UNIVERSIDADE FEDERAL DA BAHIA
FACULDADE DE DIREITO
GRADUAÇÃO EM DIREITO

LIPE SCHKRAB ALVES

HÁBITOS DE NAVEGAÇÃO E VIOLAÇÕES CONSTITUCIONAIS NA ERA DOS ALGORITMOS

Salvador

2019

LIPE SCHKRAB ALVES

HÁBITOS DE NAVEGAÇÃO E VIOLAÇÕES CONSTITUCIONAIS NA ERA DOS ALGORITMOS

Trabalho de Conclusão de Curso de graduação em Direito pela Faculdade de Direito da Universidade Federal da Bahia como requisito para obtenção do grau de Bacharel em Direito.
Orientador: Prof. Dr. João Glicério de Oliveira Filho

Salvador
2019

LIPE SCHKRAB ALVES

HÁBITOS DE NAVEGAÇÃO E VIOLAÇÕES CONSTITUCIONAIS NA ERA DOS ALGORITMOS

Trabalho de Conclusão de Curso apresentado ao Curso de Direito da Faculdade de Direito da Universidade Federal da Bahia, como requisito parcial para obtenção do grau de bacharel em Direito.
Orientador: Prof. João Glicério de Oliveira Filho

Aprovado em _____ de _____ de 2019

João Glicério de Oliveira Filho (Orientador)_____
Doutor em Direito pela Universidade Federal da Bahia.

Bruno César de Carvalho Coêlho _____
Especialista em Direito Processual Civil pela Fundação Faculdade de Direito da Bahia/UFBA. Mestre em Políticas Sociais e Cidadania pela Universidade Católica do Salvador/UCSal

Lara Britto de Almeida Domingues Neves _____
Mestre em Direito dos Negócios pela Fundação Getúlio Vargas – Escola de Direito de São Paulo

AGRADECIMENTOS

Agradeço ao meu pai, Guilherme Barbosa Alves, pelo vigoroso e inestimável suporte durante todo o percurso, do primeiro ao último dia.

Agradeço a minha mãe, Selma Schkrab Alves, pelos ensinamentos diários sobre grande força emocional.

A meu irmão, Igor Schkrab Alves, pelo apoio moral e por se mostrar presente nos momentos difíceis.

A meus companheiros de jornada Victor Ferreira, Lara Freire, Rafael Fortunato, Bruno Freire, Rafael Quina, Guilherme Campos, Tomás Sampaio; amigos insubstituíveis com quem tenho o privilégio de compartilhar meus dias e que permanecerão, em mim, imortais.

A meus amigos e colegas de faculdade, sobretudo as amizades cultivadas durante meu tempo no subnúcleo de Direito Ambiental no NCI. Antônio Castro, Mariana Choratto, Ruy Mello, Laísa Branco, Isabela Dias, Ana Luísa e todos os demais; indivíduos brilhantes com quem construí memórias de meus melhores dias na faculdade.

A meu orientador, Prof. João Glicério de Oliveira Filho, por demonstrar excepcional zelo e competência como educador.

A todos os professores que fizeram parte da minha experiência acadêmica, antes e durante a faculdade.

E também a todos os outros que, de uma forma ou de outra, contribuíram para quem eu fui, sou e serei.

Meu humilde obrigado.

ALVES, Lipe Schkrab. **Hábitos de Navegação e Violações Constitucionais na Era dos Algoritmos**. 63 fls. Monografia (Graduação) – Faculdade de Direito, Universidade Federal da Bahia, Salvador, 2019.

RESUMO

A presente monografia tem como objetivo uma análise crítica do uso de dados de navegação dos usuários da internet por empresas. O estudo é contextualizado por um plano de fundo jurídico que permite a exploração dos hábitos de navegação por empresas que, alimentando algoritmos com dados colhidos muitas vezes sem o conhecimento dos usuários, maximizam seus lucros oferecendo serviços meticulosamente direcionados. As previsões projetadas pela programação de algoritmos possibilitaram o surgimento e o aperfeiçoamento de serviços de grande conveniência que rapidamente conquistaram popularidade, ao passo que criaram novos paradigmas que desafiam a legislação atual sobre o tema. O projeto tem um âmbito exploratório, ambicionando a criação de familiaridade com os riscos representados pela internet aos direitos fundamentais, cotejando os erros e acertos da legislação no enfrentamento destas ameaças. Aos dados coletados pela pesquisa será aplicada abordagem qualitativa. A técnica de coleta de dados consistiu de uma ostensiva pesquisa bibliográfica, abrangendo livros, artigos e periódicos, sem prejuízo do emprego de meios digitais para obtenção de informações pertinentes.

Palavras-chave: Marco Civil da Internet, Lei Geral de Proteção de Dados, Direitos Fundamentais, Algoritmos, Direito Digital

ALVES, Lipe Schkrab. **Internet Navigation Habits and Constitutional Violations in the Age of Algorithms**. 63 pages. Monograph (Bachelor) – Law Faculty, Federal University of Bahia, Salvador, 2019.

ABSTRACT

This monograph aims to present a critical rundown on the applications of user data by tech companies. Insubstantial legislation on the matter sets the stage for exploits on user navigation habits by big tech companies that feed algorithms with data gathered from thousands of non-consenting individuals. These companies maximize their profits by offering goods and services to audiences that have been previously scanned with algorithms that can pinpoint their interests and tastes. Efficient and precise estimations made by these *softwar*es paved the way for the creation of new services as well as the improvement of older ones, which has brought a great deal of comfort to everyday life. In turn, however, these softwares have set new paradigms that challenge the current legislation with problems that may require new legal solutions. This project aims to explore the matter while also creating familiarity with the risks implied by the internet towards fundamental rights, which requires careful consideration of the positives and negatives of current laws. Qualitative approach will be given to data collected for this research. Data gathering techniques have consisted of bibliographic research that included books and articles while also using other digital means to obtain relevant information.

Key-words: Marco Civil da Internet, Lei Geral de Proteção de Dados, Fundamental Rights, Algorithms, Digital Law

SUMÁRIO

1. INTRODUÇÃO

Os usos da internet nos rodeiam e cercam-nos de todos os lados. Em troca, mergulhamos de cabeça na nova “era dos algoritmos”; fazemos uso constante de aplicativos, *sites*, mídias sociais e outras aplicações de rede que determinaram o surgimento de novos hábitos, novas técnicas, novos problemas.

A funcionalidade de diversas aplicações da internet está condicionada ao emprego de “super algoritmos” capazes de realizar o tratamento de um volume descomunal de dados pessoais, estes que são coletados, muitas vezes, sem consentimento de milhões de usuários. O equilíbrio entre a proteção de dados pessoais e a aplicação de novas tecnologias que beneficiam a sociedade é tópico de grande relevância para o cenário jurídico de hoje.

Os usos da internet no ordenamento pátrio restam disciplinados pela Lei n. 12.965/2014, o Marco Civil da Internet. O indigitado diploma normativo contribui não apenas para a fixação de princípios atinentes ao direito digital, como também estabelece direitos e deveres dos atores envolvidos no acesso à rede e disponibilização de serviços *online*, inclusive contribuindo para o estabelecimento de critérios para a responsabilização criminal de eventuais crimes cometidos na rede.

Outro corpo normativo relevante a essa monografia é a Lei Geral de Proteção de Dados (LGDP), Lei nº 13.709/2018, responsável pela disciplina legal dirigida especificamente ao tratamento de dados e amplamente inspirada pela legislação europeia a respeito do tema, mormente a General Data Protection Regulation (GDPR). A LGDP impõe sobre empresas que coletam dados no país uma série de obrigações e limites, fixando uma série de critérios necessários à legitimação do tratamento de dados e combatendo o excesso de poderes que essas empresas detém no acesso de dados pessoais em bancos de dados com milhões de usuários.

Esta monografia ambiciona uma análise crítica dos desdobramentos observados pelas aplicações da internet sobre direitos fundamentais, pontuando ameças representadas por diversas tecnologias de comunicação e informação e demonstrando, sempre que possível, como elas atacam os direitos fundamentais tratados neste trabalho.

Dada a complexidade do tema, escolhas difíceis foram tomadas na delimitação dos direitos fundamentais trabalhados. Optou-se por uma análise de alguns, mas não todos, direitos fundamentais particularmente ameaçados pelos usos das tecnologias de informação, vez que o esgotamento do tema se faz impossível ante o escopo do presente trabalho.

Direitos fundamentais como o direito à vida, à liberdade, ou à propriedade, entre outros, foram deixados de lado seja porque não foram compreendidos como particularmente ameaçados pela conjuntura atual, senão a nível reflexo, seja porque a complexidade exigida para o tratamento destes direitos traria embaraços à entrega tempestiva desta monografia.

Optou-se pela divisão do trabalho em três capítulos, já descontadas a introdução e a conclusão. O segundo capítulo destina-se à colocação do problema abordado, indicando os aspectos e características da sociedade da informação no que tange o surgimento de novos hábitos e, principalmente, dos novos negócios envolvendo a mercantilização de hábitos de navegação através da venda de dados coletados de usuários da internet. No terceiro capítulo, o tratamento jurídico das questões atinentes ao direito digital é abordado, oportunidade em que serão discutidos princípios e seus reflexos, bem como serão tratados com mais vagar as ofensas constitucionais consumadas através do “mercado de informações”. Finalmente, o quarto capítulo destina-se a uma análise tanto preditiva quanto contemplativa das aplicações de rede, indicando experiências estrangeiras de aplicações produtivas das tecnologias de comunicação – principalmente no setor público – e, sempre que possível, contextualizando a introdução dessas novas tecnologias no cenário brasileiro, levando em consideração as dificuldades de acesso à rede no Brasil, bem como outras questões próprias à realidade fática observada no país.

Malgrado as críticas tecidas contra as violações constitucionais que exsurgem da fé cega em interpretações extraídas de bancos de dados por intermédio de algoritmos ou dos desdobramentos não regulados de aplicações de rede, a monografia pretende também abrir espaço para o debate sobre os bons usos e práticas da internet, indicando, sempre que possível, experiências de sucesso na implementação de tecnologias de comunicação e informação, bem como propondo,

nos casos em que a implementação cobra custos na forma de direitos constitucionalmente estabelecidos, soluções para o saneamento das violações perpetradas.

2. HÁBITOS DE NAVEGAÇÃO E A MERCANTILIZAÇÃO DAS PREFERÊNCIAS

Em tempos onde a intenção por trás de cada clique diz tanto sobre o indivíduo do outro lado da tela, nenhum acesso na internet passa despercebido. Rastros deixados no acesso a *sites* ou uso de aplicativos geram dados explorados por empresas que fazem lucrativos negócios em cima dos hábitos de navegação de centenas de milhares de usuários da internet.

2.1. A ERA DOS ALGORITMOS

A capacidade de aprender, notável trunfo evolutivo do *Homo sapiens* em sua extensa evolução biológica, proveu à humanidade uma miríade de soluções para problemas das mais diversas complexidades. A história das civilizações humanas confunde-se, em muitos momentos, com a história de suas soluções tecnológicas para superação de obstáculos naturais. Nas palavras de Milton Santos:

> O desenvolvimento da história vai de par com o desenvolvimento das técnicas. Kant dizia que a história é um progresso sem fim; acrescentemos que é também um progresso sem fim das técnicas. A cada evolução técnica, uma nova etapa histórica se torna possível.[1]

Em seu processo de adaptação ao meio em que vive, a humanidade acumulou vitórias sobre entraves de diversas naturezas, superando obstáculos opostos pela topografia, hidrografia, vegetação e outros elementos naturais.

Estas vitórias sobre o meio ambiente costumam ser inseparavelmente associadas a descobertas de técnicas e invenções capazes de suplantar adversidades outrora insuperáveis, revolucionando, passo a passo, diferentes instâncias da experiência humana na Terra. A invenção da roda, instrumentalizada de maneira versátil em diversos ramos da produção; a domesticação das plantas, responsável pelo abandono da vida nômade e pela revolução neolítica; a descoberta

1 SANTOS, Milton. Por uma outra globalização: do pensamento único à consciência universal. 10. ed. Rio de Janeiro: Record, 2003. p. 24

da penicilina, importante passo no tratamento de infecções; eventos como esses, ainda que episódicos, têm em comum o fato de serem divisores de águas na maneira com que o homem interagiu com o meio que o rodeia.

Precisamente pela relevância destes episódios é que, dentre os diversos campos do saber, talvez destaque-se de maneira particularmente singular a História; senão pela coragem de se incumbir da sisífica tarefa de registro e estudo das interações humanas, tentando delas extrair ensinamentos, certamente por abrir os horizontes do conhecimento ao se voltar para uma contemplação dos passos traçados pela humanidade no curso de sua inusitada existência.

Neste sentido, pode-se dizer que a perspectiva histórica ganha valor ao atribuir sentido aos eventos que revolucionaram a interação homem-ambiente, posto que elas raramente advém do mero acaso e, em geral, se inserem em um contexto maior que determina sua ocorrência. A título de exemplo: embora a concepção do "planeta esférico" já fosse amplamente divulgada àquela época, a oportunidade para produção de uma evidência fotográfica amplamente divulgada na imprensa só foi possibilitada no contexto de uma corrida espacial e de influência entre as duas grandes potências da época, os EUA e a União Soviética. A primeira fotografia do planeta Terra, assim, foi tirada a bordo da Apollo 17 enquanto abandonava a órbita terrestre em direção à Lua, comprovando que o planeta Terra tem o formato de um elipsoide de revolução[2].

Dessarte, a leitura dos avanços nos marcos tecnológicos aliada a uma contextualização socioeconômica de suas implementações culmina na histórica tarefa de separação e classificação em fases da história da humanidade. Emprega-se o termo "Idade Contemporânea" para delimitar, no tempo, um certo conjunto especificado de eventos e condições que assinalam as civilizações atuais. A cada era histórica são atribuídos conjuntos de condições que são, em geral, facilmente distinguíveis, e embora possam existir divergências acadêmicas quanto aos eventos que formalmente deflagram e encerram as fases históricas que a História convencionou delimitar, em geral os aspectos característicos desta ou das demais épocas são consensualmente aceitos.

---

2 NATURAL GEOGRAPHIC. Grandes Marcos da Fotografia no Espaço. Disponível em: <https://www.natgeo.pt/photography/2018/02/grandes-marcos-da-fotografia-no-espaco?image=6428 > Acesso em: 20 out. 2019.

O progresso das ciências, sobretudo daquelas relacionadas à produção de novas tecnologias que possibilitam uma facilitação da árdua tarefa de coleta, armazenamento e transferência de dados, possibilitou o surgimento de um novo estilo de vida com base nas trocas quase imediatas de quantidades massivas de informação entre diferentes pontos do planeta.

Quando Gilberto Gil canta, em Parabolicamará, *"Antes mundo era pequeno / porque Terra era grande / hoje mundo é muito grande / porque Terra é pequena"*, está se referindo ao desmonte de uma realidade ultrapassada onde as limitações físicas determinavam o distanciamento das pessoas. O advento da internet revolucionou as possibilidades de comunicação e, tão logo se popularizou, começou a tecer uma nova realidade socioeconômica.

