UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS JURÍDICAS

DEPARTAMENTO DE DIREITO

ANA CLÁUDIA HOSTERT

PROTEÇÃO DE DADOS PESSOAIS NA INTERNET: A NECESSIDADE DE LEI ESPECÍFICA NO ORDENAMENTO JURÍDICO BRASILEIRO

Florianópolis (SC)

2018

Ana Cláudia Hostert

PROTEÇÃO DE DADOS PESSOAIS NA INTERNET: A NECESSIDADE DE LEI ESPECÍFICA NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada à Universidade Federal de Santa Catarina para obtenção do título de Bacharel em Direito

Orientadora: Profa. Dra. Liz Beatriz Sass

Florianópolis
2018

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS JURÍDICAS

COORDENADORIA DE MONOGRAFIA

ATA DE SESSÃO DE DEFESA DE TCC

Aos **05** dias do mês de **julho** do ano de 2018, às **09** horas e **30** minutos, na Sala 111 do CCJ, foi realizada a defesa pública do Trabalho de Conclusão de Curso (TCC) intitulado **"Proteção de dados pessoais na internet: a necessidade de lei específica no ordenamento jurídico brasileiro",** elaborado pela acadêmica **Ana Cláudia Hostert**, matrícula **13200044**, composta pelos membros **Liz Beatriz Sass, Sarah Helena Linke e Gustavo Becker Monteiro**, abaixo assinados, obteve a aprovação com nota 9,5 (nove e meio), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

(X) Aprovação Integral
( ) Aprovação Condicionada aos seguintes reparos, sob fiscalização do Prof. Orientador

Florianópolis, **05 de julho de 2018**.

Liz Beatriz Sass
Professora Orientadora

Sarah Helena Linke
Membro de Banca

Gustavo Becker Monteiro
Membro de Banca

UNIVERSIDADE FEDERAL DE SANTA CATARINA

CENTRO DE CIÊNCIAS JURÍDICAS

COLEGIADO DO CURSO DE GRADUAÇÃO EM DIREITO

TERMO DE APROVAÇÃO

O presente Trabalho de Conclusão de Curso, intitulado "**Proteção de dados pessoais na internet: a necessidade de lei específica no ordenamento jurídico brasileiro**", elaborado pela acadêmica **Ana Cláudia Hostert**, defendido em **05/07/2018** e aprovado pela Banca Examinadora composta pelos membros abaixo assinados, obteve aprovação com nota 9,5 (nove e meio), cumprindo o requisito legal previsto no art. 10 da Resolução nº 09/2004/CES/CNE, regulamentado pela Universidade Federal de Santa Catarina, através da Resolução nº 01/CCGD/CCJ/2014.

Florianópolis, 05 de Julho de 2018

Liz Beatriz Sass
Professor Orientador

Sarah Helena Linke
Membro de Banca

Gustavo Becker Monteiro
Membro de Banca

Universidade Federal de Santa Catarina

Centro de Ciências Jurídicas

COORDENADORIA DO CURSO DE DIREITO

TERMO DE RESPONSABILIDADE PELO INEDITISMO DO TCC E ORIENTAÇÃO IDEOLÓGICA

Aluna: Ana Cláudia Hostert
RG:
CPF:
Matrícula: 13200044
Título do TCC: Proteção de dados pessoais na internet: a necessidade de lei específica no ordenamento jurídico brasileiro
Orientador(a): Liz Beatriz Sass

Eu, Ana Cláudia Hostert acima qualificada; venho, pelo presente termo, assumir integral responsabilidade pela originalidade e conteúdo ideológico apresentado no TCC de minha autoria, acima referido

Florianópolis, 05 de julho de 2018.

Ana C. Hostert

ANA CLÁUDIA HOSTERT

A Deus e aos meus pais, pelo amor constante. Aos meus avós e tio Xande, pelo apoio imensurável, preocupação e afeto.

AGRADECIMENTOS

E mais uma etapa da vida se conclui. Um período de 5 anos, que vale dizer, se passaram voando. Eu não seria a pessoa que vos escreve sem os aprendizados, convívios, aulas, puxões de orelha e conselhos que recebi durante esse tempo. Nada disso seria possível sem as pessoas que tanto me ajudaram.

Agradeço especialmente à minha orientadora, professora Liz Beatriz Sass, pela disposição, por não medir esforços em sua assistência, e por instigar um tema tão cativante já em suas aulas.

Aos meus pais, Elke Hostert e Gérson Rodolfo Hostert, por serem exemplo de amor, carinho e caráter. Obrigada por serem as minhas duas bases tão autênticas e amorosas.

Ao meu tio, Alexandre Hostert, pois foi meu segundo pai! Obrigada por todo o apoio, preocupação e pelas palavras certeiras.

Aos meus avós, Alzira Hostert e Waldemar Hostert, por serem os melhores avós que poderia pedir. Obrigada pela ajuda, apoio, carinho e preocupação.

E por fim, aos meus irmãos, Gérson Rodolfo Hostert Junior e Ester Jéssica Hostert, por serem meus alicerces.

RESUMO

A proteção aos dados pessoais é tema muito discutido na atualidade. Ela abarca desde direitos fundamentais como a proteção à intimidade e a vida privada e avança até ao seu entendimento de um direito autônomo. Enfrenta questões inéditas acerca de seu uso, decorrentes da introdução de novas tecnologias e da internet, além da mudança de paradigmas nas relações sociais e na economia. O objetivo deste trabalho é demonstrar a necessidade urgente de resguardar a privacidade e regulamentar o uso dos dados pessoais colhidos na internet através de lei específica. Nesse intuito, a partir de pesquisa bibliográfica, e documental, por meio de notícias, artigos e relatórios realizados acerca do tema, o trabalho trata, num primeiro tópico acerca dos conceitos de privacidade e intimidade e da proteção de dados pessoais como um direito autônomo e fundamental, para, num segundo tópico, demonstrar as diversas utilizações dos dados coleados. Por fim, o terceiro tópico aborda o Regulamento 2016/679 da União Europeia, o Marco Civil da Internet no Brasil, o Projeto de Lei n° 5.276/2016, o Projeto de Lei n° 330/2013, Projeto de Lei n° 4.060/2012, e o Projeto de Lei n° 53/2018.

Palavras-chave: Proteção de Dados Pessoais. Internet. Regulamentação.

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Com o advento de inúmeros escândalos envolvendo vigilância, redes sociais, empresas privadas, vendas de dados pessoais - frisa-se muitos colhidos sem consentimento – e até utilização por partidos e candidatos políticos, vê-se a incontestável necessidade de regulamentação da utilização dos dados pessoais visando sua proteção e privacidade.

Tem-se que o problema é ainda mais complexo uma vez que as pessoas não tem conhecimento da quantidade de informações que despejam na internet, e muito menos o que acontece posteriormente.

