Review ,vol. IV, 15 de dezembro de 1890.

WILSON, Chuck. *O papel do blockchain em um ecossistema de identificação em franca evolução.* Valid. 2018. Disponível em: <https://valid.com/pt-br/blockchainid_por/> Último acesso em: 15.07.2020.

WINDLEY, Philip. *How blockchain makes self-sovereign identities possible.* Computer World. 2018. Disponível em: <https://www.computerworld.com/article/3244128/how-blockchain-makes--self-sovereign-identities-possible.html> Último acesso em: 07.07.2020.



Acesse nossas redes

itsrio.org