A banalização do acesso a cada vez mais dispositivos conectados à rede possibilitou o surgimento de um novo estilo de vida com características únicas, hábitos novos e, certamente, novos problemas. Outrora, celebrava-se o triunfo tecnológico responsável pela fotografia do planeta e a constatação de que as previsões matemáticas feitas da curvatura da Terra estavam corretas; hoje, a popularização de um conjunto de percepções equivocadas da realidade, entre as quais se destaca a crença no "terraplanismo", é sintomática do fluxo descontrolado de informações que inunda a grande rede[3]. Não por acaso, apenas recentemente o termo "*fake news*" (notícias falsas) foi oficialmente adicionado ao dicionário Oxford[4], mesmo existindo desde 1890, consoante artigo da editora estadunidense Merriam-Webster[5]. A compreensão dos fenômenos que levaram a esta conjuntura tem significativo valor para esta pesquisa.

O "empréstimo" do termo técnico histórico realizado no título do presente trabalho, ao aludir a uma "era dos algoritmos", passa longe de pretender uma efetiva campanha pelo reconhecimento acadêmico de um conjunto de elementos

---

3 'Fake News' é eleita palavra do ano e vai ganhar menção em dicionário britânico: palavra foi amplamente usada pelo presidente dos EUA, Donald Trump, na campanha eleitoral, e acabou se disseminando pelo mundo todo. **Portal de Notícias G1**, 02 nov. 2017. Educação. Disponível em: <https://g1.globo.com/educacao/noticia/fake-news-e-eleita-palavra-do-ano-e-vai-ganhar-mencao-em-dicionario-britanico.ghtml>. Acesso em: 21 out. 2019.

4 New words list October 2019. **OED**. 2019. Disponível em: <https://public.oed.com/updates/new-words-list-october-2019/ >. Acesso em: 21 out. 2019

5 The Real Story of 'Fake News': The term seems to have emerged around the end of the 19th century. **Merriam-webster**. [s. d.]. Disponível em: <https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news>. Acesso em: 21 out. 2019

socioeconômico-culturais próprios a uma nova era histórica, mesmo porque tal façanha seguramente foge do escopo de um trabalho de conclusão de curso de Direito. O emprego do termo enquanto recurso narrativo, porém, facilita a constatação de que o surgimento de tecnologias e recursos digitais foi acompanhado da criação de novos e inusitados desafios jurídicos centrados nos fenômenos sociais que seguiram a criação de novos hábitos.

2.2. NOVOS HÁBITOS, NOVOS PROBLEMAS. COLOCAÇÃO DO PROBLEMA DA MERCANTILIZAÇÃO DE HÁBITOS DE NAVEGAÇÃO E SEUS EFEITOS SOBRE A VIDA PRIVADA

A constatação da existência de novos hábitos não demanda muito esforço. Em verdade, pode-se dizer que sua constatação está ao alcance das mãos; hoje, pela primeira vez em séculos, carteiras e chaves perdem seu espaço consagrado nos bolsos de calças para celulares, que aos poucos começam a desempenhar a função de ambos. O consumo destes eletrodomésticos demonstrou crescimentos vertiginosos nos últimos anos**,** justificados pelo cultivo de uma cultura que incentiva e, em certos casos, premia a conexão em tempo integral.

A intensificação massiva das trocas de informações por intermédio da grande rede foi paulatinamente acompanhado por um interesse na fiscalização e controle destas trocas. A preocupação com este espaço de livre troca de dados cresceu por uma conjunção de fatores de diferentes naturezas, atraindo o interesse de entes públicos e privados.

Com o crescimento das comunicações digitais, afinal, os registros das interações, vale dizer, as “pegadas eletrônicas” que deixam suas marcas na grande rede começaram a ganhar grande complexidade. A criação de um termo para os enormes volumes de dados que impactam o mercado, o “Big Data”, aliado a tantos outros termos cibernéticos criados nas últimas décadas, é a um só tempo fenômeno linguístico que acompanha a revolução dos hábitos humanos e fator sintomático de uma posição de destaque desses dados no cenário econômico do novo milênio.

O processo de registro de dados acumulados de centenas de milhares de interações cibernéticas operadas mundo afora cria um emaranhado extremamente denso de informações. Experiências (pessoais e econômicas) de sucesso e

fracasso, atos fraudulentos, compras, incidentes políticos – tudo é convertido em dados e registrado[6], criando um retrato extraordinariamente complexo (e, por isso, também extraordinariamente fiel) da sociedade. A constatação de que os potenciais de computação das máquinas poderiam ser colocadas à disposição do homem para extração de padrões de comportamento em um oceano tão vasto de informações "cruas" compreendido pelo big data foi responsável por uma reviravolta socioeconômica.

A mera obtenção dos dados de usuários não é a finalidade última das empresas interessadas em lucrar com os hábitos de navegação alheios. Em verdade, a instrumentalização destas informações, que geralmente vêm na forma de arquivos contendo Gigabytes ou Terabytes de dados colhidos de milhares de usuários, impõe um sério problema logístico. Nas palavras de Eric Siegel, "à medida que os dados se acumulam, temos uma verdadeira corrida do ouro. Mas os dados não são o ouro (…). Ouro é o que é descoberto com eles"[7].

Por concentrarem alta densidade de informação em arquivos digitais, a interpretação destes dados por seres humanos de maneira direta se faz impraticável. A exploração dos dados pelas empresas se faz de forma mediata, usando programas que se baseiam em algoritmos criados com os dados colhidos. A esse processo de extração de padrões através de big data se dá o nome de "data mining", "mineração de dados", termo que, não por acaso, remete à corrida do ouro.

O valor dos hábitos de navegação para as empresas não está na sua obtenção, mas sim nas interpretações deles extraíveis, pois o tratamento destes dados possibilita, entre outras coisas, o discernimento de padrões de interesses entre os consumidores de determinados produtos e a criação projeções de negócios com altos níveis de fidelidade. Este processo culmina na adoção de manobras econômicas e de publicidade estrategicamente pensadas, maximizando os resultados e lucros.

Nos ensina Milton Santos:

> Estamos diante de um novo "encantamento do mundo", no qual do discurso e a retórica são o princípio e o fim. Esse imperativo e essa onipresença da informação são insidiosos, já que a informação atual

6 SIEGEL, Eric. **Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die**. John Wiley & Sons, Inc.: New Jersey, 2013. p. 03

7 SIEGEL, Eric. **Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die**. John Wiley & Sons, Inc.: New Jersey, 2013. p. 04

> tem dois rostos, um pelo qual ela busca instruir, e um outro, pelo qual ela busca convencer. Este é o trabalho da publicidade. Se a informação tem, hoje, essas duas caras, a cara do convencer se torna muito mais presente, na medida em que a publicidade se transformou em algo que antecipa a produção. Brigando pela sobrevivência e hegemonia, em função da competitividade, as empresas não podem existir sem publicidade, que se tornou o nervo do comércio.[8]

A instrumentalização da programação a serviço das estratégias de marketing é fenômeno recente, por isso muitos estudos ainda estão em progresso acerca de seus efeitos, mas a ocorrência de propagandas especificadamente direcionadas para o usuário de internet é fato amplamente divulgado e, em algumas circunstâncias, facilmente perceptível, conforme sugerem estudos que demonstram a maior incidência de propagandas relacionadas a palavras-chaves gravadas no histórico de pesquisa de sites de busca.

A exploração dos hábitos de navegação tem enorme valor e significado para os setores de publicidade, pois hoje possibilita, através da abstração dos interesses de milhões de usuários da internet, aquilo que nunca se pensou possível nos primórdios da propaganda: o convencimento meticulosamente direcionado ao modo de pensar de cada um.

> Falava-se, antes, de autonomia da produção, para significar que uma empresa, ao assegurar uma produção, buscava também manipular a opinião pela via da publicidade. Nesse caso, o fato gerador do consumo seria a produção. Mas, atualmente, as empresas hegemônicas produzem o consumidor antes mesmo de produzir os produtos. […] Então, na cadeia atual, a chamada autonomia da produção cede lugar ao despotismo do consumo.[9]

8 SANTOS, Milton. Por uma outra globalização: do pensamento único à consciência universal. 10. ed. Rio de Janeiro: Record, 2003. p. 20

9 SANTOS, Milton. Por uma outra globalização: do pensamento único à consciência universal. 10. ed. Rio de Janeiro: Record, 2003. p. 24

3. TRATAMENTO JURÍDICO DOS USUÁRIOS DA GRANDE REDE

Entender a natureza e dimensão das violações constitucionais consubstanciadas no uso desregulado da internet demanda que primeiro se compreendam os princípios gerais que informam o uso consciente da grande rede.

Conquanto verdadeira a assertiva de que o debate sobre violações constitucionais neste ramo perca-se em meio a discussões a respeito do que efetivamente poderia vir a ser considerado um uso abusivo dos dados de internet, a legislação pertinente ao tema possibilita a constatação de certas noções introdutórias, como princípios básicos assegurados a todo usuário da internet.

Não há como contextualizar as previsões legais dispostas pelo ordenamento jurídico no tratamento dos direitos do usuário de internet sem o vislumbre de uma sociedade que exige do indivíduo um estado de permanente conexão e interatividade. Os usos da internet criaram novos hábitos, muitos dos quais ainda são muito recentes, razão pela qual, diante de novos e inusitados problemas jurídicos que desafiam o operador do direito, é necessário que se identifiquem no ordenamento os princípios que protegem o usuário da internet da prática de abusos contra direitos fundamentais que lhe assistem.

3.1. PRINCÍPIOS QUE ASSISTEM O USO DA INTERNET NO BRASIL E SUAS IMPLICAÇÕES

O processo de elaboração da legislação atinente à temática digital no ordenamento brasileiro, buscando a diminuição do descompasse entre a realidade fática e a letra fria da lei, buscou informar o processo legiferante de princípios condizentes com a tutela de determinados direitos particularmente afetados pelas dinâmicas *online*. O interesse na tutela do direito à privacidade e outros direitos que delimitam os direitos da personalidade, bem como de demais direitos fundamentais caros à manutenção da vida digna nos novos tempos, culminou na criação de princípios adiante elucubrados que informam o direito digital.

3.1.**1**. PRINCÍPIO DA PRESERVAÇÃO DA INTIMIDADE E PRIVACIDADE

Em uma sociedade perpetuamente conectada, uma das principais preocupações do direito moderno consiste na manutenção do direito fundamental à intimidade e privacidade. Uma das principais razões pelas quais estes direitos têm sido particularmente atingidos no desenvolvimento de novas dinâmicas sociais reside na maneira com que a grande rede remove do usuário o controle sobre seus dados. Uma consequência natural da proliferação de aplicações da internet que têm como núcleo o compartilhamento de informações é a perda de agência do indivíduo sobre o fluxo de dados a seu respeito que circulam na internet.

Postagens realizadas por outros usuários, curtidas, comentários e registros de acesso a sites são apenas alguns dos dados que trafegam com grande velocidade pelos confins da grande rede, e o poder que estes e outros fenômenos digitais têm de alterar substancialmente vidas alheias em poucos cliques enseja grande preocupação com a preservação legal da privacidade como veículo oficial de resgate a ao menos algum nível de controle sobre as vidas privadas.

Não há consenso doutrinário ou jurisprudencial na discriminação entre os direitos da privacidade e da intimidade, de modo que o tratamento jurídico dispensado a ambos sempre tornou confuso o discernimento entre aquilo que se entende por privado e o que se entende por íntimo. Em verdade, a defesa de ambos pelo ordenamento pátrio está quase sempre relacionada, razão pela qual se faz tão difícil aquilatar características que são únicas a cada.

Tércio Sampaio Ferraz Júnior sugere como “direito à intimidade” a tutela de informações que o indivíduo reserva ao seu conhecimento exclusivo, isto é, dados de “foro íntimo” que conferem identidade à personalidade de seu titular e que exigem de eventual receptor grande lealdade e profunda confiança[10]; ao passo que descreve como “direito à privacidade” a tutela de informações que, malgrado não atinjam o nível de exclusividade das informações íntimas, não deixam de ser privativas a um

10 Ferraz Júnior, T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. *Revista Da Faculdade De Direito, Universidade De São Paulo*, *88*, 439-459. p. 448. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 nov 2019.

núcleo reduzido de receptores, de modo que o devassar da privacidade atingiria o indivíduo em sua integridade moral[11].

A distinção apresentada, embora não tenha caráter definitivo, contribui na compreensão da defesa desses direitos no contexto das interações *online* promovidas pelo próprio indivíduo tutelado. Exceções à parte, via de regra o usuário da internet mediano, mesmo quando compartilha dados que em certa medida "publicizam" alguns fatos de sua vida privada, o faz com a intenção de alcançar seus círculos de amizade mais imediatos, pois o constante intercâmbio de experiências tornou-se o padrão na sociedade da informação.

É razão suficiente para se repelir o antiquado e, em certa medida, ingênuo pensamento de que o problema da privacidade na internet resume-se a uma falta de resguardo do indivíduo, como se as ameaças a esse direito fundamental pudessem sempre ser evitadas mediante abstenção do compartilhamento de informações na grande rede. Trata-se de expectativa desarrazoada ante uma sociedade que já se acomodou a novos hábitos e que exige que o indivíduo esteja sempre a par das últimas tendências tecnológicas; o Direito deve intervir para assegurar sempre os direitos fundamentais indisponíveis e combater, onde existirem, os abusos de direito.

Nesta senda, intimidade e privacidade situam-se nos chamados "direitos da personalidade", os direitos subjetivos de um indivíduo à defesa do que lhe próprio, como a vida, a identidade, a liberdade, imagem, privacidade e honra[12]. À luz da sociedade da informação, a tutela dos direitos da personalidade tem assumido grande relevância no direito digital, vez que o exponencial volume, intensidade e implicações das interações virtuais tem criado efeitos nocivos ao indivíduo que o Poder Legiferante já não mais pode ignorar.

A proteção à intimidade e à vida privada do indivíduo encontra respaldo constitucional na forma do disposto no art. 5º, incisos X e XII da Constituição Cidadã, que disciplina a inviolabilidade da intimidade, da vida privada, da honra e imagem das pessoas, bem como o sigilo de correspondências e comunicações telegráficas.

---

11 Ferraz Júnior, T. S. (1993). **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. *Revista Da Faculdade De Direito, Universidade De São Paulo*, *88*, 439-459. p. 449. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 nov 2019.

12 DINIZ, Maria Helena. **Código Civil Anotado**. 17ª Ed. São Paulo: Saraiva, 2014. 1542 p. p. 87. ISBN 978-85-02-21537-5.

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> (...)
>
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;
>
> (...)
>
> XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; (Vide Lei nº 9.296, de 1996)

A proteção à privacidade também informa a disciplina do uso da internet no Brasil, consoante os seguintes dispositivos do Marco Civil da Internet (Lei nº 12.965/2014):

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
>
> (...)
>
> II - proteção da privacidade;
>
> (...)
>
> Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Outro diploma legal de particular relevância para o direito digital, a Lei Geral de Proteção de Dados (Lei nº 13.709/2018) elenca a defesa da vida privada e da intimidade em seus arts. 2º e 17º, abaixo transcritos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> I - o respeito à privacidade;
>
> (...)
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.

3.1.2. PRINCÍPIO DA LIBERDADE DE EXPRESSÃO

O desmonte do direito à liberdade de expressão nos anos da ditadura militar deixou como legado para as gerações futuras de juristas no Brasil a compreensão de seu histórico valor e importância para a concretização de um Estado Constitucional de Direito verdadeiramente democrático e plural.