A noção de urgência e seriedade para o assunto, já que recente, está presente somente aos que tem algum contato com o assunto, qual seja: poucas pessoas. Apesar do tema envolver toda a sociedade e referir-se a direitos fundamentais o não conhecimento e, assim, a não prioridade na solicitação de medidas, direciona para a possibilidade dos que tem acesso a esses dados agirem da maneira que lhes é conveniente – ou seja, sem considerar quaisquer direitos do titular dos dados pessoais.

Nesse sentido, destaca-se que no Brasil não há lei que regulamente especificamente acerca da coleta, guarda, consentimento de dados pessoais, como devem ser os procedimentos das empresas e do governo, quais as responsabilidades dos provedores de aplicação, os direitos dos usuários, entre outras questões relativas à proteção de dados. E é nesse ponto a proposta da presente pesquisa, ao discutir a urgência da questão e, principalmente, suas implicações negativas, demonstrando a necessidade de lei específica acerca dos dados pessoais.

Assim, através da utilização do método indutivo, esta pesquisa busca responder à problemática proposta a partir da sua estruturação em três capítulos. No primeiro capítulo verificar-se-ão: a realidade da sociedade informacional, o desenvolvimento do direito à privacidade, intimidade e vida privada e a proteção dos dados pessoais como um direito autônomo e fundamental. O segundo capítulo deste trabalho terá por escopo demonstrar como se dá a utilização dos dados pessoais no âmbito comercial, em campanhas políticas, na vigilância governamental e na governança eletrônica, demonstrando, desta forma, a urgência do tema e os seus mais diversos desdobramentos.

Por fim, o terceiro capítulo expõe que, apesar da existência de leis que tutelam vagamente os dados pessoais, há a necessidade de lei específica – que abarque em seu conteúdo medidas e procedimentos visando à efetiva proteção dos titulares dos dados pessoais

– uma vez que há lacunas no Marco Civil da Internet em relação aos dados pessoais. Além disso, também discorre acerca dos projetos de lei em pauta no Brasil, quais sejam: o Projeto de Lei n° 5.276/2016, o Projeto de Lei n° 330/2013, Projeto de Lei n° 4.060/2012, e, por fim, o Projeto de Lei n° 53/2018. E, bem como, analisa o Regulamento 2016/679 da União Europeia, o qual contém princípios e diretivas efetivos para a efetiva proteção dos dados pessoais e seus titulares.

1 ASPECTOS INTRODUTÓRIOS CONCERNENTES À PROTEÇÃO DE DADOS PESSOAIS NA INTERNET

Para uma melhor análise do tema é necessário explorar preliminarmente o histórico, algumas definições, bem como elencar alguns pontos relacionados à proteção de dados pessoais na internet. Essencial também aclarar que as definições serão feitas a fim de se ater ao assunto específico, isto é, serão apresentados sob o prisma da internet.

1.1 BREVE CONTEXTO HISTÓRICO

Quando há uma questão em voga, sabe-se que para sua correta apreciação é imprescindível buscar a fundo as suas origens e suas mudanças ao longo da história, dessa forma, compreender o contexto ao qual está inserido o tema é de extrema relevância.

Vive-se hoje o período que procede a ‘’pós-modernidade’’[1], trata-se daquele que os mais antigos vislumbravam maravilhados em filmes: com um clique se pode ver ao vivo o que se passa do outro lado do globo, é possível conversar com os amigos e também divulgar em diversas mídias sociais as experiências e o cotidiano.

E tudo isso tem uma razão de existir: a internet, que através de equipamentos tecnológicos possibilita facilidades antes inimagináveis.

Com toda a revolução tecnológica vislumbra-se, portanto, uma sociedade diferente, a qual se move em torno das informações que circulam.

O economista Fritz Machlup foi pioneiro em constatar, já em 1962, o valor econômico da informação, em seu livro *The Production and Distribution of Knowledge in the United States*, o qual gerou o termo ‘’sociedade da informação’’.

Nesse sentido, cita-se Sérgio Amadeu da Silveira (2017, p. 13 e 14), o qual afirma que:

> As sociedades informacionais são sociedades pós-industriais que tem a economia fortemente baseada em tecnologias que tratam informações como seu principal produto. Portanto, os grandes valores gerados nessa economia não se originam principalmente na indústria de bens materiais, mas na produção de bens imateriais, aqueles que podem ser transferidos por redes digitais. Também é possível constatar que as sociedades informacionais se estruturam a partir de tecnologias cibernéticas, ou seja, tecnologias de informação e de controle, as quais apresentam consequências sociais bem distintas das tecnologias analógicas, tipicamente industriais.

[1]Acerca do conceito de pós-modernidade, esclarece-se que o termo foi difundido principalmente por três teóricos e escritores, quais sejam: Jean François Lyotard, Jean Baudrillard e Fredric Jameson.

O fator decisivo para o surgimento da sociedade da informação é, sem duvidas, o advento do computador. Emerge-se, consequentemente, a ‘’economia do imaterial’’, substituindo as variáveis centrais anteriores, quais sejam: o trabalho e o capital por informação e conhecimento (GONÇALVES, 2003, p. 28 e 29).

O computador surgiu no cenário da Segunda Guerra Mundial (1939-1945), na Inglaterra, Alemanha e Estados Unidos da América, praticamente simultaneamente. Eram ‘’máquinas’’ bem diferentes das atuais, seu uso era restrito aos governos e sua principal função era bélica[2].

Desde lá os avanços tecnológicos proporcionaram enormes desenvolvimentos, seu uso expandiu para o cidadão comum – *personal computer* -, e suas funções passaram a englobar a comunicação, a pesquisa, o lazer, a educação e os serviços, encontrando-se hoje no que se denomina de ‘’quarta geração’’ (GUGIK, 2009).

Tem-se como principal resultado da internet e do computador a globalização e uma profunda mudança na dinâmica da vida em sociedade. Os governos, as empresas e os próprios cidadãos tiveram que se ajustar à nova realidade.

Nessa nova conjuntura, conforme afirma o sociólogo CASTELLS (2003, p. 225)

> A Galáxia Internet é um novo ambiente de comunicação. Como a comunicação é a essência da atividade humana, todos os domínios da vida social estão sendo modificados pelos usos disseminados da Internet, como este livro documentou. Uma nova forma social, a sociedade de rede, está se construindo em torno do planeta, embora sob uma diversidade de formas e com consideráveis diferenças em suas consequências para a vida das pessoas.

Ainda, ressalta (CASTELLS, 2016, p. 84 e 85):

> Gostaria de fazer uma distinção analítica entre as noções de ‘’sociedade da informação’’ e ‘’sociedade informacional’’ com consequências similares para a economia da informação e a economia informacional. O termo sociedade da informação enfatiza o papel da informação na sociedade. Mas afirmo que informação, em seu sentido mais amplo por exemplo, como comunicação de conhecimentos, foi crucial a todas as sociedades, inclusive à Europa medieval que era culturalmente estruturada e, até certo ponto, unificada pelo escolatiscismo, ou seja, no geral uma infraestrutura intelectual (ver Southern 1995). Ao contrario, o termo informacional indica o atributo de uma forma especifica de organização social em que a geração, o processamento e a transmissão da informação tornaram-se as fontes fundamentais de produtividade e poder devido às novas condições tecnológicas surgidas nesse período histórico. Minha terminologia tenta estabelecer um paralelo com a distinção entre indústria e industrial. Uma sociedade industrial (conceito comum na tradição sociológica) não é apenas uma sociedade em que há industrias, mas uma sociedade em que as formas sociais e tecnológicas de organização industrial permeiam todas as esferas de atividade, começando com as atividades predominantes localizadas no sistema econômico e na tecnologia militar e alcançando os objetos e hábitos da vida cotidiana. Meu emprego dos termos

[2]Para uma compreensão mais detalhada do desenvolvimento do computador sugere-se a leitura dos textos disponíveis em https://mundoestranho.abril.com.br/tecnologia/como-surgiu-o-computador/ e http://www2.ic.uff.br/~aconci/evolucao.html .

> ‘’sociedade informacional’’ e ‘’economia informacional’’ tenta uma caracterização mais precisa das transformações atuais, além da sensata observação de que a informação e os conhecimentos são importantes para nossas sociedades. Porém o conteúdo real de ‘’sociedade informacional’’ tem de ser determinado pela observação e análise. É exatamente esse o objetivo deste livro. Por exemplo, uma das características principais da sociedade informacional é a logica de sua estrutura básica em redes, o que explica o uso do conceito de ‘’sociedade em redes’’ [...].

É, portanto, com atenção as características contemporâneas da sociedade informacional mencionadas alhures que se deve lançar olhar ao estudo aqui dirigido. A atualidade traz singularidades observadas de forma inédita na história do mundo, logo, alerta para a necessidade de se ater as suas consequências. Afinal, as facilidades tecnológicas e os novos meios de comunicação e relações sociais também trazem consigo suas facetas nocivas.

1.2 CONCEITOS NECESSÁRIOS PARA SEU ESTUDO

Para compreender a magnitude da necessidade de proteção dos dados pessoais na internet é, por certo, forçoso precisar as definições relativas aos dados pessoais. Qualquer indivíduo que utiliza da ferramenta internet, em seus mais diversos campos e propósitos, há de deixar rastros e informações a seu respeito, e dessa maneira, seus dados pessoais.

Nesse tópico, discorrer-se-á os conceitos de dados pessoais – e suas espécies –, bem como da internet e conceitos decorrentes deste, quais sejam: os metadados, o seu tratamento, os *cookies*, *big data,* algoritmos, e *bots*.

1.2.1 Conceito de dados pessoais

Os dados pessoais foram definidos no Regulamento 2016/679 da União Europeia (*General Data Protection Regulation* – GDPR) em seu art. 4º, n. 1, que *in verbis* estipula[3]:

> «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrónica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular;

Ressalta-se que apesar da já entrada em vigor da Lei nº 12.965/2014 – Marco Civil da Internet –, não há definição legislativa para os dados pessoais nas leis brasileiras.

[3]Utilizamos a versão portuguesa, disponível no link: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

Ainda, importa alencar que há outras leis internacionais, em especial na Europa, que precisam seu conceito, porém, com a eminente entrada em vigor (25/05/2018) do Regulamento 2016/679 da União Europeia e no intuito de não dar margem a conceitos defasados adotaremos a definição mais recente estipulada na Lei Europeia de Regulamentação de Dados Pessoais.

Nesse sentido, os dados pessoais coletados podem referir-se a uma universalidade de ‘’informações’’, desde dados cadastrais como nome, endereço, e-mail, ao endereço de IP, dados biométricos, de raça, saúde (LIMA, 2014, p. 155).

As redes sociais – em especial Facebook, Twitter e Instagram – se destacam como plataformas de coleta desses dados, o que se dá geralmente por meio de testes, elaborados de forma atraente aos usuários, e que por meio do ‘’aceite’’ do sujeito têm acesso a diversos dados como nome, idade, e-mail, e todas as fotos contidas no perfil do usuário (MENDONÇA, 2018).

A fim de desenvolver o seu conceito, convém apontar alguns tipos de dados pessoais, quais sejam: dados biométricos, dados genéticos, dados relativos à saúde, e dados sensíveis.

Conceitua a GDPR, em seu art. 4º, n. 14, que dados biométricos são ‘’*resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos*;’’

Nesse sentido, representam características únicas (variam a depender da pessoa em questão), permanentes (não variam no tempo), acessíveis e quantificáveis. E permitem, dessa forma, a identificação ou a autenticação do individuo. (CASTRO, 2005, p. 83).

Ensina CASTRO (2005, p. 83) que os dados biométricos podem ser segmentados em dois grupos, quais sejam: relativos a características físicas e dados relativos a características comportamentais. Do primeiro grupo cita-se de exemplo ‘’*a impressão digital, a geometria da mão e dedos, das veias da face, ou da orelha, a íris, a retina, o odor, a voz, ou o DNA*’’ enquanto que o outro engloba a ‘’*sua assinatura escrita, a forma como toca nas teclas ou na forma como fala*’’.

Ainda consoante a lei mencionada, os dados genéticos são definidos em seu art. 4º, n. 13, como ‘’*relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;*’’.

No intuito de se ilustrar a questão, menciona CASTRO (2005, p. 94)

> Estes dados podem demonstrar, *v.g.*, se duas pessoas são ou não da mesma família, podem revelar a presença ou ausência de uma característica num individuo, assim como a presença ou ausência do risco/probabilidade de doença.

A jurista citada alhures ressalva que os dados genéticos podem ser utilizados para fins legais com o propósito de identificação, de paternidade ou origem étnica (CASTRO, 2005, p. 95).

No tocante aos dados relativos à saúde, a Lei Europeia de Proteção de Dados Pessoais em seu art. 4º, n. 15, os define como ‘’*dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde;*’’.

Adverte-se que os dados relativos à saúde não se restringem ao diagnóstico médico, mas contemplam ‘’*todos aqueles que permitem apurá-lo, incluindo resultados de análises clínicas, imagens de exames radiológicos, imagens vídeo ou fotografias que sirvam o mesmo fim*’’ (CASTRO, 2005, p. 91).

Por fim, ainda encontramos na Lei Europeia de Proteção de Dados Pessoais outra distinção acerca dos mesmos, qual seja: a de dados sensíveis, na qual se reserva uma proteção especial.