Proteger a liberdade de expressão no contexto da sociedade de informação significa assegurar os meios para concretização de uma internet verdadeiramente colaborativa e livre de censura, proibindo por parte do Poder Estatal ou quaisquer pessoas naturais ou jurídicas o controle sobre a produção, distribuição, tratamento e acesso a conteúdos jogados na grande rede.

A experiência da censura cibernética em países com regimes mais autoritários como a China[13] e a Coreia do Norte[14] indica que a liberdade de expressão deve permanecer sob a tutela da legislação pátria, razão pela qual não há surpresa em constatar que os diplomas normativos atinentes ao direito digital são informados pelo princípio da proteção ao livre manifesto de opiniões, ideias e pensamentos *online*.

Embora a liberdade de expressão enquanto conceito à luz de uma sociedade acostumada com o ininterrupto compartilhamento de dados por intermédio das mídias sociais possa parecer trivial, sabiamente cuidou o legislador pátrio, relembrando os anos despóticos da ditadura, de incluir nos diplomas legais atinentes ao uso da internet a salvaguarda desta que é das mais sagradas instituições do Estado de Direito democrático.

Primeiramente, a liberdade de expressão encontra guarida na Constituição Federal, que disciplina, em seu art. 220, o direito à livre manifestação:

> Art. 220. A manifestação do pensamento, a criação, a expressão e a informação, sob qualquer forma, processo ou veículo não sofrerão qualquer restrição, observado o disposto nesta Constituição.

13 ‘Busca sob censura’: por que o suposto plano do Google para chegar à China é polêmico. Portal de Notícias G1, [s. l.], 2 ago 2018. Disponível em: <https://www.bbc.com/portuguese/salasocial-45042713 >. Acesso em: 27 nov 2019.

14 15 coisas que são proibidas na Coreia do Norte: No país mais fechado do mundo não se pode usar calça jeans, celebrar o Natal ou conversar com estrangeiros. Veja, Angela Nunes, 01 set 2017. Disponível em: <https://veja.abril.com.br/mundo/15-coisas-que-sao-proibidas-na-coreia-do-norte/ >. Acesso em: 27 nov 2019.

> § 1º Nenhuma lei conterá dispositivo que possa constituir embaraço à plena liberdade de informação jornalística em qualquer veículo de comunicação social, observado o disposto no art. 5º, IV, V, X, XIII e XIV.
>
> § 2º É vedada toda e qualquer censura de natureza política, ideológica e artística.

A temática é retomada, ainda, no Marco Civil da Internet. Ao versar sobre o tema no indigitado corpo normativo, cuidou o legislador de adotar postura afirmativa no uso da internet, reconhecendo o papel que desempenha, inclusive na cidadania, enquanto instrumento de enorme relevância social. O princípio da proteção à liberdade de expressão encontra-se sustentado por uma série de dispositivos que, na medida em que asseguram a natureza plural e colaborativa da rede, garantindo que a internet não seja reduzida a mero veículo midiático de propaganda, confirmam também o direito mais amplo à livre manifestação do pensamento.

Importante destacar que a proteção à liberdade de expressão *online* que se pretenda genuína confunde-se, em alguns momentos, com o apoio à implementação de políticas públicas que visem assegurar e facilitar o acesso à internet, garantindo que os recursos cibernéticos não se tornem uma regalia das elites. Os dispositivos da Lei nº 12.965/2014 abaixo transcritos, dessarte, são particularmente instrumentais na defesa da liberdade de expressão, direta ou indiretamente:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
> I - o reconhecimento da escala mundial da rede;
> (…)
> III - a pluralidade e a diversidade;
> IV - a abertura e a colaboração;
> (...)
> VI - a finalidade social da rede.
>
> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
> (…)
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> (…)
> VII - preservação da natureza participativa da rede;
>
> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

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

A liberdade de expressão tem espaço também na Lei Geral de Proteção de Dados, onde ela aparece sustentada nos seguintes termos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> (…)
> III - a liberdade de expressão, de informação, de comunicação e de opinião;

3.1.3. PRINCÍPIO DA PROTEÇÃO DE DADOS PESSOAIS

O grande fluxo de dados observado na rede hoje é explicado em grande parte pela natureza das aplicações de internet, que quase sempre demandam, em benefício da funcionalidade, o compartilhamento de uma série de dados das mais variadas naturezas. A comodidade dos aplicativos e sobretudo das mídias sociais seduz milhões de usuários no mundo inteiro a inundar a rede, todos os dias, com 2,5 quintilhões de bytes[15] em novos dados, que incluem fotografias, vídeos, músicas, curtidas, comentários, dentro outros registros de interação.

Por si só, os modos de obtenção desses dados já compreendem sério problema a ser tratado pelos operadores do direito do futuro, vez que frequentemente aproveitam-se da ignorância por parte dos titulares de dados acerca da natureza e finalidade das informações colhidas. Sucede, porém, que a aplicação desses dados têm finalidades que muitas vezes aviltam severamente certos direitos constitucionalmente estabelecidos, o que será explorado em maiores detalhes adiante. Por ora, basta situar o interesse pela proteção de dados pessoais a um

15 How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. **Forbes**, Bernard Marr, 21 mai 2019. Disponível em: <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#3eae63de60ba >. Acesso em: 27 nov 2019.

contexto de usos da internet que exploram o envio de dados do usuário como lucrativo negócio entre empresas em troca de uma maior comodidade na oferta de serviços.

O entendimento dos dados pessoais enquanto bens jurídicos tutelados pelo direito digital pode ser interpretado como corolário indireto dos direitos à privacidade e intimidade, vez que, na dinâmica de interações *online,* são os dados, ou melhor ainda, a sua transmissão que fazem as vezes de “veículos da personalidade”. Vale dizer: é através da transmissão de dados que se expressa, na forma de postagens, compartilhamentos, fotos, vídeos e demais meios, a personalidade na internet.

Informações a respeito de um indivíduo armazenadas na grande rede e que trafegam a internet na forma de dados devem ser protegidas de abusos por parte de terceiros na medida em que constituem à sua própria maneira, na esfera virtual, a vida privada do indivíduo, condição que as submete à tutela da lei sem prejuízo da sistemática que orienta o ordenamento jurídico pátrio.

À luz do exposto, o princípio da proteção a dados pessoais informa uma série de dispositivos na legislação digital do país. De modo geral, a legislação orienta-se no sentido de tentar limitar a prática de abusos no uso de dados de usuários da grande rede, determinando a responsabilização legal por eventuais infrações e danos patrimoniais e extrapatrimoniais causados. Outra preocupação, ainda, consiste na delimitação de critérios para legitimar o acesso desses dados como forma de conciliar o direito à privacidade com princípios como os da razoabilidade, adequação e necessidade, de modo a não comprometer demasiadamente a higidez de empreendimentos e serviços legítimos que dependem, em certa medida, do uso de dados.

Nesta senda, disciplina o art. 3º da Lei nº 12.965/2014, abaixo exposto, que o uso da internet no Brasil tem como princípios:

> Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
> (…)
> III - proteção dos dados pessoais, na forma da lei;
> (…)
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> (...)

> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

A Lei Geral de Proteção de Dados, Lei nº 13.709/2018, dispõe com mais vagar acerca da proteção de dados pessoais, estabelecendo uma maior quantidade de critérios quanto às formas de proteção desses dados e quanto às hipóteses legítimas de tratamento de dados. Este diploma normativo consagra a proteção de dados pessoais nos seguintes termos:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação;
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Cumpre destacar a relevância do art. 2º, II acima exposto, posto que a lei consagra expressamente neste dispositivo o direito do titular dos dados à agência sobre o tratamento dos mesmos, o que reveste de legitimidade a pretensão do titular de dados pessoais em não apenas ter conhecimento das finalidades a que se destinam o emprego de seus dados por terceiros, mas também em ver reconhecido o seu direito de oposição a determinados tratamentos de dados que venham a alcançar finalidades para as quais o indivíduo não tenha dado consentimento.

O direito à autodeterminação informativa compreende natural desdobramento da proteção dos dados pessoais e encontra amparo em diversos dispositivos orientados no sentido de garantir clareza ao titular dos dados na consulta e gerenciamento das informações a seu respeito que rondam a internet (frise-se, o que inclui o direito ao término do tratamento de dados, caso assim prefira o titular), entre os quais se destacam, na LGPD: art. 6º, IV, V e VI; art. 7º, I; art. 11º, I; art. 14, §§1º, 2º; arts. 14 a 20; e art. 23.

Outros dispositivos de grande relevância à proteção de dados pessoais podem ser encontrados distribuídos na LGPD, como o art. 6º, que sujeita o tratamento de dados a critérios de finalidade, adequação e necessidade, ou o art. 7º, responsável por fixar as hipóteses de cabimento dos tratamentos de dados.

Merece destaque, ainda, o art. 11 da LGPD, responsável por consagrar expressamente o tratamento diferenciado conferido a dados pessoais sensíveis, termo assim definido no indigitado diploma normativo:

> Art. 5º Para os fins desta Lei, considera-se:
>
> (…)
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

O legislador, reconhecendo a existência de dados pessoais particularmente vulneráveis, conferiu maior rigor ao tratamento desse tipo de dados, exigindo, por exemplo, consentimento destacado e especificado do titular ou de seu responsável legal para finalidades específicas. O tratamento de dados pessoais sensíveis deve ater-se aos limites do que é disciplinado pelo art. 11, o que confere ao titular maior segurança jurídica na salvaguarda de seus direitos.

O princípio da proteção aos dados pessoais informa, ainda, o art. 14, que versa sobre o tratamento de dados pessoais de crianças e adolescentes. Parcela significativa da população brasileira que utiliza a internet é ainda jovem e carece de tutela diferenciada por parte da legislação, sobretudo considerados os riscos intrínsecos ao tráfego descontrolado de informações pessoais de crianças e adolescentes.

3.1.4. PRINCÍPIO DA NEUTRALIDADE DE REDE

O princípio da neutralidade de rede garante ao usuário o direito ao tratamento isonômico dos pacotes de dados oriundos de seu tráfego na rede pelas empresas responsáveis pela transmissão, comutação ou roteamento de internet, vedando a discriminação de velocidade de conexão por conteúdo, origem e destino, serviço, terminal ou aplicação. Em outras palavras, a neutralidade de rede confere ao usuário a garantia de que sua provedora de internet não fixará velocidades menores de tráfego em determinados sites em detrimento a outros.

A discussão acerca da neutralidade de rede encontrou forte resistência por parte dos defensores da livre iniciativa e autonomia da vontade. A princípio, afinal, a celebração de contratos estabelecidos com consentimento mútuo estabelecendo o condicionamento de acesso veloz a determinados serviços ao pagamento de pacotes de dados mais caros não parece causar grandes danos a direitos do usuário. Naturalmente, é difícil aquilatar os desdobramentos jurídicos implícitos em se permitir que empresas provedoras de conexão ofereçam planos que neguem acesso a alguns sites em detrimento de outros.

A tutela da neutralidade de rede pode parecer, à primeira vista, uma defesa trivial do que pode ser enxergado como mera comodidade. Trata-se, no entanto, de pensamento que deve ser repelido, vez que é a garantia de uma rede efetivamente neutra que garante ao usuário um espaço cibernético verdadeiramente plural e colaborativo. Entregue às arbitrariedades da lógica de mercado sem a tutela da neutralidade de rede, em pouco tempo o tráfego de dados na internet cindir-se-ia em estratos reflexos do fosso existente entre as camadas sociais, realidade que o ordenamento deve combater no interesse de uma internet democratizada. Foi com esse propósito que o legislador consagrou a neutralidade de rede no ordenamento pátrio enquanto princípio informador do uso da internet.

O art. 9º do Marco Civil da Internet versa sobre a aplicação desse princípio no uso da internet no país:

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
>
> § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente

> da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
>
> I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
>
> II - priorização de serviços de emergência.
>
> § 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º , o responsável mencionado no **caput** deve:
>
> I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;
>
> II - agir com proporcionalidade, transparência e isonomia;
>
> III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
>
> IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
>
> § 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

O legislador estabeleceu em rol taxativo de hipóteses, portanto, critérios para discriminação ou degradação do tráfego de dados, determinando através do dispositivo em tela que elas só se justificam diante da existência de requisitos técnicos indispensáveis à prestação adequada dos serviços, isto é, quando subsistirem razões técnicas que justifiquem a abstenção da neutralidade de rede em prol da prestação adequada de serviços e aplicações, ou quando a tutela da neutralidade de rede vir a colidir com a priorização de serviços de emergência, vale dizer, nas eventuais hipóteses em que a neutralidade de rede possa representar uma ameaça ao acesso do cidadão a serviços online prestados pela polícia ou pelo Serviço de Atendimento Móvel de Urgência (SAMU), por exemplo.

3.1.5. OUTROS PRINCÍPIOS DO USO DA INTERNET NO BRASIL

Além dos princípios já elucubrados de tutela da privacidade, da liberdade de expressão, da proteção de dados pessoais e da neutralidade de rede, pode-se falar

ainda em alguns outros princípios que encontram relevante expressão no ordenamento jurídico próprio ao direito digital.

Exemplo disso é o princípio da proteção ao funcionamento, segurança e estabilidade da rede, que estabelece como prioridade a promoção de medidas que assegurem o emprego de técnicas aptas a garantir a continuidade do serviço de internet no país. A estabilidade da rede é princípio basal do direito digital, vez que é responsável por assegurar a própria existência de uma rede à qual os brasileiros possam se conectar, e encontra significativa expressão figurando como fundamento do uso da internet no Brasil consoante art. 2º do Marco Civil da Internet, bem como determinando, no art. 4º do referido diploma legal, a promoção de medidas que assegurem sempre o fomento de novas tecnologias de uso e acesso à internet:

> Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:
>
> (...)
>
> V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
>
> Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
>
> (...)
>
> III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
>
> IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Há que se falar, ainda, no princípio de proteção do desenvolvimento econômico através da internet. Apesar de existirem limitações ao uso de dados de indivíduos e uma grande responsabilidade por parte daqueles que tomam decisões sobre os destinos dessas informações, essas limitações devem ser encaradas como indispensáveis à tutela de direitos fundamentais, e não como fatores limitadores a empreendimentos que lancem mão da internet como meio de negócios.

A despeito da existência de extensivo rol de direitos a serem respeitados no direito digital e sobre os quais esta monografia trata, não há óbice a que, respeitados

os limites legais impostos pelo ordenamento, empresas façam uso extensivo dos meios tecnológicos disponíveis em seus negócios.

A livre iniciativa nos meios digitais encontra guarida no art. 2º da LGPD, abaixo transcrito:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
>
> (…)
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;

Cumpre destacar de forma breve que, naturalmente, nos casos em que a internet é utilizada como intermédio de negociações, o estabelecimento de uma relação de consumo enseja, sem prejuízo do disposto nos demais diplomas normativos sobre o tema, a aplicação do Código de Defesa do Consumidor, legislação que, muito antes da criação de leis específicas como o Marco Civil e a LGPD, já versava, ainda que de forma incipiente, sobre compras *online.* Tópico já muito debatido, por exemplo, é o art. 49 do CDC, que garante o direito do arrependimento posterior em face de contratação de fornecimento de produtos e serviços fora do estabelecimento comercial, especialmente por telefone ou a domicílio.

3.2. O USO DE DADOS E NOVAS TECNOLOGIAS DE INFORMAÇÃO SOB A PERSPECTIVA DAS VIOLAÇÕES PERPETRADAS CONTRA ALGUNS DIREITOS FUNDAMENTAIS

A experiência cibernética hoje é assinalada pelo uso de novas tecnologias de comunicação e informação cuja funcionalidade encontra-se, do ponto de vista técnico, indissociável do uso de dados pessoais.

A simplicidade programada na interface das aplicações com que os usuários interagem esconde processos extraordinariamente complexos, entre os quais serão foco da presente monografia os tratamentos dispostos a dados pessoais de usuários**.**

A análise das violações constitucionais oriundas das aplicações de tecnologias de comunicação e informação não pode proceder senão à luz dos desdobramentos práticos atrelados a diversos usos da grande rede, vez que várias práticas aparentemente inócuas escondem ameaças preocupantes a direitos fundamentais.

A reflexão acerca do tratamento de dados pessoais como matéria-prima de algoritmos que sustentam a funcionalidade das aplicações de internet é um bom ponto de partida para um debate jurídico acerca dos efeitos nocivos que os novos tempos têm criado sobre direitos fundamentais, pois situa os novos usos da internet em um contexto de verdadeira exploração da vida privada por grandes empresas.

Não sem efeito, grande parte da comodidade de certos aplicativos vem da maneira com que são programados para parecer que foram feitos sob medida para cada usuário. Os esforços de programadores para fazer o usuário se sentir “em casa” com seus aplicativos assumem várias expressões: a interface costuma ser limpa e eficiente, com a menor quantidade possível de poluição visual; os comandos são, sempre que possível, intuitivos para usuários experientes, mas aconchegantes para iniciantes. Com a finalidade de criar uma conexão com o usuário, muitas aplicações têm optado por "adivinhar" suas preferências, lançando mão, para tal, da análise de hábitos de uso dos usuários.

Quando o Google tenta prever a intenção de seus usuários, sugerindo uma série de pesquisas relacionadas às palavras-chave inseridas no campo de busca através da ferramente “AutoCompletar”, na verdade está se valendo de um histórico registrado de milhões de buscas realizadas por outros usuários, o que permite ao software comparar as palavras-chave já inseridas a um acervo monumental de pesquisas realizadas com aqueles termos. Assim, o software “entende” que quem insere “constituição” no campo de busca geralmente está procurando por “constituição federal” e não “constituição física”, por exemplo.

Percebe-se, portanto, que no cerne da funcionalidade desta aplicação da internet, como tantas outras, está o acesso a dados inseridos por usuários. Os hábitos de navegação dos usuários da internet criam um verdadeiro oceano de dados conhecido como Big Data – uma malha extraordinariamente complexa de informações dispersas e inter-relacionadas que representa, a um só tempo,

preferências, aspirações, medos, inclinações políticas, enfim, vidas de centenas de milhões de usuários.

A concentração de tantas informações nos hábitos de navegação, consubstanciadas nos dados pessoais que trafegam a grande rede em enormes volumes, aliada a um cenário de grande interesse sobre os interesses privados por parte de governos e empresas, compreendem fatores responsáveis pela criação de uma conjuntura propícia à ameaças de certos direitos fundamentais.

Nesta senda, a presente monografia orienta-se robustamente no sentido de que a mercantilização de hábitos de navegação, estabelecida enquanto lógica de mercado, atinge, em seus mais diversificados desdobramentos, uma série de direitos que remontam a lutas históricas pela consagração de fundamentos demasiado caros ao Estado democrático de direito como o conhecemos hoje.

Por “direitos fundamentais” compreende-se, em apertada síntese, o conjunto de “situações jurídicas sem as quais a pessoa humana não se realiza”[16]. Neste sentido, interessam ao presente trabalho os desdobramentos das tecnologias de comunicação e informação que de alguma maneira possam interferir na expressão desses direitos, malgrado reste impossibilitado, por razões práticas, o esgotamento do tema.

Precisamente em virtude da impossibilidade de esgotamento da temática, oriunda, sobretudo, da complexidade intrínseca à análise das inovações tecnológicas, bem como porque a digressão a um raciocínio dos critérios de classificação dos direitos fundamentais foge ao âmbito do presente trabalho, convém tratar de alguns direitos fundamentais violados *em espécie*. Sem prejuízo de classificações doutrinárias consagradas, tratar dos direitos fundamentais em espécie na presente monografia possibilita um a seleção de um rol mais delimitado de direitos a serem tratados e garante um tratamento mais direcionado das ameças representadas pelas novas tecnologias, garantindo um maior aprofundamento nas questões abordadas.

16 SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25ª Ed. São Paulo: Malheiros Editores Ltda, 2005. 925 p. p. 178. ISBN 85.7420.868-5

3.2.1. A MERCANTILIZAÇÃO DE HÁBITOS DE NAVEGAÇÃO E AS VIOLAÇÕES AO DIREITO À PRIVACIDADE

Consoante destacado com mais ênfase em outro momento, a legislação pátria relevante ao direito digital consagra enquanto princípio informador dos usos da internet a proteção à privacidade. Cumpre, agora, analisar as formas assumidas pelas novas tecnologias de informação, contextualizadas a um mercado que transforma hábitos de navegação em valiosos recursos, no embaraço do direito à privacidade.

Aquilatar as ofensas do direito à privacidade perpetradas pelos usos das tecnologias de informação e comunicação demonstra-se tarefa particularmente difícil porque demanda atenção para diversas facetas da vida privada que são diuturnamente violadas sem muito alarde.

Não há, por parte da população, estranhamento à publicação de fotos, vídeos e comentários em mídias sociais – são atos reputados como comuns no mundo moderno e integram uma série de novos hábitos que acompanham a era dos algoritmos. Via de regra, cumpre notar, sob uma perspectiva jurídica, não há que se falar em lesão a direito quando a opção pela publicação desses dados emanar de seu próprio titular, pois os resultados dessa publicação encontrar-se-ão envoltos pelo manto do consentimento.

Segundo ensina Patricia Peck:

> O grande paradigma não está no conceito ético ou mesmo filosófico se a privacidade deve ou não ser protegida. Claro que deve ser. Mas sim no modelo de negócios estabelecido, visto que a informação virou não apenas a riqueza do século XXI como também a moeda de pagamento.[17]

Esclarece a autora, ainda, que o cadastro em serviços digitais acaba por gerar dois tipos de informação: as informações inseridas diretamente pelo usuário são as informações cadastrais, ao passo que o próprio uso do serviço pelo usuário gera um segundo tipo de informação, a informação comportamental[18].

17 PECK PINHEIRO, Patricia. Direito Digital. 5ª Ed. São Paulo: Saraiva, 2013. 323 p. p. 43. ISBN 978-85-02-20166-8.

18 PECK PINHEIRO, Patricia. Direito Digital. 5ª Ed. São Paulo: Saraiva, 2013. 323 p. p. 43. ISBN 978-85-02-20166-8.

As informações comportamentais atêm-se, portanto, a vislumbres menos objetivos da personalidade, que o usuário “deixa escapar” em seus hábitos de navegação. Quando o usuário declara em suas redes sociais que pensa em viajar, por exemplo, ou quando o seu histórico de buscas revela indícios desse interesse, o uso desses dados pode vir a culminar com o direcionamento de propagandas de serviços de hotelaria e turismo àquele indivíduo. A coleta desses dados com esse propósito, se não for fruto de algum acesso excessivo (e, portanto, ilegítimo), não fere, a rigor, o direito à privacidade, pois concilia o direito de expressão virtual do usuário com o interesse econômico de empresas interessadas em potenciais consumidores. Na prática, contudo, muito pouco é divulgado a respeito de como os dados são coletados e utilizados.

Com efeito, os famosos “termos de aceite” preludiam, hoje, praticamente todo acesso a serviços digitais que se baseiem nesse “mercado de informações”. A pressão exercida por movimentos internacionais (inclusive extrajudiciais) de conscientização acerca dos usos de dados por empresas de tecnologias culminou na criação de medidas públicas que cobram das empresas maior transparência nas maneiras de uso dos dados de usuários. Por essa razão, diversas empresas grandes do setor passaram, sobretudo nos últimos anos, por grandes mudanças em suas políticas de privacidade[19] de modo a incluir informações mais precisas acerca da destinação dos dados extraídos dos hábitos de uso e navegação de seus clientes.

Conquanto bem intencionada, a disposição detalhada das políticas de privacidade por empresas, notável conquista do usuário da internet, não é suficiente para assegurar a salvaguarda do direito à privacidade. A razão é flagrantemente simples: o usuário mediano das aplicações de rede não lê as condições de uso dos serviços que utiliza[20].

---

19 Após escândalo, Facebook muda termos de uso e política de privacidade: Uma das novidades é que a rede social vai deixar mais claro quais empresas fazem parte do grupo, como WhatsApp, Instagram e Oculos. **Veja**, [s. l.], 04 abr 2018. Disponível em: <https://veja.abril.com.br/economia/apos-escandalo-facebook-vai-mudar-termos-de-uso-e-politica-de-dados/ >. Acesso em: 27 nov 2019.

20 Click to agree with what? No one reads terms of service, studies confirm: apparently losing rights to data and legal recourse is not enough of a reason to inspect online contracts. So how can websites get users to read the fine print? **The Guardian**, David Berreby, 03 mar 2017. Disponível em: <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print >. Acesso em: 27 nov 2019.

Clicar em “aceito” sem ler os termos de uso de serviços *online* tornou-se um hábito de centenas de milhões de usuários da internet, o que possibilita às empresas a inserção de todo tipo de cláusula no corpo do texto sem grandes dificuldades, obrigando o consumidor à adesão de cláusulas que podem lhe ser bastante inconvenientes, como cláusulas de eleição de foro ou cláusulas que dispõem sobre os direitos da empresa fornecedora de serviços ao compartilhamento de seus dados.

A situação piora quando se avalia a praticidade dos contratos de adesão enquanto veículos idôneos de expressão do consentimento. O artigo “The Cost of Reading Privacy Policies” (“O custo de ler políticas de privacidade”) [21] descreve os achados da pesquisa conduzida por pesquisadores americanos sobre contratos de adesão constantes dos sites mais acessados nos Estados Unidos. Segundo indica o artigo, presumindo uma taxa de leitura de 250 palavras por minuto para cada usuário, a média de tempo de leitura para contratos de adesão é de cerca de 4 a 12 minutos (variando conforme a velocidade de leitura e o tamanho do contrato), o que levou a conclusões preocupantes; para ler as políticas de privacidade de todos os sites acessados em um ano (em média, 119 sites, conforme a pesquisa), o americano precisaria gastar até 304 horas anuais, o que representaria, com base em cálculos sobre uma média do valor do salário, um custo anual de até U$5.038,00 por cidadão americano. O prazo a que os pesquisadores chegaram não incluiu, conforme indicado no próprio artigo, o cálculo do tempo necessário para que, com vistas à tomada de decisões adequadamente informadas acerca das disposições de seus direitos de privacidade, o indivíduo fizesse comparações entre os contratos.

Se transportados os dados da pesquisa americana para o caso brasileiro tão somente no que tange o tempo de leitura dos contratos, constata-se que, respeitada a disposição do art. 7º, inciso XIII da Constituição Federal de duração máxima da jornada de trabalho em oito horas, 304 horas representariam 38 dias de trabalho por ano que o indivíduo precisaria apenas para fazer a leitura dos contratos que lhe são disponibilizados pelos sites e serviços de que se utiliza.

Assim, constatada não apenas a ignorância de grande parte dos usuários de internet quanto ao conteúdo dos contratos de adesão representados pelas políticas

21 Disponível em: <https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf >. Acesso em: 27 nov 2019.

de privacidade e termos de serviço, mas também, em certa medida, a impossibilidade prática de se exigir do usuário a leitura de todas as cláusulas, há que se reconhecer uma posição de vulnerabilidade por parte do usuário de internet quanto ao tratamento de dados realizado por empresas de tecnologia. Trata-se de conjuntura que traz à baila discussões pertinentes acerca da possibilidade de reconhecimento de vícios de consentimento nos contratos de adesão celebrados sobretudo por intermédio das vias telemáticas, onde no mais das vezes o consentimento é extraído de um simples clique.

São diversas as tecnologias de informação que interferem no direito à privacidade, sobretudo com o vertiginoso crescimento de um mercado centrado no direcionamento de campanhas de publicidade a indivíduos estrategicamente selecionados. O sistema é alimentado pelo registro de hábitos de uso e navegação das aplicações de rede, que, convertidos na forma de dados e comercializados, colocam na mão de empresas dados concernentes a diversas preferências íntimas e privadas dos usuários da internet.

Neste sentido, convém destacar o importante papel desempenhado pelos princípios de “privacy by design” e “privacy by default”, incluídos na General Data Protection Regulation (GDPR) europeia (legislação internacional particularmente influente no processo de elaboração da LGPD brasileira), na proteção do direito à privacidade.

Privacy by design consiste na exigência da boa prática por parte das empresas que façam o tratamento de dados no sentido de assegurar, ainda durante o processo de desenvolvimento e programação das aplicações de rede, medidas que visem proteger a esfera privada da vida dos futuros usuários. Por sua vez, a privacy by default disciplina a limitação da quantidade de informações coletadas pelos aplicativos em seu funcionamento, assegurando, assim, que a coleta de dados faça sentido ante a natureza dos serviços prestados e inibindo o excesso na coleta e mercantilização de dados pessoais.

Tratam-se de princípios que têm conquistado amplo espaço no cenário digital ante os escândalos de privacidade noticiados pela mídia e que encontram perfeita consonância com as disposições da LGDP brasileira, razão pela qual espera-se que

sejam absorvidos pela jurisprudência brasileira no tratamento de casos em que empresas e entes estatais façam uso de dados pessoais.

Segundo José Afonso da Silva, a Constituição ambiciona proteger o indivíduo da violação de duas prerrogativas: o segredo da vida privada e a liberdade da vida privada[22]. Ver assegurado o segredo da vida privada significa ter garantida a expansão da personalidade; ver assegurada a liberdade da vida privada, por sua vez, significa ter ampla liberdade para realizá-la sem perturbação de terceiros. Ensina o autor, então, que o segredo da vida privada se vê ameaçado pelo recrudescimento de "divulgações ilegítimas por aparelhos registradores de imagem, sons e dados, infinitamente sensíveis aos olhos e ouvidos"[23].

Para além das violações de privacidade consubstanciadas na mercantilização dos hábitos de navegação, a observação apontada faz-se particularmente pertinente hoje, com a divulgação de vídeos filmados muitas vezes sem consentimento e até mesmo com o surgimento de tecnologias de reconhecimento facial capazes de identificar e discernir rostos em meio a multidões[24]. Tratam-se de aplicações sobre as quais os futuros operadores do Direito deverão se debruçar, com o fito de impedir a prática de abusos por parte tanto de empresas quanto de entidades estatais.