Apesar de não instituir uma definição propriamente dita do termo, a referida lei assevera em sua consideração n. 51[4]:

> **Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais.** Deverão incluir-se neste caso os **dados pessoais que revelem a origem racial ou étnica**, não implicando o uso do termo «origem racial» no presente regulamento que a União aceite teorias que procuram determinar a existência de diferentes raças humanas. **O tratamento de fotografias não deverá ser considerado sistematicamente um tratamento de categorias especiais de dados pessoais, uma vez que são apenas abrangidas pela definição de dados biométricos quando forem processadas por meios técnicos específicos que permitam a identificação inequívoca ou a autenticação de uma pessoa singular.** Tais dados pessoais não deverão ser objeto de tratamento, salvo se essa operação for autorizada em casos específicos definidos no presente regulamento, tendo em conta que o direito dos Estados-Membros pode estabelecer disposições de proteção de dados específicas, a fim de adaptar a aplicação das regras do presente regulamento para dar cumprimento a uma obrigação legal, para o exercício de funções de interesse público ou para o exercício da autoridade pública de que está investido o responsável pelo tratamento. Para além dos requisitos específicos para este tipo de tratamento, os princípios gerais e outras disposições do presente regulamento deverão ser aplicáveis, em especial no que se refere às condições para o tratamento lícito. Deverão ser previstas de forma explícita derrogações à proibição geral de tratamento de categorias especiais de dados pessoais, por exemplo, se o titular dos dados der o seu consentimento expresso ou para ter em conta necessidades específicas, designadamente quando o tratamento for

[4]Utilizamos a versão portuguesa, disponível no link: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

> efetuado no exercício de atividades legítimas de certas associações ou fundações que tenham por finalidade permitir o exercício das liberdades fundamentais. [grifo nosso]

Com a finalidade de complementar o entendimento, a Diretiva 95/46 da União Europeia em seu art. 8º, n. 1, estabelece que[5]:

> Os Estados-membros proibirão o tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, bem como o tratamento de dados relativos à saúde e á vida sexual.

Podemos encontrar no site [6] da Comissão Europeia – versão portuguesa – em relação aos dados sensíveis a seguinte recomendação de ‘*’Tenha salvaguardas extraordinárias para informações sobre saúde, raça, orientação sexual, religião e convicções políticas.*’’

Nesse sentido, extrai-se que a particularização de alguns dados conferida pela lei se fez pela necessidade de proteção maior a esses, porquanto seu tratamento e utilização podem implicar em ‘’*riscos significativos para os direitos e liberdades fundamentais*‘’, conforme apregoa a própria GDPR em sua consideração n. 51.

Frisa-se que essa classificação especial – dados sensíveis – compreende inclusive os dados biométricos e os genéticos (MONTEIRO, 2018).

Dessa forma, superada a compreensão acerca dos dados pessoais, passa-se a discorrer a respeito da internet e concepções dela decorridas.

1.2.2 Conceito de internet

O estudo em questão se concentra no âmbito da internet, e por lógico, necessário entender sua compreensão.

A Lei nº 12.965/2014 (Marco Civil da Internet) a conceitua em seu art. 5º , I, como ‘’*o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes*;’’

Em relação à Lei Europeia de Regulamentação de Dados Pessoais, não há qualquer definição acerca da nomenclatura.

Porém, conforme aponta o advogado Victor Hugo Pereira (GONÇALVES, 2017, p. 2)

> [...] a melhor conceituação não seria internet, mas tecnologias de informação e comunicação. Internet é um nome localizado no espaço e tempo restritos que pode,

[5]Utilizamos a versão portuguesa, disponível no link: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT

[6]A orientação encontra-se disponível no link: http://ec.europa.eu/justice/smedataprotect/index_pt.htm .

> dentro em breve, ser ultrapassado por outras nomenclaturas melhores e mais atualizadas. Já há em curso uma revolução de convergências de mídias de comunicação, o que coloca em duvida a utilização do conceito de internet, que foi formulado na década de 1990.

Dessa forma, contrariando o termo internet, que será por muito utilizado nesse trabalho – pelo único propósito de facilitar a compreensão dos leitores – a posição adotada é que utilizar a referida terminologia é equívoca.

1.2.3 Metadados

Os metadados – do grego ‘’meta’’, significa ‘’além de’’ – são informações que acrescem aos dados, e tem como finalidade auxiliar a utilização dos dados (SAFERNET, 2018).

Simplificando, são ‘’*informações a respeito de outras informações’’* (NETO; MORAIS; 2014, p. 418).

A fim de aprofundar seu conceito, cita-se os esclarecimentos encontrados na página da web da SaferNet Brasil[7]:

> Praticamente todos os dispositivos digitais geram metadados a partir do uso que fazemos. Por exemplo, ao tirar uma foto, além de gravar a foto na memória da foto, metadados são associados a esta foto descrevendo informações sobre o modelo da câmera, tipo de ISO, data, tamanho e formato do arquivo e até o local de onde a foto foi tirada se o aparelho tiver GPS.
> Ao fazer login em um site de redes sociais ou de compras várias informações são registradas além daquelas que escrevemos diretamente nos sites, como por exemplo, o endereço IP, o nome e versão do navegador, horário exato de entrada e saída, bem como outros detalhes sobre os seus cliques durante aquela navegação.
> Os tipos mais comuns de metadados são:
> - Número de telefones, endereços de email e os nomes das pessoas que usam serviços;
> - Dados de Localização: onde está o seu telefone celular;
> - Data e hora em que foram feitas as ligações, emails, arquivos e fotos;
> - Informações do aparelho que você está usando;

Para ilustrar ‘’em cores’’ suas implicações, cita-se o programa de computador *Immersion*, desenvolvido pelo físico César Hidalgo, pesquisador do Massachussetts Institute of Technology (MIT), em conjunto com seus parceiros, que após a permissão do usuário para acessar a sua conta do Gmail gera diversos gráficos interativos – evidenciando os períodos e quais relações sociais o mesmo tinha/tem com as pessoas que se comunicou/comunica. Apesar de o software não ter acesso ao conteúdo das mensagens, ele tem o potencial de constatar questões de extrema intimidade, como no caso de sua namorada não gostar do

[7]C.f.: http://new.safernet.org.br/node/199 .

‘*’grupo de amigos formado durante o seu relacionamento anterior’’*, e o faz a partir de ‘*’apenas informações como destinatário do e-mail, para quem ele foi enviado, quem está copiado e dados relativos ao horário do envio*’’. E o próprio o pesquisador alerta que o uso de metadados pode implicar em violação à privacidade (CABRAL, 2018).

Dessa forma, devido ao seu extenso alcance – está por toda a internet e em dispositivos digitais –, é necessária atenção quando se alia metadados à possível perspectiva de propósitos comerciais, administrativos e políticos sem a devida cautela.