3.2.2. ALGORITMOS E O DIREITO À IGUALDADE

A massificação no modo de tratamento de indivíduos na grande rede encontra respaldo em diversos instrumentos da vida cotidiana. Os contratos de adesão, já explorados neste trabalho, compreendem precisamente uma alternativa do empreendedor para conseguir celebrar contratos com mais rapidez e facilidade ante um grande número de clientes, e a despeito das críticas feitas à higidez desses

22 SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25ª Ed. São Paulo: Malheiros Editores Ltda, 2005. 925 p. p. 208. ISBN 85.7420.868-5

23 SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25ª Ed. São Paulo: Malheiros Editores Ltda, 2005. 925 p. p. 208. ISBN 85.7420.868-5

24 Inteligência artificial: Por que as tecnologias de reconhecimento facial são tão contestadas: As ferramentas de inteligência artificial são tão boas quanto o banco de dados que usam para funcionar, mas e se essas informações forem enviesadas? **Portal de Notícias G1**, [s. l.], 06 jul 2019. Disponível em: <https://g1.globo.com/mundo/noticia/2019/07/06/inteligencia-artificial-por-que-as-tecnologias-de-reconhecimento-facial-sao-tao-contestadas.ghtml >. Acesso em: 27 nov 2019.

contratos enquanto veículos de expressão do consentimento, o fato é que os contratos de adesão trazem enorme comodidade ao mundo contemporâneo pois possibilitam o tratamento homogêneo a um grande número de indivíduos.

Conforme revelam as estratégias de *marketing* virtual, porém, as novas tecnologias de informação vão além e possibilitam, sem maiores embaraços, um tratamento cada vez mais particularizado dos usuários de internet, possibilitando o direcionamento de sugestões que combinem com as preferências de cada indivíduo.

Conforme explicado, o tratamento de dados pessoais possibilita às máquinas a identificação de complexos padrões comportamentais através do *data mining*, processo que culmina na criação de algoritmos que tentam prever o comportamento humano com base em grandes acervos contendo dados referentes a hábitos de milhões de usuários.

No campo das políticas públicas, os algoritmos assumem certo destaque na expressão de novas possibilidades de aproximação entre os usos da tecnologia e a efetivação do direito à igualdade, vez que a igualdade, enquanto direito constitucionalmente estabelecido, não se reduz ao sentido formal do termo. Nos termos estabelecidos pela Constituição e em atendimento à sistemática do ordenamento pátrio, a igualdade compreende respeito a situações que legitimam o tratamento jurídico diferenciado para situações idênticas envolvendo indivíduos distintos, conforme ensina José Afonso da Silva:

> Quando se diz que o legislador não pode distinguir, isso não significa que a lei deva tratar todos abstratamente iguais, pois o tratamento igual – esclarece Petzold – não se dirige a pessoas integralmente iguais entre si, mas àquelas que são iguais sob os aspectos tomados em consideração pela norma, o que implica que os “iguais” podem diferir totalmente sob outros aspectos ignorados ou considerados como irrelevantes pelo legislador. Este julga, assim, como “essenciais” ou “relevantes”, certos aspectos ou características das pessoas, das circunstâncias ou das situações nas quais essas pessoas se encontram, e funda sobre esses aspectos ou elementos as categorias estabelecidas pelas normas jurídicas; por consequência, as pessoas que apresentam os aspectos “essenciais” previstos por essas normas são consideradas encontrar-se nas “situações idênticas”, ainda que possam diferir por outros aspectos ignorados ou julgados irrelevantes pelo legislador; vale dizer que as pessoas ou situações são iguais ou desiguais de modo relativo, ou seja, sob certos aspectos.[25]

25 SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25ª Ed. São Paulo: Malheiros Editores Ltda, 2005. 925 p. p. 216. ISBN 85.7420.868-5

Assim, ao possibilitar a particularização do tratamento a parcelas diferentes da população, os algoritmos abrem um leque de possibilidades na efetivação do direito de igualdade se instrumentalizado a serviço da administração pública em prol dos administrados.

A despeito do exposto acima, porém, experiências estrangeiras de implementação dessas tecnologias na vida pública vêm demonstrando que grande cautela é necessária na intermediação de serviços públicos realizada por algoritmos. Apesar de empreendimentos (em sua maioria ainda incipientes) de *deep learning* e *machine learning* que tentam conferir certa autonomia a inteligências artificiais na condução de tarefas tipicamente humanas, os algoritmos não são dotados de pensamento próprio ou livre-arbítrio. O funcionamento do algoritmo toma como base o acervo de dados colocado à sua disposição, de modo que o desempenho dos softwares, que inclui a tomada de decisões e avaliação de prioridades, estará intrinsecamente ligado à qualidade das informações que fundamentam sua programação.

Diversos exemplos ilustram a imensa relevância deste aspecto técnico de funcionamento dos algoritmos. Em 2016, a Microsoft criou um perfil no Twitter para hospedar uma inteligência artificial desenvolvida para aprender através de interações humanas. Nascia Tay, a *chatbot* da Microsoft que interagia com respostas de outros usuários e aprendia tentando replicar comportamentos *online*. Levou apenas algumas horas até que usuários da rede social conseguissem, através de repetidas menções e referências nazistas e de cunho racista, fazer com que a inteligência artificial começasse a reproduzir suas primeiras postagens preconceituosas[26]. O algoritmo que gerava as postagens de Tay, alimentado por um grande volume de *posts* preconceituosos e sem uma supervisão humana de filtragem, começou a replicar comportamentos humanos discriminatórios.

---

26 Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter: Attempt to engage millenials with artificial intelligence backfires hours after launch, with TayTweets account citing Hitler and supporting Donald Trump. **The Guardian,** Elle Hunt, 24 mar 2016. Disponível em: <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter >. Acesso em: 27 nov 2019.

Experiências estrangeiras já demonstraram a aplicação de algoritmos cuja implementação, malgrado orientada por critérios razoáveis, terminou por gerar resultados práticos que violavam direitos fundamentais. Neste sentido, um caso particularmente ilustrativo dos efeitos nocivos de algoritmos ao direito de igualdade ocorreu em instituições de saúde nos EUA, onde algarismos de planos de saúde que determinavam o fator de risco de pacientes dificultavam o acesso de negros a planos de saúde melhores[27].

Análises preliminares demonstraram um equilíbrio na quantidade de doentes brancos e negros, mas uma quantidade muito maior de brancos entre os assistidos pelos melhores planos de saúde. Investigando o caso, os pesquisadores descobriram que o algoritmo lançava mão de informações como gastos de pacientes com saúde ao longo de um ano para quantificar a taxa de risco de cada indivíduo, atribuindo risco mais alto a pacientes que gastavam mais com tratamentos de saúde e ofertando-lhes planos com mais serviços. Avaliou-se, então, que “gastos com saúde” tratava-se de uma métrica com forte viés racial em razão de desigualdades econômicas atreladas à cor da pele, o que fazia com que pacientes negros, que tinham mais dificuldade de acesso à saúde, gastassem consequentemente menos com tratamentos, o que era interpretado equivocadamente pelo algoritmo como um sinal de saúde desses indivíduos, já que eles não precisavam gastar muitos recursos com a preservação da saúde.

Outro caso particularmente relevante, sobretudo considerada a realidade brasileira, diz respeito à aplicação de algoritmos nas dinâmicas de segurança pública. A utilização de algoritmos para aperfeiçoar a manutenção da ordem pública já é realidade em alguns países como Inglaterra e Estados Unidos, e considerados os problemas nacionais com combate à criminalidade, uma análise dos resultados experimentados lá pode seguramente contribuir para a adoção de medidas públicas mais competentes no caso brasileiro. Renata M. O’Donnell[28] explica que detalhes acerca dos critérios utilizados no policiamento orientado por tecnologias de

27 Racial bias found in widely used health care algorithm: an estimated 200 million people are afected each year by similar tools that are used in hospital networks. NBC News, Quinn Gawronski, 06 nov 2019. Disponível em: <https://www.nbcnews.com/news/nbcblk/racial-bias-found-widely-used-health-care-algorithm-n1076436 >. Acesso em: 27 nov 2019.

28 Disponível em: <https://www.nyulawreview.org/wp-content/uploads/2019/06/NYULawReview-94-3-ODonnell.pdf >. Acesso em: 27 nov 2019.

informação são escassos, dado que as autoridades policiais resistem à publicização dessas informações, mas aduz que, de modo geral, os algoritmos atuam quantificando fatores de risco e atribuindo pontuações a pessoas e lugares, gerando, assim, duas vertentes do "policiamento preditivo": policiamento orientado por pessoas e policiamento orientado por lugar.

Enquanto o policiamento orientado por pessoas atribui uma pontuação individualizada de risco para cada indivíduo, o policiamento orientado por lugares individualiza o risco delimitado a determinadas áreas de maior criminalidade. Preocupa, porém, que ambas formas de individualização dos fatores de risco sejam intrinsecamente relacionadas a vieses discriminatórios

Nos Estados Unidos, assim como no Brasil[29], na Inglaterra[30] e em muitos outros países, práticas policiais discriminatórias são muito mais frequentes contra indivíduos de pele negra. Entre 2004 e 2012, a polícia de Nova Iorque registrou 4,4 milhões de abordagens das quais mais de 80% foram realizadas em negros[31]. O registro de atividades policiais racistas no banco de dados da corporação, na medida em que informam os algoritmos de policiamento preditivo, acabam por contribuir para a perpetuação de um policiamento discriminatório.

Trata-se de realidade que pode reverberar negativamente em uma série de políticas públicas, vez que bairros com maior população negra, sob o policiamento preditivo de algoritmos, acabam sendo desnecessariamente pontuados como mais perigosos, o que pode conduzir à destinação infundada de recursos para o combate à criminalidade em áreas que não apresentam tanta demanda, deixando desassistidas áreas que efetivamente necessitem de mais policiamento.

---

29 Taxa de negros mortos pela polícia de SP é 3 vezes a de brancos, diz estudo: Policiais envolvidos, entretanto, são, em sua maioria, brancos (79%). Professora da UFSCar fala em 'racismo institucional'; SSP analisará dados. **Portal de Notícias G1,** Thiago Reis, 26 mar 2014.. Disponível em: <http://g1.globo.com/sao-paulo/noticia/2014/03/taxa-de-negros-mortos-pela-policia-de-sp-e-3-vezes-de-brancos-diz-estudo.html >. Acesso em: 27 nov 2019.

30 Police officers raise concerns about 'biased' AI data. **BBC News**, [s. l.], 16 set 2019. Technology. Disponível em: <https://www.bbc.com/news/technology-49717378 >. Acesso em: 27 nov 2019.

31 Disponível em: <https://www.nyulawreview.org/wp-content/uploads/2019/06/NYULawReview-94-3-ODonnell.pdf >. Acesso em: 27 nov 2019. pág. 554

3.2.3. O ESVAZIAMENTO DE DIREITOS POLÍTICOS E AS CAMPANHAS ELEITORAIS À LUZ DAS FAKE NEWS

O sistema democrático encontra-se sustentado por uma série de direitos políticos essenciais à legitimação do poder público. Nas palavras de Gilmar Mendes, sobre a pujança dos direitos políticos:

> A expressão ampla refere-se ao direito de participação no processo político como um todo, ao direito ao sufrágio universal e ao voto periódico, livre, direto, secreto e igual, à autonomia de organização do sistema partidário, à igualdade de oportunidade dos partidos.[32]

A aguerrida tutela dos direitos políticos tomados em seu *lato sensu* reverbera no ordenamento pátrio através da estipulação de jurisdição especializada no tratamento de questões próprias à sua esfera de interesse, consubstanciada na criação da Justiça Eleitoral. Têm foro na Justiça Eleitoral as questões atinentes ao processo eleitoral, compreendidas na proteção do extenso rol de direitos políticos que exsurgem da Constituição Cidadã e que são inestimáveis à manutenção do Estado democrático de direito.

Contextualizado à era dos algoritmos, o processo de votação, ao menos à primeira vista, não muda substancialmente. Cidadãos continuam a se dirigir de quatro em quatro anos para suas Zonas Eleitorais, onde exercem o direito (e obrigação) de voto, regularizam suas situações eleitorais e retornam às suas vidas normais, aguardando mais quatro anos até as próximas eleições.

Afora a adoção das urnas eleitorais como alternativa às antigas cédulas e os vultosos investimentos indispensáveis à manutenção de um sistema eleitoral seguro contra fraudes, as novidades tecnológicas não provocaram mudanças substanciais neste campo senão no sentido de aperfeiçoamento das técnicas de registro e controle das votações, o que inclui os recentes esforços empenhados no recadastramento biométrico dos eleitores brasileiros[33]. Respeitados os limites ao acesso excessivo dos dados criados com essas novas técnicas de registro por parte

32 Disponível em: <http://noosfero.ucsal.br/articles/0010/3238/gilmar-mendes-curso-de-direito-constitucional.pdf>. Acesso em: 27 nov 2019. pág. 779

33 Disponível em: <http://www.tse.jus.br/eleitor/recadastramento-biometrico/seguranca-na-identificacao>. Acesso em: 27 nov 2019.

de autoridades administrativas, não há que se falar em violações constitucionais se o tratamento dessas informações visa aperfeiçoar o sistema de votação, sobretudo levando em consideração que a coleta de dados é revertida, inclusive, em vantagens significativas para o eleitor, que hoje pode consultar virtualmente seu local de votação, sua situação junto à Justiça Eleitoral, dentre outros serviços a que pode ter acesso virtualmente.

A perspectiva muda, porém, quando nos voltamos para as grandes reviravoltas operadas nas formas de convencimento dos eleitores de que dispõem os partidos políticos. O destaque outrora conferido à televisão enquanto principal instrumento de convencimento dos candidatos cedeu lugar a um novo ambiente de guerra de influências: as redes sociais. Publicações de usuários e partidos políticos inundam sites como o Facebook, Twitter e Instagram com um abundante oceano de fatos e *fake news* que torna particularmente difícil a tarefa de discernimento da verdade por parte dos eleitores.

O fluxo descontrolado de informações, dessarte, tem causado sérias complicações à condução de eleições verdadeiramente democráticas, pois o novo cenário de verdadeira guerrilha informacional cria óbices à expressão livre da vontade do povo. Trata-se de conjuntura que o ordenamento repele, vez que as eleições compreendem, segundo melhor doutrina, o “modo pelo qual o povo participa na formação de vontade do governo”[34].

Os direitos políticos, por representarem, na visão de diversos autores, os direitos de participação popular no Poder, são esvaziados de sentido à luz da prática de abusos por parte de empresas de marketing político que conseguem, através das tecnologias da informação, interferir significativamente nos resultados de eleições.

O escândalo da Cambridge Analytica em 2018, quando descobriu-se a influência da empresa sobre os resultados da eleição de Donald Trump nos Estados Unidos e do sucesso da campanha pró-Brexit na Inglaterra, bem como sobre diversas eleições realizadas na Nigéria, Quênia, República Tcheca, índia, Argentina e Brasil[35], contribuiu como um gatilho para o debate das tecnologias de comunicação e informação à luz da tutela do livre convencimento nas eleições.

34 SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25ª Ed. São Paulo: Malheiros Editores Ltda, 2005. 925 p. p. 368. ISBN 85.7420.868-5

Através de dados coletados sem consentimento ou notificação de milhões de usuários ao redor do globo, a Cambridge Analytica conseguiu discernir complexos perfis comportamentais da qual lançou mão para oferta de conteúdo dirigido aos usuários (“*behavior microtargeting”* ou, em tradução livre, micro-direcionamento comportamental). No contexto das eleições, conhecer a fundo as personalidades dos eleitores de cada partido abre a possibilidade de bombardear cada lado com notícias que comprovem seus medos, instigando a instauração de um clima de grande animosidade responsável pelo acirramento dos posicionamentos políticos[36]. Com os extremos políticos robustamente delineados, a tendência natural entre os eleitores é de assumir um dos lados[37], o que culmina em uma substancial modificação do cenário eleitoral – tudo através de uma intervenção artificial gerada por empresas como a Cambridge Analytica e patrocinada por interesses econômicos e políticos desconhecidas pelos indivíduos.