1.2.4 Tratamentos

Com o fenômeno da Dossier Society, em que a informática concedeu poder às informações e os bancos de dados conquistaram valor de mercado, não há como não se discutir também os tratamentos concebidos a esses últimos (AIAETA, 2014, p. 701).

O conceito de tratamento adotado nesse estudo será o mesmo definido na Lei Europeia de Proteção de Dados Pessoais em seu art. 4º, n. 2, qual seja[8]:

> «Tratamento», uma operação ou um conjunto de operações efetuadas sobre dados pessoais ou sobre conjuntos de dados pessoais, por meios automatizados ou não automatizados, tais como a recolha, o registo, a organização, a estruturação, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a divulgação por transmissão, difusão ou qualquer outra forma de disponibilização, a comparação ou interconexão, a limitação, o apagamento ou a destruição;

Ainda, a fim de complementar o entendimento cita-se CASTRO (2005, p. 187)

> Os tratamentos de dados pessoais pelos serviços públicos podem revestir um caráter muito diverso: do simples tratamento dos dados nome, morada e instituição a que alguém pertence, para efeitos de envio de convites ou para outros contactos, até ao tratamento de dados sensíveis como os dados de saúde, v.g., no caso dos estabelecimentos de saúde públicos, ou os dados relativos a condições socioeconômicas, v.g., por parte de organismos com funções sociais, *etc*, são hoje várias as possibilidades, graças à quase infinita capacidade de armazenamento de informações dos computadores e às suas faculdades de cruzamento e pesquisa de informação.

Por fim, esclarece-se que o Marco Civil Brasileiro da Internet não trouxe uma definição a espeito da nomenclatura.

1.2.5 *Cookies*

Para esse estudo usaremos o conceito de *cookies* apresentado pelo advogado brasileiro Victor Gameiro (DRUMMOND, 2003, p. 98), que assim o define:

[8]Utilizamos a versão portuguesa, disponível no link: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN

> Os cookies são pequenos programas colocados no computador do usuário sem a sua permissão durante uma navegação no ambiente da Internet. Em verdade, sem sequer seu conhecimento, visto que nenhum indicativo irá suceder-se na tela do computador que possa vir a evidenciar a sorrateira entrada daqueles programas de computador. Estes pequenos programas ficam armazenados, assim, no próprio computador do usuário.

Seu principal intuito é de colaborar a próxima utilização do usuário em um mesmo sitio cibernético (DRUMMOND, 2003, p. 98).

Esclarece-se ainda que essa ferramenta é utilizada para traçar um perfil do usuário, e dessa maneira, oferecer produtos de acordo (DRUMMOND, 2003, p. 100).

Observa-se, portanto, que se trata de uma forma de coleta, armazenamento e possível tratamento de dados pessoais dos sujeitos que utilizam a internet. Uma das inúmeras maneiras de se apropriar de dados pessoais sem o consentimento do seu titular e mais uma para nos mostrar o quanto os nossos dados pessoais são negligenciados e sua falta de proteção necessária.

1.2.6 *Big Data*

Após exaurimos o conceito dos dados pessoais e metadados é possível assimilar que em razão do uso constante das tecnologias disponíveis há uma imensa ‘’produção’’ – por assim dizer –, de dados. E é diante desse contexto de inúmeros dados que se revelou o *Big Data*.

Apesar de não haver consenso único entre os estudiosos da área a respeito do que se trata o *Big Data*, usar-se-á o conceito definido no relatório Big Data no projeto Sul Global - Relatório sobre estudos, elaborado pelo Instituto de Tecnologia e Sociedade do Rio de Janeiro, que assim preconiza[9]:

> [...] é, literalmente, o conjunto de dados cuja existência só é possível em consequência da coleta massiva de dados que se tornou possível nos últimos anos, graças à onipresença de aparelhos e sensores na vida cotidiana e do número crescente de pessoas conectadas a tais tecnologias por meio de redes digitais e também de sensores.

No mais, ressalta-se que o termo *‘’comporta diversas interpretações e variados significados, principalmente por ser utilizada por diversos setores, como especialistas em tecnologia, juristas e autoridades publicas’’* (GOMES, 2018, p. 233).

[9] Disponível no link: https://itsrio.org/wp-content/uploads/2017/01/ITS_Relatorio_Big-Data_PT-BR_v2.pdf

Assim sendo, esclarece-se que para uma definição mais apropriada seria necessário um estudo complexo, uma vez que o termo envolve vários conceitos técnicos da Ciência da Informação e dedicação voltada às diversificadas áreas de uso, o que não é a proposta do trabalho.

Prosseguindo em seu conceito, percebe-se que o big data manifesta três atributos, denominados ‘’3 V’s’’, quais sejam (MCAFFE; BRYONJOELFSSON; apud SANTOS, 2018, p. 11):

> (i) volume – a sociedade atual é altamente conectada e tecnológica, todos os dias milhões de transações e comunicações são realizadas *online*, seja troca de e-mails, mensagens por comunicadores instantâneos, fotos, vídeos, digitalização de documentos, cadastros; (ii) velocidade – esses dados são criados de forma acelerada e praticamente instantânea, portanto, atualizadas; e (iii) variedade – os dados coletados são aleatórios, variados e advém das mais diversas ferramentas – mídias sociais, celular, gps, sistemas integrados etc.

Nesse sentido (MAYER-SCHONBERGER, Viktor; CUKIER, 2013, p. 190 apud GOMES, 2018, p. 236):

> O acúmulo de conhecimento e informação, que um dia significou estudar, conhecer e compreender o passado, esta se transformando, significando, com o big data, a habilidade de prever o futuro.

Portanto, após a explanação desses apontamentos, é nítida a importância do *Big Data* para os estudos e o manuseio dos dados pessoais colhidos na internet. E, nesse sentido da complexa dinâmica da internet, suas ferramentas, tecnologias e sua interação com os dados pessoais, frisa-se a necessidade de voltar-se conjuntamente sobre todos os conceitos abordados nesse tópico para a plena compreensão de seu mecanismo.

1.2.7 Algoritmos

Seu conceito abarca uma infinidade de questões, podendo ser compreendido de forma mais ampla como ‘*’uma receita que mostra passo a passo os procedimentos necessários para a resolução de uma tarefa. Ele não responde a pergunta “o que fazer?”, mas sim “como fazer”* e de forma mais técnica como *‘’uma sequência lógica, finita e definida de instruções que devem ser seguidas para resolver um problema ou executar uma tarefa’’* (PEREIRA, 2018).

Para maior compreensão, uma vez que podem ser entendidos por uma esfera subsidiária da inteligência artificial, cita-se a definição dessa última, preconizada pelos juristas Coriolano Aurélio de Almeida Camargo Santos e Marcelo Crespo (2016):

> [...] significa a realização, por uma máquina, de tarefas geralmente ultimadas por um humano. Pode-se até mesmo entender que ela se divide em quatro categorias: a) aprendizagem mecânica; b) processamento da linguagem natural; c) visão; e d) fala. A aprendizagem mecânica nada mais é que um sistema que processa dados para melhorar continuamente o desempenho na realização de uma tarefa. Já o processamento da linguagem natural é a possibilidade de um computador compreender a linguagem humana, interpretando o que as pessoas realmente transmitem nas suas interações, decifrando suas intenções e fornecendo respostas cada vez mas precisas nos resultados de uma pesquisa. Já a visão é a habilidade de interpretar imagens, identificá-las e descrevê-las, o que geralmente é feito de forma automática pelos humanos. Por fim, a fala é o sistema que permite uma máquina interpretar a linguagem oral e propiciar interação entre os humanos e as máquinas.

Observa-se a aplicação dos algoritmos na *''informática e telemática, inteligência artificial (Artificial Intelligence), aprendizado de máquina (Machine Learning), aprendizado profundo (Deep Learning), redes neurais (Neural Networks), Internet das coisas (Internet of Things) e outros''* (ELIAS, 2018).

Sua utilização vai desde realizar a distribuição de processos no Supremo Tribunal Federal (SUSSEKIND, 2017), nas buscas do Google, em sites como Amazon, Netflix, e até na campanha presidencial do então candidato a presidente dos Estados Unidos Barack Obama (PROXXIMA, 2018).

Nessa seara, observa-se um fenômeno denominado ‘’filtro bolhas’’ ou ‘*’filter bubble’’,* assunto difundido pelo autor e ativista politico e da internet Eli Pariser.

Em uma conferência do TedTalks [10] , ele explica que ocorreram mudanças significativas na internet. Ele observou tal fenômeno primeiramente no Facebook, quando identificou que não recebia mais as notícias dos amigos que tinham pensamentos políticos opostos aos seus. E afirma que essa ferramenta é utilizada pelo Google, New York Times, Netflix, Amazon. Ressalta que, em verdade, não existe mais um Google – para pesquisas – padrão, uma vez que cada usuário obtém resultados diferentes, levando em conta as informações que a plataforma tem sobre ele.

Sua preocupação decorre que dessa forma, praticamente tudo que esta na internet é dado ‘’sob medida’’ para cada usuário, e que o mesmo não escolhe os filtros e, na maioria das vezes, não sabe da sua existência, há uma edição invisível da web.

[10] Disponível em: https://www.youtube.com/watch?v=B8ofWFx525s

Eli denomina o filtro bolhas como o conjunto de todos os filtros que há na internet, o que resulta com cada indivíduo em seu universo online único de informações. As informações que ultrapassam esse filtro dependem de quem é, o que a pessoa faz.

O ativista alerta que os algoritmos que procedem essa filtração se baseiam em escolhas primárias – geralmente as primeiras – de cada usuário, e portanto, podem perder o equilíbrio ao apresentar informações por vezes polarizadas.

Também compara com a sociedade de transmissão (tv, rádio e jornal), em que são os editores que fazem o controle do que passa para os cidadãos ou não, e que hoje esse papel é dado aos algoritmos. Seu apontamento enfatiza que os editores tem uma noção de ética dos conteúdos a serem mostrados ou não, o que não ocorre com os algoritmos.

Ele defende que os algoritmos, em seus papéis de ‘’curadores do mundo’’ devem mostrar para além de informações relevantes – que é o princípio que seguem os algoritmos – e sim, informações importantes, desafiadoras e outros pontos de vista.

Nesse sentido, ele reflete que para ter uma democracia em funcionamento é necessário um bom – aqui se entende por qualidade e quantidade – fluxo de informações. E por fim, acentua que os algoritmos devem prestigiar em seus códigos um senso de vida pública, um senso de responsabilidade cívica, que tenham seu funcionamento claro para os usuários, e que estes últimos tenham controle para decidir os limites das bolhas.

1.2.8 *Bots*

Como se pode perceber, a rede na atualidade é cheia de mecanismos, ferramentas e fenômenos que comprovam manipulações, disparidades entre os sujeitos – usuário, provedor, plataforma utilizada – e a imprescindibilidade de regulação para essas relações.

Outra ferramenta que vem sendo usada são os bots, em abreviação para robôs. Na página online do ITSRio, encontra-se a seguinte definição (ITSRIO, 2018):

> [...] são programas de computador criados para executar tarefas específicas. Os primeiros robôs não tinham intenções maliciosas, e ainda hoje existem os bons bots, que têm como propósito exigir prestação de contas de políticos, viralizar causas para a igualdade de gênero ou ajudar a organizar as (muitas) tarefas diárias de seus usuários. Mas no final da década de 1990, os bots começaram a desenvolver uma reputação negativa.
>
> Alguns têm sido usados no envio de SPAMs por e-mail, no roubo de dados pessoais de usuários, em fraudes de cartão de crédito e em ataques de desinformação para manipulação da esfera pública. Esses bots têm como objetivo espalhar mentiras para influenciar narrativas, um fenômeno que desde 2014 vem ganhando escala global. E pior: eles estão por aí e quase ninguém sabe como funcionam, quem os desenvolve e por quem são financiados.

Ressalta-se que seu uso é abundante em campanhas políticas. Nas redes sociais ele pode *''seguir pessoas, postar e direcionar mensagens, inserir links ou hashtags. Eles muitas vezes servem para multiplicar as informações distribuídas na rede, passando-se por contas de pessoas reais''* (ITAGIBA, 2017, p.3).

E ainda:

> Com a evolução da inteligência artificial, bots terão a habilidade de mimetizar o comportamento humano de forma quase perfeita, o que dificulta o processo de checagem de fatos.

Nesse sentido, destaca-se uma parceria entre o Instituto de Tecnologia e Sociedade do Rio de Janeiro (ITS Rio) e o Instituto Equidade & Tecnologia, que conjuntamente desenvolveram o PegaBot[11], um dispositivo que permite calcular a probabilidade de um perfil de Twitter ser bot.

1.3 PRIVACIDADE E INTIMIDADE: PALAVRAS-CHAVE

No âmbito jurídico há diversos institutos e princípios que visam proteger aspectos e direitos da vida do cidadão. Nesse sentido, os direitos que originaram a proteção aos dados pessoais foram o direito à vida privada e o direito à intimidade.

A teoria dos direitos da personalidade surgiu nos países de língua germânica, a qual se baseava na ideia de um direito subjetivo além dos direitos reais e pessoais (GIACCHETTA; MENEGUETTI, 2014, p.377).