A disseminação de *fake news* na época de eleição instiga sérios questionamentos a respeito dos efeitos nocivos inerentes à prática da desinformação e suscita novos problemas enfrentados na seara das campanhas eleitorais, pois os partidos políticos tornam-se alvos de mentiras que dificultam sensivelmente a tomada de escolha consciente por parte do eleitor.

No Brasil, a primeira Lei a regulamentar o uso da internet em campanhas eleitorais no Brasil foi a Lei n. 9.504/1997[38]. O cenário político e tecnológico era extremamente diferente àquela época, de modo que o ordenamento pátrio assistiu à elaboração de diversas outras disposições normativas a respeito da campanha eleitoral na grande rede.

---

35 Cambridge Analytica e a nova era Snowden na proteção de dados pessoais: Talvez os escândalos sirvam para fomentar a adoção de tecnologias que permitam uma transparência quase que radical nas campanhas eleitorais digitais. **El País,** [s. l.], 20 mar 2018. Tecnologia. Disponível em: <https://brasil.elpais.com/brasil/2018/03/20/tecnologia/1521582374_496225.html >. Acesso em: 27 nov 2019.

36 **PRIVACIDADE Hackeada.** Direção: Karim Amer, Jehane Noujaim. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. Roteiro: Karim Amer, Pedro Kos, Erin Barnett. EUA: Netflix, 2019. Disponível em: netflix.com. Acesso em: 15 novembro de 2019.

37 **PRIVACIDADE Hackeada.** Direção: Karim Amer, Jehane Noujaim. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. Roteiro: Karim Amer, Pedro Kos, Erin Barnett. EUA: Netflix, 2019. Disponível em: netflix.com. Acesso em: 15 novembro de 2019.

38 PECK PINHEIRO, Patricia. **Direito Digital**. 5ª Ed. São Paulo: Saraiva, 2013. 323 p. p. 149. ISBN 978-85-02-20166-8.

Hoje, a manutenção de perfis em diversas redes sociais de diversos candidatos políticos desafia os limites da conceituação de campanhas eleitorais, pois reinventa o sentido do marketing político. Tal prática, ainda nova no cenário político, recebe o tratamento de propaganda eleitoral antecipada:

> (…) é a venda da imagem de determinado candidato como o mais apto ao exercício da função pública antes do período eleitoral. Dessa forma, é possível manter *sites* (institucional, *blog*, etc.) e perfis em redes sociais (Twitter, Facebook, Youtube etc.) fora do período eleitoral, mas é preciso estar atento que a imagem do possível candidato não esteja sendo vendida, como já foi visto em diversas jurisprudências.[39]

Exemplo dos desdobramentos acima ilustrados no Brasil foram noticiados à época das eleições de 2018. A Folha de São Paulo publicou uma matéria em que indicava a partcipação de empresários em campanhas contra o PT pelo Whatsapp[40], alegando que empresas apoiadoras do então candidato Jair Bolsonaro utilizaram um serviço de “disparos em massa” para impulsionar mensagens contra o PT no WhatsApp. Segundo a reportagem, a prática configuraria doação de campanha por empresas, prática vedada pela legislação eleitoral e não declarada. Cumpre, aqui, salientar a jurisprudência do STF na ADI n. 4.650 de 17/09/2015, responsável por fixar o entendimento da Corte no sentido contrário à possibilidade de recebimento de doações feitas por pessoas jurídicas a campanhas eleitorais. Destaca-se o voto vencedor do Ministro Luiz Fux, que assim dispôs a respeito do tema:

> A doação por pessoas jurídicas a campanhas eleitorais, antes de refletir eventuais preferências políticas, denota um agir estratégico destes grandes doadores, no afã de estreitar suas relações com o poder público, em pactos, muitas vezes, desprovidos de espírito republicano.[41]

Nesse sentido, o atrofiamento de direitos políticos à luz das novas dinâmicas de marketing político, deixado sem supervisão por parte de autoridades competentes

---

39 PECK PINHEIRO, Patricia. **Direito Digital**. 5ª Ed. São Paulo: Saraiva, 2013. 323 p. p. 150. ISBN 978-85-02-20166-8.

40 Empresários bancam campanha contra o PT pelo Whatsapp: Com contratos de R$ 12 milhões, prática viola a lei por ser doação não declarada. **Folha de São Paulo,** Patrícia Campos Mello, 18 out 2018. Disponível em: <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml >. Acesso em: 27 nov 2019.

41 Disponível em: <https://www.conjur.com.br/dl/acordao-doacao-eleitoral-empresas.pdf >. Acesso em: 18 nov 2019.

para a investigação das táticas de desinformação realizadas por empresas durante as eleições de 2018, pode representar sérios entraves a eleições livres e justas no futuro[42].

3.2.4 CRÍTICAS AO ACESSO DE DADOS PESSOAIS POR AUTORIDADES ADMINISTRATIVAS À LUZ DA TEORIA DOS LIMITES DOS LIMITES

Extensa doutrina reconhece a inexistência de direitos fundamentais absolutos. Milita nesse sentido Alexandre de Moraes, que assim versa sobre o tema:

> Os direitos humanos fundamentais, dentre eles os direitos e garantias individuais e coletivos consagrados no art. 5.° da Constituição Federal, não podem ser utilizados como um verdadeiro escudo protetivo da prática de atividades ilícitas, nem tampouco como argumento para afastamento ou diminuição da responsabilidade civil ou penal por atos criminosos, sob pena de total consagração ao desrespeito a um verdadeiro Estado de Direito.
> Os direitos e garantias fundamentais consagrados pela Constituição Federal, portanto, não são ilimitados, uma vez que encontram seus limites nos demais direitos igualmente consagrados pela Carta Magna (Princípio da relatividade ou convivência das liberdades públicas).[43]

Assim, a tutela desses direitos deve proceder nos termos da relativização que estabelecem ante outros direitos e garantias fundamentais igualmente consagradas pela Constituição Federal. O ordenamento jurídico não impõe óbices absolutos a que o legislador restrinja direitos fundamentais. Naturalmente, contudo, configura hipótese igualmente repelida pelo Direito a concentração de poderes suficientes para dizimar direitos fundamentais. Assim, as limitações impostas pelo legislador também não podem fazer desaparecer tais direitos. É este o cerne da teoria dos "limites dos limites" (ou *Schranken-Schranken,* expressão alemã cunhada, segundo leciona Gilmar Mendes[44], por K. H. Wernicke).

Os limites imanentes ou "limites dos limites" se prestam à orientação das limitações estipuladas pelo legislador das quais são destinatários direitos

---

42 **PRIVACIDADE Hackeada.** Direção: Karim Amer, Jehane Noujaim. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. Roteiro: Karim Amer, Pedro Kos, Erin Barnett. EUA: Netflix, 2019. Disponível em: netflix.com. Acesso em: 15 novembro de 2019.

43 MORAES, Alexandre de. **Direito Constitucional**. 13ª Ed. São Paulo: Editora Atlas S.A., 2003. 594 p. p. 48. ISBN 85-224-3352-6.

44 Gilmar Ferreira MENDES; Paulo Gustavo Gonet BRANCO e Inocência Mártires COELHO. **Curso de direito constitucional**. 4ª ed. São Paulo: Saraiva. 2009. 1486 p. p. 348. ISBN 978-85-02-07819-2.

fundamentais de modo a assegurar, a um só tempo, a proteção de um núcleo essencial e o respeito a critérios de clareza, determinação, generalidade e proporcionalidade nas restrições[45].

A colocação do tema de excesso de prerrogativa consubstanciado no acesso de autoridades administrativas a dados pessoais sem a exigência de uma ordem judicial demanda um olhar atento à existência de limites à relativização de direitos fundamentais relevantes ao indivíduo, como o direito à privacidade e intimidade. Nesse sentido, questiona-se a proporcionalidade de certos dispositivos legais a seguir elucubrados na relativização do direito à privacidade.

Em que pese o uso da internet no Brasil, consoante art. 3º do Marco Civil da Internet, seja informado, dentre outros, pelos princípios da proteção da privacidade e dos dados pessoais, não surpreende que os dados referentes aos hábitos de navegação de milhões de internautas brasileiros atraia o interesse das instituições governamentais.

O discurso pelo acesso governamental a dados dos usuários brasileiros da internet é legitimado por bandeiras de diversas naturezas, entre as quais se destaca a segurança nacional. Trata-se de conjuntura que não é exclusiva ao Brasil, vez que, no exterior, o recrudescimento de atentados terroristas com grande visibilidade midiática articulados por intermédio da grande rede[46] e o crescimento no número de *mass shooters*[47] (indivíduos armados que disparam contra multidões procurando maximizar o número de vítimas fatais) instaurou um clima de instabilidade social que ensejou o acirramento do conflito entre privacidade e segurança pública enquanto princípios nos discursos políticos.

Apesar das reações públicas negativas a escândalos como os da interferência eleitoral da *Cambridge Analytica* em 2016[48] ou da espionagem pela

45 Gilmar Ferreira MENDES; Paulo Gustavo Gonet BRANCO e Inocência Mártires COELHO. **Curso de direito constitucional**. 4ª ed. São Paulo: Saraiva. 2009. 1486 p. p. 349. ISBN 978-85-02-07819-2.

46 Why social media and terrorism make such a perfect fit. **The Washington Post,** Max Boot, 16 mar 2019. Global Opinions. Disponível em: <https://www.washingtonpost.com/opinions/2019/03/16/why-social-media-terrorism-make-perfect-fit/ >. Acesso em: 15 out 2019.

47 There have been more mass shootings than days this year. **CBS News,** Jason Silverstein, 15 nov 2019. Disponível em: <https://www.cbsnews.com/news/mass-shootings-2019-more-mass-shootings-than-days-so-far-this-year/ >. Acesso em: 20 nov 2019.

48 Cambridge Analytica, empresa pivô no escândalo do Facebook, é fechada: A pedra de clientes e os altos custos jurídicos relacionados com o vazamento de dados pessoais pela rede social provocaram a decisão de fechar a companhia. **El País,** Pablo Guimón, 02 maio 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/05/02/internacional/1525285885_691249.html >. Acesso em: 15 out 2019.

NSA durante o governo Obama em 2013[49], indicativas de que ainda há expressivo apoio popular à defesa da privacidade como um direito fundamental, em verdade a comodidade e conveniência para o cotidiano de certas aplicações da internet, aliada a uma generalizada desinformação e falta conscientização sobre o tema, contribuíram significativamente para certo esmaecimento da cobertura midiática.

Constata-se que a despeito da insatisfação com a manipulação de dados da vida privada, a sociedade segue encarando com naturalidade os famosos “termos de aceite”. Ao menos é o que sugere o mercado de ações, visto que as empresas mais lucrativas hoje permanecem sendo as que geram, usam e retém informações[50].

A análise do contexto de criação do Marco Civil da Internet, primeira legislação a tratar exclusivamente dos usos da internet, assume local de destaque no debate acerca da legitimação do Estado enquanto órgão fiscalizador das atividades na rede. A elaboração do indigitado diploma legal, afinal, teve início com reações negativas em larga escala ao Projeto de Lei n. 84/1999, cuja redação determinava, com a finalidade de registrar de todas as atividades cibernéticas dos cidadãos brasileiros, o cadastro obrigatório dos usuários da internet.

A proposta tinha o fito de permitir a fiscalização de todas as atividades desenvolvidas ao longo da navegação dos usuários, medida supostamente legitimada pela ameaça provocada por lacunas legislativas que determinariam a prática continuada de crimes cibernéticos[51]. Em apertada síntese, pode-se dizer que “essa postura de vigilância abstrata e universal pelo Estado é que conformou uma mobilização conjuntural e catalisou uma reação em rede por usuários e acadêmicos”[52]

Os debates acerca do tema criaram um amadurecimento da temática que, na esfera legislativa, culminou na criação do Marco Civil da Internet através de um

---

49 NSA violou normas e lei de espionagem milhares de vezes: Agência de Segurança Nacional americana descumpriu regras de proteção à privacidade nos EUA e ultrapassou suas funções legais frequentemente desde 2008, revelam documentos publicados pelo jornal ‘The Washington Post’. **Veja,** [s. l.], 16 ago 2013. Disponível em: <https://veja.abril.com.br/mundo/nsa-violou-normas-e-lei-de-espionagem-milhares-de-vezes/ >. Acesso em: 15 out 2019.

50 **PRIVACIDADE Hackeada.** Direção: Karim Amer, Jehane Noujaim. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. Roteiro: Karim Amer, Pedro Kos, Erin Barnett. EUA: Netflix, 2019. Disponível em: netflix.com. Acesso em: 15 novembro de 2019.

51 Disponível em: <https://teses.usp.br/teses/disponiveis/2/2133/tde-20012015-094628/publico/Dissertacao_Anna_Carolina_Finageiv_Peixoto.pdf >. Acesso em: 21 out 2019. pág. 27

52 Disponível em: <https://teses.usp.br/teses/disponiveis/2/2133/tde-20012015-094628/publico/Dissertacao_Anna_Carolina_Finageiv_Peixoto.pdf >. Acesso em: 21 out 2019. pág. 27

processo legislativo diferenciado, notadamente pelo teor colaborativo de sua elaboração.

Em seu *caput*, o art. 10 do Marco Civil da Internet, abaixo transcrito, traz redação cujo teor enfatiza a proteção do direito à privacidade e intimidade, vez que determina como critérios da guarda e disponibilização dos dados de um indivíduo a preservação de aspectos relevantes à sua vida privada. De mais a mais, cuidou o legislador de proteger o indivíduo do acesso por terceiros ao conteúdo de suas mensagens, determinando que apenas ordem judicial possa quebrar o sigilo do fluxo de suas comunicações privadas.

Optou o legislador, contudo, pela adição de uma exceção para permitir a autoridades administrativas acesso de dados cadastrais que informem qualificação pessoal, filiação e endereço.

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
> (...)
> § 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

O dispositivo em comento, ao legitimar um excesso de prerrogativa por parte de autoridades administrativas, caminha na direção contrária das demais previsões do diploma legal em que se insere. Em vez de proteger as informações do usuário de internet, o Marco Civil, com este dispositivo, passa a ampliar o rol de sujeitos legitimados ao acesso de seus dados, fragilizando a proteção à privacidade do cidadão.

Não sem efeito, a redação do §3º emprega a terminologia “pelas autoridades administrativas que detenham competência legal para sua requisição”. A natural implicação do sentido semântico da frase como foi inserida pelo legislador é existência de autoridades administrativas que não detenham competência legal para requisição do acesso a dados cadastrais. Conquanto a escrita do dispositivo esboce a intenção de uma limitação subjetiva dos agentes legitimados ao acesso das informações do *caput*, é flagrante que a lei resta silente quanto à definição das

autoridades autorizadas e não autorizadas. Trata-se de lacuna legislativa que pode ter como catastrófico resultado a banalização do acesso a dados de usuários por autoridades administrativas não autorizadas.

Nota-se ainda que a legislação não faz menção a qualquer obrigação por parte da autoridade administrativa em informar ao indivíduo que os seus dados foram consultados. O cidadão brasileiro torna-se refém das autoridades administrativas, que podem a qualquer momento investigar seus dados cadastrais sem necessidade de ordem judicial prévia.