A percepção da esfera privada se deu com o surgimento da sociedade burguesa e o declínio da sociedade feudal. As relações dos indivíduos do período feudal eram excessivamente interligadas, dada a sua estrutura social, e o isolamento era raro, usufruído somente por monges, místicos, pastores e bandidos. Um dos principais aspectos decorrentes das transformações socioeconômicas à época foi a implementação de novas técnicas de construções – quando houve uma divisão do lugar em que se vive e o local de trabalho, e assim uma noção de uma esfera privada (RODOTÀ, 2008, p. 26).

Samuel Warren e Louis Brandeis publicaram um artigo intitulado de *''The right to privacy''* na *Harvard Law Review*, em 1890, que postulava o direito à privacidade, sob o aspecto da personalidade humana, compreendido como *''right to be let alone''* (CASTRO, 2005, p. 17).

[11] C.f.: https://itsrio.org/pt/projetos/pegabot/

Antes do artigo, conforme enfatiza a jurista portuguesa Catarina Sarmento e Castro (2005, p. 17) a questão havia sido somente tutelada em sede jurisprudencial, ‘’*mediante o recurso à violação do direito de propriedade privada, à violação da confidencialidade, da confiança, ou de uma obrigação contratual’’*.

A denominação dada à privacidade elabora pelos juristas foi se transmutando conforme o surgir de diferentes necessidades a serem resguardadas. No cenário atual de recolhimento de dados, definições como: ‘’*o direito a controlar a maneira na qual os outros utilizam as informações a nosso respeito*‘’(A. Westin); ‘’*a proteção de escolhas de vida contra qualquer forma de controle público e estigma social*’’(L. M. Friedman); ‘’*reinvindicação dos limites que protegem o direito de cada indivíduo de não ser simplificado, objetivado, e avaliado fora de contexto*’’ (J. Rosen) são de extrema valia (RODOTÁ, 2008, p. 15).

Outra definição encontrada nos estudos é a de Vinicius Gameiro Drummond (2003, p. 141), na qual afirma que: ‘*’A privacidade é a distância confortável que uma pessoa mantém, espontaneamente, desde sua mais profunda individualidade até o mundo exterior’’*.

Para Rodotà (2008, p. 17) o avanço do conceito de privacidade atual abarca também ‘’*o direito de controle sobre as informações de alguém e determinar como a esfera privada deve ser construída’’*.

Ressalva-se aqui, que muitos autores distinguem o direito à vida privada e o direito à intimidade, ambos relacionados a uma noção de privacidade – direito à privacidade - no sentido mais geral.

A fim de se aclarar a questão, destaca-se alguns entendimentos acerca da definição de intimidade, quais sejam: ‘’*a esfera secreta do individuo na qual este tem o poder legal de evitar os demais’’* (DOTTI, 1980, p. 69); “*modo de ser de determinado indivíduo, consistindo fundamentalmente na exclusão do conhecimento pelos demais daquilo que somente a ele diz respeito*” (FARIAS, 1996, p. 104); ‘’*a esfera mais secreta da vida de cada um*’’ (MOTTA; BARCHET, 2007, p. 180); ‘’*são questões de foro personalíssimo de seu detentor, não competindo a terceiros invadir este universo intimo’’* (LAZARI, p. 8)

Para contraponto, apresentam-se as concepções relativas à vida privada: ‘’*uma forma de externalização desta esfera secreta em locais afastados do contato com estranhos, a exemplo do domicilio da pessoa’’* (MOTTA; BARCHET, 2007, p. 180); ‘’*poderíamos ilustrar a vida social como um grande círculo, dentro do qual um menor, o da privacidade, em cujo interior seria aposto um ainda mais constrito e impenetrável, o da intimidade*’’

(ARAÚJO; NUNES ARAÚJO, 2001, p. 109); ‘‘*são questões que apenas dizem respeito a seu detentor, desde que realizadas em ambiente intimo*’’ (LAZARI, p. 8)

Já o jurista brasileiro José Afonso da Silva (2005, p. 206) prefere ‘‘*usar a expressão direito à privacidade, num sentido amplo e genérico, de modo a abarcar todas as manifestações de esfera íntima, privada e da personalidade*’’.

Importa mencionar que a matéria foi tratada em diversas leis, tanto nacionais, quanto internacionais, podendo-se citar a Declaração Americana dos Direitos e Deveres do Homem (1948), a Declaração Universal dos Direitos do Homem, O Pacto Internacional sobre Direitos Civis e Políticos (reconhecido no Brasil em 1992), a Convenção Americana Sobre Direitos Humanos (Pacto de São Jose da Costa Rica, sendo legitimado no Brasil em 1992) (GUERRA, p. 398).

Desse modo, devido as diferentes posições acerca da diferenciação entre direito à intimidade e direito à vida privada, esclarece-se que adotaremos a visão mais ampla, referindo-se de maneira geral por direito à privacidade. Além do mais, referidas distinções não prejudicam o tema especifico, qual seja, a proteção devida aos dados pessoais na internet.

Retomando ao desenvolvimento do direito à privacidade, verifica-se que a Carta de Direitos Fundamentais da União Europeia, promulgada em 2000, culminou uma verdadeira divisão do direito à privacidade e a proteção de dados pessoais, ao conhecer este último como um direito autônomo (RODOTÀ, 2008, p. 16).

Suas diferenças estão esculpidas principalmente porquanto a proteção à vida privada embasa-se numa proteção estática e negativa, caracterizada pela objeção em se interferir na vida privada e familiar de um singular, enquanto que a proteção de dados pessoais é mais ativa, regra os instrumentos de processamento de dados e designa legitimidade para os atores necessários a fim de se cumprir as medidas de proteção (RODOTÀ, 2008, p. 17).

E é nesse ponto que, dada a cisão – um enorme progresso, em verdade – do reconhecimento da proteção de dados pessoais como autônomo, que se faz necessário reservar o próximo tópico, em separado, para sua melhor apreciação.

1.5 PROTEÇÃO AOS DADOS PESSOAIS COMO UM DIREITO AUTONÔMO E FUNDAMENTAL

Conforme visto no tópico anterior no intuito didático de representar a divisão entre o direito à privacidade e a proteção concedida especificamente aos dados pessoais, continuaremos aqui seus estudos.

Foi assentada nessas circunstâncias favoráveis a ‘’*autonomia do individuo na sociedade de informação,* [que] *uma decisão histórica da Corte Constitucional Alemã de 1983 reconheceu a ‘’auto-determinação informativa’’*’’ (RODOTÁ, 2008, p. 15).

O grande jurista italiano aponta que ‘*’a proteção de dados contribui para a ‘’constitucionalização da pessoa’’*, e se configura como um recurso para o ‘’*o livre desenvolvimento da personalidade*’’, podendo ainda ser vislumbrada como ‘’*um conjunto de direitos que configuram a cidadania do novo milênio*’’ (RODOTÀ, 2008, p. 17).