À luz do ordenamento jurídico pátrio, não parecem subsistir motivos relevantes para justificar a inexistência de notificação ao titular dos dados cadastrais, mesmo porque a Constituição prevê o *habeas data* como remédio constitucional para assegurar a retificação, complementação e o conhecimento de informações relativas ao impetrante quanto a dados constantes de registros ou bancos de dados de entidades governamentais ou de caráter público.

Nos termos do art. 8º da Lei 9.507/1997, que regula o *habeas data*, a petição inicial da ação constitucional indigitada deve ser instruída de prova da recusa do órgão público em conceder acesso, retificar ou complementar os dados:

> Art. 8° A petição inicial, que deverá preencher os requisitos dos arts. 282 a 285 do Código de Processo Civil, será apresentada em duas vias, e os documentos que instruírem a primeira serão reproduzidos por cópia na segunda.
>
> Parágrafo único. A petição inicial deverá ser instruída com prova:
>
> I – da recusa ao acesso às informações ou do decurso de mais de dez dias sem decisão;
>
> II – da recusa em fazer-se a retificação ou do decurso de mais de quinze dias, sem decisão; ou
>
> III – da recusa em fazer-se a anotação a que se refere o § 2° do art. 4° ou do decurso de mais de quinze dias sem decisão.

Sucede que o indivíduo que teve seus dados cadastrais investigados digitalmente pela autoridade administrativa dificilmente será notificado desta investigação, dado que, conforme acima elucubrado, as autoridades administrativas não estão obrigadas à notificação da consulta ao titular dos dados cadastrais. Como pode-se esperar que o indivíduo, ignorante tanto da consulta enquanto fato quanto

do órgão que a realizou, seja capaz de aduzir em juízo prova da recusa do órgão público em realizar uma das três hipóteses descritas?

Trata-se de conjuntura que avilta a garantia constitucional do *habeas data* às informações administrativamente situadas sobre o titular das credenciais e que fragiliza os direitos do usuário da internet, tornando o ambiente cibernético propício a abusos por parte do Poder Público.

Face ao exposto, delimitam-se com nitidez os contornos do problema de acesso governamental a dados pessoais à luz da teoria dos limites dos limites, vez que: a) não houve observância a critérios de proporcionalidade, posto que o acesso a dados pessoais por parte de autoridades administrativas sem a necessidade de uma autorização judicial configura verdadeiro excesso de prerrogativa; b) tampouco houve clareza na limitação do direito fundamental à privacidade, vez que a legislação não esclarece quais autoridades administrativas estão legitimadas ao acesso dos dados acima indigitados.

Acerca da temática de *mass surveillance* governamental, paralelos perturbadores podem ser traçados com os escândalos de espionagem americana denunciados pelo ex-contratado da NSA (National Security Agency) Edward Snowden durante o governo Obama. Em 2013, Snowden vazou informações sigilosas da NSA, agência de segurança nos Estados Unidos, denunciando a existência de uma vasta rede de espionagem. A declaração do delator, na época, foi assim noticiada nos jornais:

> Eu estou disposto a me sacrificar porque eu não posso, em sã consciência, deixar que o governo dos Estados Unidos destrua a privacidade, a liberdade de Internet e os direitos básicos de pessoas em todo o mundo, tudo em nome de um maciço serviço secreto de vigilância que eles estão desenvolvendo.[53]

Com efeito, os vazamentos de Snowden contribuíram de maneira definitiva para a deflagração de inúmeros debates acerca da dicotomia entre privacidade e segurança, gerando discussões tanto fora quanto dentro dos Estados Unidos, onde

53 Entenda o caso de Edward Snowden, que revelou espionagem dos EUA: Procurado pelos Estados Unidos, ex-técnico da CIA obteve asilo da Rússia. Caso gerou crise para o governo Obama e debate sobre privacidade online. **Portal de Notícias G1,** [s. l.], 02 jul 2013. Mundo. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html >. Acesso em: 16 nov 2019.

os cidadãos demonstraram-se revoltados com a constatação de que a agência americana coletava dados privados armazenados em quase 5 bilhões de celulares[54]. Os documentos vazados indicaram que a NSA, utilizando-se dos programas à sua disposição, podiam rastrear a localização de indivíduos, bem como suas trajetórias passadas, assim como analisar padrões de comportamento através de informações pessoais que incluíam relacionamentos com outros usuários na rede[55].

Guardadas as devidas proporções e consideradas as diferenças com a realidade brasileira, a experiência americana parece demonstrar que a segurança proporcionada pela interferência emanada do Poder Público cobra um preço caro em liberdades civis. O acesso desregulamentado a dados de usuários da internet por entes governamentais cria um contexto propício ao abuso de direitos fundamentais à privacidade e intimidade, conjuntura repelida pela Constituição Federal de 1988, e é tópico de grande relevância para o presente projeto, conforme demonstrado, vez que o Marco Civil da Internet institucionalizou desnecessariamente práticas que podem culminar na violação de direitos fundamentais.

54 Snowden documents show NSA gathering 5bn cell phone records daily. **The Guardian,** Paul Lewis, 05 dez 2013. World. Disponível em: <https://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden >. Acesso em: 16 nov 2019.

55 Snowden documents show NSA gathering 5bn cell phone records daily. **The Guardian,** Paul Lewis, 05 dez 2013. World. Disponível em: <https://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden >. Acesso em: 16 nov 2019.

4. O FUTURO DAS APLICAÇÕES DE INTERNET E DO EMPREGO DE ALGORITMOS NO BRASIL: CONSIDERAÇÕES COM BASE EM EXPERIÊNCIAS NACIONAIS E ESTRANGEIRAS

Subestimar o potencial das novas tecnologias de informação em alterar significativamente o papel do Poder Público e os instrumentos de que dispõe este poder no atendimento interesses sociais é equívoco que não tem mais espaço na era dos algoritmos.

4.1. GOVERNANÇA ELETRÔNICA

As ondas de evolução tecnológica consistentes na criação de novas plataformas e aplicações da grande rede, à primeira vista, podem parecer destinadas ao consumo das massas apenas. A realidade, contudo, é que a marcha de alterações técnico-científicas tem operado mudanças em áreas diversas e por vezes até inusitadas.

Para o presente projeto, que aborda os desdobramentos jurídicos dos usos da internet, importam em particular as alterações operadas sobre ramos do Direito no Brasil, vez que parte substancial da discussão sobre o uso consciente e democrático da grande rede passa por uma análise prévia das aplicações pelas quais o Brasil demonstra ou poderia demonstrar interesse.

Nesta senda, a Administração Pública compreende área de grandes possibilidades para aplicação das tecnologias de informação e comunicação, e por razões bastante lógicas.

Por um lado, dentre os princípios constitucionais que informam a Administração Pública, destacam-se a proporcionalidade, impessoalidade, eficiência e finalidade como os princípios que melhor se aproveitam das tecnologias de comunicação e informação, dado que são princípios orientados para o tratamento impessoal dos administrados por um Poder Público eficiente e guiado pelo interesse público. Dessarte, a oferta de serviços públicos *online* acessíveis a qualquer momento do dia para o atendimento personalizado de parcela significativa da

população não pode ser descrita como menos do que uma verdadeira revolução dos moldes da gestão pública.

Por outro lado, a revolução logística proporcionada pelo advento de dispositivos de armazenamento de dados e a banalização da oferta de conexão de banda larga cada vez mais rápida **(fonte)** possibilitou um significativo corte de gastos à Administração Pública na forma de redução da mão de obra e de gastos de manutenção. No cerne do debate pela aplicação das novas tecnologias da informação na Administração Pública repousa o interesse por uma gestão pública centrada na eficácia e eficiência, robustamente lastreado em dados que expressam o potencial dessas tecnologias na melhoria dos serviços públicos.

O termo “governança eletrônica” remete precisamente a uma realidade de reformas administrativas orientadas no sentido de facilitar e aperfeiçoar, com o uso das tecnologias de informação, a prestação de serviços públicos pelo Poder Administrativo.

Quando fala-se em governança eletrônica, duas abordagens básicas se compementam[56]; a primeira é centrada na oferta de serviços públicos *online*, colocando o “governo em um só lugar”[57] e aumentando, com isso a eficiência administrativa, visto que o “governo se torna menor, mais barato, mais rápido e mais fácil de gerenciar”[58]. A segunda consiste no saneamento da “exclusão digital”, visto que uma parcela significativa da população, sobretudo em países em desenvolvimento, tem acesso limitado à internet e, por consequência, às tecnologias da informação e comunicação, permanecendo à margem de um processo que, sem a interferência de políticas públicas adequadas, pode produzir uma realidade em que indivíduos com e sem acesso à internet são respectivamente “mais” ou “menos” cidadãos.

4.2. O APERFEIÇOAMENTO DOS SERVIÇOS PÚBLICOS

56 Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf>. Acesso em: 19 out 2019. p. 36

57 Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf>. Acesso em: 19 out 2019. p. 36

58 Lawson, apud Klaus Frey. Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf>. Acesso em: 19 out 2019. p. 36

Até pouco tempo atrás, as limitações de ordem prática e técnica na gestão de processos demandava, para cada Vara da Justiça, um correspondente Cartório onde serventuários da justiça auxiliavam o juiz na movimentação do processo. Com o aperfeiçoamento das tecnologias de armazenamento de dados, a demanda por mão de obra para auxiliar na prestação jurisdicional deu lugar ao surgimento dos primeiros Cartórios Integrados, permitindo não apenas uma redução substancial no quadro de profissionais encarregados de auxiliar as Varas, mas também a unificação dos Cartórios, que sob nova dinâmica, passam a auxiliar três, quatro ou mais Varas sem prejuízo da organização.

Após dois anos de instalação dos Cartórios Integrados nas Varas de Relações de Consumo da Comarca de Salvador, informações divulgadas pela Diretoria de Primeiro Grau (DPG) revelaram redução expressiva da taxa de congestionamento das Varas em comparação ao período anterior á junção das unidades que compõem o sistema dos integrados.

Lista de Cartórios Integrados de Relações de Consumo	**Taxa de congestionamento das varas reunidas antes da união**	**Taxa de congestionamento das varas reunidas após da união (dados de 2018)**
1º Cartório Integrado (reúne 2ª, 5ª, 10ªe 11ª Varas de Relações de Consumo de Salvador)	97,53%	81,55%
2º Cartório Integrado (reúne 8ª, 9ª, 15ª e 19ª Varas de Relações de Consumo de Salvador)	99,58%	73,81%
3º Cartório Integrado (reúne 3ª, 6ª, 14ª e 16ª Varas de Relações de Consumo de Salvador)	97,30%	59,78%
4º Cartório Integrado (reúne 1ª, 7ª, 12ª e 13ª Varas de Relações de Consumo de Salvador)	99,29%	85,88%
5º Cartório Integrado (reúne 4ª, 17ª, 18ª e 20ª Varas de Relações de Consumo de Salvador)	98,49%	83,03%

Dados disponíveis em: <http://www5.tjba.jus.br/portal/cartorios-integrados-completam-dois-anos-com-resultados-expressivos-para-o-justica-em-numeros/>. Acesso em: 10 out 2019.

4.3. COMUNIDADES VIRTUAIS LOCAIS E AS POTENCIALIDADES DE EMPODERAMENTO MUNICIPAL

Outro exemplo de aplicação das novas tecnologias de comunicação à realidade administrativa consiste na criação de comunidades virtuais locais que estimulam a participação do cidadão comum na gestão urbana. A possibilidade de acesso direto a plataformas de comunicação imediata e pública com agentes da política local contribui para o desenvolvimendo de uma "cidadania digital" ou "interativa"[59]. Resultados dessa iniciativa podem ser observadas em municipalidades europeias, onde os esforços na democratização do acesso à gestão pública rendeu a criação de comunidades virtuais como o Conselho Jovem de Espoo, organização capaz de submeter moções diretamente à assembleia municipal[60].

Podemos estabelecer alguns paralelos com essa iniciativa no caso brasileiro. Não raro, diversas instituições públicas administram e gerenciam, hoje, páginas e perfis nas mídias sociais. Em alguns cliques, o cidadão brasileiro pode acessar *posts* do Conselho Nacional de Justiça em quaisquer de suas várias redes sociais, como perfis no Facebook, Instagram e até mesmo um canal no Youtube. As postagens são institucionalmente condizentes com a função do órgão, geralmente voltadas à conscientização de direitos úteis ao cotidiano do cidadão médio, como direitos do consumidor, ou instrutivos no modo de denúncia de crimes como violência doméstica, indicando números de telefone disponíveis para esta finalidade.

O hábito de gerenciar mídias sociais não se limita à esfera federal das instituições públicas, de modo que podemos encontrar perfis no Instagram da Polícia Militar do Estado da Bahia[61], da Prefeitura de Salvador[62] e mesmo um perfil exclusivo

59 Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf>. Acesso em: 27 out 2019. pág. 41

60 Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf >. Acesso em: 27 out 2019. pág. 42

61 Disponível em: <https://www.instagram.com/pmdabahia/?hl=pt-br >. Acesso em: 27 out 2019.

62 Disponível em: <https://www.instagram.com/prefsalvador/?hl=pt-br >. Acesso em: 27 out 2019.

do Prefeito de Salvador[63], possibilitando ao usuário, ainda que apenas em tese, uma linha de contato direta com a maior instância executiva a nível municipal.

Com o adequado incentivo político, esta iniciativa poderia, se desenvolvida no Brasil, garantir uma maior democratização na participação política nas esferas municipal, estadual e federal, possivelmente facilitando o processo de comunicação com os administrados. O sucesso de uma experiência como essa, porém, demandaria não apenas esforços na criação de uma plataforma sólida de contato com as instituições públicas, mas também o desenvolvimento de políticas públicas capazes de garantir o acesso à internet para as populações mais desfavorecidas. Nas cidades europeias, o acesso à rede costuma ser franqueado em pontos de acesso público à internet:

> Por outro lado, em Bologna, mas sobretudo em todas as cidades finlandesas de Helsinki, Espoo e Tampere, o acesso gratuito à Internet foi posto à disposição da população em quase todas as bibliotecas públicas. Nas cidades finlandesas, as bibliotecas são pontos de referência cultural aonde as pessoas não vão apenas para ler livros ou jornais, mas acima de tudo para se encontrar e conversar em um café ou restaurante próximos, ouvir ou tocar música. As bibliotecas são locais de intensa interação social e são altamente valorizadas pelos cidadãos. Além disso, há outros locais com aceso público à Internet para grupos específicos, como por exemplo para a população idosa. Tanto em Helsinki como em Bologna, há também pontos de acesso público no centro das cidades, que – no caso de Bologna – servem também como centros de informação ao cidadão e – no caso de Helsinki – como um grande centro de comunicação. A existência de uma cultura que valoriza o conhecimento, que existe na Europa e sobretudo na Finlândia, tem que ser considerada uma vantagem fundamental desses países para implementar estratégias de e-governança.[64]

63 Disponível em: <https://www.instagram.com/acmnetooficial/?hl=pt-br >. Acesso em: 27 out 2019.

64 Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf>. Acesso em: 20 nov 2019. pág. 40

5. CONCLUSÃO

No curso da presente monografia, foram analisados uma série de desdobramentos próprios a aplicações de rede que geram efeitos jurídicos negativos e positivos. Coube a este projeto detalhar, onde possível, as ameaças representadas pela interferência não regulamentada de novas tecnologias, demonstrando os motivos pelos quais alguns usos da internet, sobretudo aqueles concentrados no uso de dados pessoais, caminham na contramão dos princípios e direitos estabelecidos pelo direito digital no uso consciente e saudável da grande rede.

Assim, com o fito de provocar reflexões acerca dos usos da internet, optou-se por uma análise da legislação relevante ao tema, oportunidade na qual se delinearam os princípios informadores dos usos de internet e de proteção dos dados pessoais. Este trabalho basilar foi essencial às partes seguintes da monografia, pois munidos de uma ideia geral acerca do que o legislador ambicionou tutelar, várias inferências e críticas puderam ser traçadas sobre as violações perpetradas por sites, aplicativos e fenômenos digitais, como as mídias sociais, a implementação não supervisionada de algoritmos, a fé cega no Big Data e a disseminação de *fake news.*

Igualmente vital foi o processo de colocação do tema, pois faz-se imprescindível ao adequado enfrentamento das questões levantadas pela monografia a constatação de os problemas de aplicação da internet não se resumem ao *micro* – estão, pelo contrário, ligados sempre a um contexto maior, de modo que combate às violações constitucionais emanadas do surgimento de novos hábitos e práticas virtuais exige uma atenção ao *macro*.

Isso decorre da natureza integrada das novas tecnologias de comunicação e informação, que estão frequentemente relacionadas a fatores tanto extrínsecos quando intrínsecos à grande rede. Não é outra a razão pela qual discute-se, por exemplo, a existência de “algoritmos racistas” conforme explicado aacima, o que sozinho já é tema de sobra para outra dissertação.

A fim de que se assegure um cenário mais democrático e participativo na internet, sem a mercantilização exacerbada de dados pessoais e o esmaecimento da vida privada, tão vital à expressão da personalidade humana, novas técnicas

mais preocupadas com a manutenção de direitos fundamentais até então ignorados devem surgir.

Quando indispensável ao aperfeiçoamento de serviços públicos e efetivação de outros direitos, a coleta de dados por parte de entes governamentais, contanto que atinente a limites claros estabelecidos em lei, pode, contanto que direcionada ao atendimento da vontade popular, impulsionar de diversas maneiras a criação de espaços de discussão de políticas públicas verdadeiramente colaborativos.

As possibilidades de inovação no que tange o setor público são muitas e variadas, e incluem a possiblidade de incremento da autonomia das municipalidades, tendência já observada na política nacional; o aperfeiçoamento da austeridade fiscal permitindo o corte de gastos com pessoal; destinação estratégica de recursos públicos com base em interpretações da realidade fática oriundas do acompanhamento supervisionado de algoritmos; o planejamento de políticas públicas direcionadas às parcelas efetivamente mais necessitadas da população com base na coleta de dados dos administrados, preferencialmente adotando métodos impessoais e sempre em consonância com a LGDP; entre muitas outras alternativas que os usos e aplicações da internet podem promover de maneira positiva.

Por outro lado, o ordenamento jurídico e os operadores do Direito devem zelar pelo rechaço às aplicações da internet que se orientem *contra legem*, vez que, conforme explicitado, as novas tecnologias de informação e comunicação representam riscos significativos a instituições demasiado caras ao Estado democrático de direito.

A monografia, espera-se, despertou nos leitores um senso crítico acerca dos usos da internet, contextualizando a aplicação do direito à realidade prática da sociedade da informação. Nos encontramos inteiramente mergulhados nas novas aplicações de rede, e só recentemente começamos a sentir os efeitos nocivos provocados pelo fluxo descontrolado de informações e tráfego incessante de dados pessoais. Assim, muito há ainda para se debater sobre o tema nos anos vindouros, sobretudo com o surgimento de cada vez mais tecnologias e hábitos próprios da vida cibernética.

REFERÊNCIAS

LEGISLAÇÃO

BRASIL. **Constituição** (1988). Constituição da República Federativa do Brasil. Brasília, DF: Senado Federal : Centro Gráfico, 1988, 292 p.

BRASIL. **Lei 12.965 de 23 de abril de 2014 (Marco Civil da Internet)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 31 out. 2019

BRASIL. **Lei Ordinária nº 13.709/2018, de 14 de agosto de 2018. (Lei Geral de Proteção de Dados Pessoais)**. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm> Acesso em: 23 set. 2019.

BRASIL. **Lei 8078/90 (Código de Defesa do Consumidor)** . Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8078.htm>. Acesso em: 31 out 2019

JURISPRUDÊNCIA

Disponível em: <https://www.conjur.com.br/dl/acordao-doacao-eleitoral-empresas.pdf>. Acesso em: 18 nov 2019.

LIVROS

SANTOS, Milton. **Por uma outra globalização: do pensamento único à consciência universal.** 10. ed. Rio de Janeiro: Record, 2003.

SIEGEL, Eric. **Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die.** John Wiley & Sons, Inc.: New Jersey, 2013.

DINIZ, Maria Helena. **Código Civil Anotado**. 17ª Ed. São Paulo: Saraiva, 2014. 1542 p. ISBN 978-85-02-21537-5.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 25ª Ed. São Paulo: Malheiros Editores Ltda, 2005. 925 p. ISBN 85.7420.868-5

PECK PINHEIRO, Patricia. **Direito Digital.** 5ª Ed. São Paulo: Saraiva, 2013. 323 p. ISBN 978-85-02-20166-8.

MORAES, Alexandre de. **Direito Constitucional**. 13ª Ed. São Paulo: Editora Atlas S.A., 2003. 594 p. ISBN 85-224-3352-6.

REPORTAGEM DE JORNAIS

NATURAL GEOGRAPHIC. Grandes Marcos da Fotografia no Espaço. Disponível em: <https://www.natgeo.pt/photography/2018/02/grandes-marcos-da-fotografia-no-espaco?image=6428 > Acesso em: 20 out. 2019.

'Fake News' é eleita palavra do ano e vai ganhar menção em dicionário britânico: palavra foi amplamente usada pelo presidente dos EUA, Donald Trump, na campanha eleitoral, e acabou se disseminando pelo mundo todo. Portal de Notícias G1, 02 nov. 2017. Educação. Disponível em: <https://g1.globo.com/educacao/noticia/fake-news-e-eleita-palavra-do-ano-e-vai-ganhar-mencao-em-dicionario-britanico.ghtml>. Acesso em: 21 out. 2019.

New words list October 2019. OED. 2019. Disponível em: <https://public.oed.com/updates/new-words-list-october-2019/ >. Acesso em: 21 out. 2019

The Real Story of 'Fake News': The term seems to have emerged around the end of the 19th century. Merriam-webster. [s. d.]. Disponível em: <https://www.merriam-webster.com/words-at-play/the-real-story-of-fake-news>. Acesso em: 21 out. 2019

'Busca sob censura': por que o suposto plano do Google para chegar à China é polêmico. Portal de Notícias G1, [s. l.], 2 ago 2018. Disponível em: <https://www.bbc.com/portuguese/salasocial-45042713 >. Acesso em: 27 nov 2019.

15 coisas que são proibidas na Coreia do Norte: No país mais fechado do mundo não se pode usar calça jeans, celebrar o Natal ou conversar com estrangeiros. Veja, Angela Nunes, 01 set 2017. Disponível em: <https://veja.abril.com.br/mundo/15-coisas-que-sao-proibidas-na-coreia-do-norte/ >. Acesso em: 27 nov 2019.

How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read. Forbes, Bernard Marr, 21 mai 2019. Disponível em: <https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#3eae63de60ba >. Acesso em: 27 nov 2019.

Após escândalo, Facebook muda termos de uso e política de privacidade: Uma das novidades é que a rede social vai deixar mais claro quais empresas fazem parte do grupo, como WhatsApp, Instagram e Oculos. Veja, [s. l.], 04 abr 2018. Disponível em: <https://veja.abril.com.br/economia/apos-escandalo-facebook-vai-mudar-termos-de-uso-e-politica-de-dados/ >. Acesso em: 27 nov 2019.

Click to agree with what? No one reads terms of service, studies confirm: apparently losing rights to data and legal recourse is not enough of a reason to inspect online contracts. So how can websites get users to read the fine print? The Guardian, David Berreby, 03 mar 2017. Disponível em: <https://www.theguardian.com/technology/2017/mar/03/terms-of-service-online-contracts-fine-print >. Acesso em: 27 nov 2019.

Inteligência artificial: Por que as tecnologias de reconhecimento facial são tão contestadas: As ferramentas de inteligência artificial são tão boas quanto o banco de dados que usam para funcionar, mas e se essas informações forem enviesadas? Portal de Notícias G1, [s. l.], 06 jul 2019. Disponível em: <https://g1.globo.com/mundo/noticia/2019/07/06/inteligencia-artificial-por-que-as-tecnologias-de-reconhecimento-facial-sao-tao-contestadas.ghtml >. Acesso em: 27 nov 2019.

Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter: Attempt to engage millenials with artificial intelligence backfires hours after launch, with TayTweets account citing Hitler and supporting Donald Trump. The Guardian, Elle Hunt, 24 mar 2016. Disponível em: <https://www.theguardian.com/technology/2016/mar/24/tay-microsofts-ai-chatbot-gets-a-crash-course-in-racism-from-twitter >. Acesso em: 27 nov 2019.

Racial bias found in widely used health care algorithm: an estimated 200 million people are afected each year by similar tools that are used in hospital networks. NBC News, Quinn Gawronski, 06 nov 2019. Disponível em: <https://www.nbcnews.com/news/nbcblk/racial-bias-found-widely-used-health-care-algorithm-n1076436 >. Acesso em: 27 nov 2019.

Taxa de negros mortos pela polícia de SP é 3 vezes a de brancos, diz estudo: Policiais envolvidos, entretanto, são, em sua maioria, brancos (79%). Professora da UFSCar fala em 'racismo institucional'; SSP analisará dados. Portal de Notícias G1, Thiago Reis, 26 mar 2014.. Disponível em: <http://g1.globo.com/sao-paulo/noticia/2014/03/taxa-de-negros-mortos-pela-policia-de-sp-e-3-vezes-de-brancos-diz-estudo.html >. Acesso em: 27 nov 2019.

Police officers raise concerns about 'biased' AI data. BBC News, [s. l.], 16 set 2019. Technology. Disponível em: <https://www.bbc.com/news/technology-49717378 >. Acesso em: 27 nov 2019.

Cambridge Analytica e a nova era Snowden na proteção de dados pessoais: Talvez os escândalos sirvam para fomentar a adoção de tecnologias que permitam uma transparência quase que radical nas campanhas eleitorais digitais. El País, [s. l.], 20 mar 2018. Tecnologia. Disponível em: <https://brasil.elpais.com/brasil/2018/03/20/tecnologia/1521582374_496225.html >. Acesso em: 27 nov 2019.

Empresários bancam campanha contra o PT pelo Whatsapp: Com contratos de R$ 12 milhões, prática viola a lei por ser doação não declarada. Folha de São Paulo, Patrícia Campos Mello, 18 out 2018. Disponível em: <https://www1.folha.uol.com.br/poder/2018/10/empresarios-bancam-campanha-contra-o-pt-pelo-whatsapp.shtml >. Acesso em: 27 nov 2019.

Why social media and terrorism make such a perfect fit. The Washington Post, Max Boot, 16 mar 2019. Global Opinions. Disponível em: <https://www.washingtonpost.com/opinions/2019/03/16/why-social-media-terrorism-make-perfect-fit/ >. Acesso em: 15 out 2019.

There have been more mass shootings than days this year. CBS News, Jason Silverstein, 15 nov 2019. Disponível em: <https://www.cbsnews.com/news/mass-shootings-2019-more-mass-shootings-than-days-so-far-this-year/ >. Acesso em: 20 nov 2019.

Cambridge Analytica, empresa pivô no escândalo do Facebook, é fechada: A pedra de clientes e os altos custos jurídicos relacionados com o vazamento de dados pessoais pela rede social provocaram a decisão de fechar a companhia. El País, Pablo Guimón, 02 maio 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/05/02/internacional/1525285885_691249.html >. Acesso em: 15 out 2019.

NSA violou normas e lei de espionagem milhares de vezes: Agência de Segurança Nacional americana descumpriu regras de proteção à privacidade nos EUA e ultrapassou suas funções legais frequentemente desde 2008, revelam documentos publicados pelo jornal 'The Washington Post'. Veja, [s. l.], 16 ago 2013. Disponível em: <https://veja.abril.com.br/mundo/nsa-violou-normas-e-lei-de-espionagem-milhares-de-vezes/ >. Acesso em: 15 out 2019.

Entenda o caso de Edward Snowden, que revelou espionagem dos EUA: Procurado pelos Estados Unidos, ex-técnico da CIA obteve asilo da Rússia. Caso gerou crise para o governo Obama e debate sobre privacidade online. Portal de Notícias G1, [s. l.], 02 jul 2013. Mundo. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html >. Acesso em: 16 nov 2019.

Snowden documents show NSA gathering 5bn cell phone records daily. The Guardian, Paul Lewis, 05 dez 2013. World. Disponível em: <https://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden >. Acesso em: 16 nov 2019.

Snowden documents show NSA gathering 5bn cell phone records daily. The Guardian, Paul Lewis, 05 dez 2013. World. Disponível em: <https://www.theguardian.com/world/2013/dec/04/nsa-storing-cell-phone-records-daily-snowden >. Acesso em: 16 nov 2019.

ARTIGOS

Disponível em: <https://kb.osu.edu/bitstream/handle/1811/72839/ISJLP_V4N3_543.pdf >. Acesso em: 27 nov 2019.

TRABALHOS ACADÊMICOS

Ferraz Júnior, T. S. (1993). Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. Revista Da Faculdade De Direito, Universidade De São Paulo, 88, 439-459. p. 448. Disponível em: <http://www.revistas.usp.br/rfdusp/article/view/67231/69841>. Acesso em: 20 nov 2019.

Disponível em: <https://www.nyulawreview.org/wp-content/uploads/2019/06/NYULawReview-94-3-ODonnell.pdf >. Acesso em: 27 nov 2019.

Disponível em: <https://teses.usp.br/teses/disponiveis/2/2133/tde-20012015-094628/publico/Dissertacao_Anna_Carolina_Finageiv_Peixoto.pdf >. Acesso em: 21 out 2019. pág. 27

Disponível em: <http://www.egov.ufsc.br/portal/sites/default/files/anexos/19407-19408-1-PB.pdf>. Acesso em: 19 out 2019. p. 36

DOCUMENTÁRIOS

PRIVACIDADE Hackeada . Direção: Karim Amer, Jehane Noujaim. Produção: Karim Amer, Pedro Kos, Geralyn Dreyfous, Judy Korin. Roteiro: Karim Amer, Pedro Kos, Erin Barnett. EUA: Netflix, 2019. Disponível em: netflix.com. Acesso em: 12 set. 2019.

SITES

Disponível em: <https://www.instagram.com/pmdabahia/?hl=pt-br >. Acesso em: 27 out 2019.

Disponível em: <https://www.instagram.com/prefsalvador/?hl=pt-br >. Acesso em: 27 out 2019.

Disponível em: <https://www.instagram.com/acmnetooficial/?hl=pt-br >. Acesso em: 27 out 2019.