Ressalta-se que no contexto atual, verifica-se presente, em relação à proteção de dados pessoais, interesses contrapostos: por um lado, há a proteção da vida privada dos indivíduos e por outro, questões relativas à segurança interna e internacional, reorganização da administração pública e interesses de mercado (RODOTÀ, 2008, p. 13).

Nesse sentido aponta o autor (RODOTÀ, 2008, p. 37):

> Raramente o cidadão é capaz de perceber o sentido que a coleta de determinadas informações pode assumir em organizações complexas e dotadas de meios sofisticados para o tratamento de dados, podendo escapar a ele próprio o grau de periculosidade do uso de dados por parte de tais organizações. Além disso, é evidente a enorme defasagem de poder existente entre o individuo isolado e as grandes organizações de coleta de dados: nessas condições, é inteiramente ilusório falar em ‘’controle’’.

Em especial às relações de mercados, ‘*’não se pode julgar decisivo o argumento do aumento dos custos para as empresas (e para a administração pública) ocasionado pelas normas sobre a proteção de dados’’* (RODOTÀ, 2008, p. 53).

Ainda, o autor defende a proteção coletiva dos dados coletados, para o qual prescreve (RODOTÀ, 2008, p. 50):

> [...] um alargamento da perspectiva institucional, superando a lógica puramente proprietária e integrando os controles individuais com aqueles coletivos; diferenciando a disciplina de acordo com as funções para as quais são destinadas as informações coletadas; analisando com maior profundidade os interesses envolvidos nas diversas operações e colocando em funcionamento novos critérios para o equilíbrio de tais interesses. Em síntese: a proteção de dados pessoais não pode mais se referir a algum aspecto especial, mesmo que seja em si muito relevante, porém requer que sejam postas em operações estratégias integradas, capazes de regular a circulação de informações em seu conjunto.

Rodotà ao observar a Convenção do Conselho da Europa de 28 de janeiro de 1981 e a Recomendação da Organização para a Cooperação e o Desenvolvimento Econômico (OCDE) de 23 de setembro de 1980, elencou alguns princípios em comum no trato dos dados pessoais, quais sejam (2008, p. 59):

> 1. *princípio da correção* na coleta e no tratamento das informações;

> 2. *princípio da exatidão* dos dados coletados, acompanhado pela obrigação da atualização;
> 3. *princípio da finalida*de da coleta de dados, que deve poder ser conhecida antes que ocorra a coleta, e que se especifica na relação entre os dados colhidos e a finalidade perseguida (princípio da pertinência); na relação entre a finalidade da coleta e a utilização dos dados (princípio da utilização não-abusiva); na eliminação, ou na transformação em dados anônimos das informações que são mais necessárias (princípio do direito do esquecimento);
> 4. *princípio da publicidade* dos bancos de dados que tratam as informações pessoais, sobre os quais deve existir um registro público;
> 5. *princípio do acesso individual*, com a finalidade de conhecer quais são as informações coletadas sobre si próprio, obter a sua cópia, obter a correção daquelas erradas, a integração daquelas incompletas, a eliminação daquelas coletadas ilegitimamente;
> 6. *princípio da segurança* física e lógica da coletânea de dados.

O autor ao analisar demais legislações estipulou outras características necessárias a fim de proteger os dados pessoais, das quais se citam algumas (RODOTÀ, 2008, p. 61 e 62):

> 1. a previsão de colocar à disposição dos usuários não somente instrumentos jurídicos, mas também meios técnicos de controle direto. [...]
> 2. extensão da obrigação de pedir o consentimento dos interessados não apenas para a coleta de dados que lhe digam respeito, mas também para utilização especificas destes [...].
> 4. proibição de compartilhar os dados coletados com terceiros [...]

Nessa toada, cita-se que a jurista Catarina Sarmento e Castro aponta os princípios da finalidade e da transparência como fundamentais no tratamento de dados pessoais. E quanto aos relativos às qualidades dos dados pessoais cita os princípios da licitude e lealdade; e os princípios da exatidão e atualização dos dados (2005, p. 229 a 237).

Em relação aos direitos dos titulares dos dados assegura os direitos ao esquecimento, à curiosidade, à informação, ao acesso, de retificação e atualização, do apagamento ou bloqueio dos dados, e o de oposição. (2005, p. 239 a 254).

Nesse sentido, a fim de se desenvolver suas implicações, tem-se que o principio geral da transparência (CASTRO, 2005, p. 229):

> [...] implica que o responsável de um tratamento de dados, devidamente identificado, deve dar a conhecer ao titular dos dados a realização do tratamento que lhe respeite, indicando, nomeadamente, os seus fins, categorias de dados tratados, período de conservação dos dados, eventuais comunicações dos mesmos, etc.

Em relação ao princípio da finalidade, destaca-se que (CASTRO, 2005, p. 230):

> [...] esta deve ser determinada – deve ser conhecida antes do inicio do tratamento -, explícita – o que exclui o tratamento de dados para fins não claramente determinados ou vagos, ou o seu desconhecimento por parte do titular dos dados-, e legítima – não podendo ser contrária à lei, designadamente atendendo à competência ou à bondade do interesse que demonstre ter o responsável pelo tratamento na sua realização.

Os princípios da licitude e lealdade correspondem, o primeiro: cumprir com as regras, normas e leis sujeitas, a observar a boa-fé e, o segundo: com a transparência devida. Além do mais ‘*’pode também considerar-se desleal a recolha de informações quando os titulares dos dados não possam opor-se à sua recolha’’* (CASTRO, 2005, p. 235).

No mais, não se aprofundará nos demais direitos e princípios, uma vez que autoexplicativos.

Por fim, Rodotà lista qualidades e particularidades necessárias para um ‘*’ambiente jurídico adequado’’* no tocante aos dados pessoais: que se estabeleçam ‘*’uma disciplina legislativa de base’’*; ‘*’normas para casos específicos’’*; ‘*’uma autoridade administrativa independente’’*; *‘’uma disciplina de recursos à autoridade judiciária’’* e ‘*’a previsão de um controle difuso, confiado à iniciativa de indivíduos e grupos’’* (RODOTÀ, 2008, p. 87 e 88).

Dessa forma, conclui-se que ‘’a preocupação com as possibilidades infinitas de combinações de dados pessoais, associadas a poderosas habilidades de pesquisa e a impressionantes capacidades de armazenamento, todas potenciadas pelo uso da informática, levederam a construção deste direito, que foi sendo acolhido como um novo direito fundamental’’ (CASTRO, 2005, p. 29).

E mais, ‘*’que não seria compatível com o direito à autodeterminação informativa a uma ordem social e jurídica na qual o cidadão não pudesse saber quem, o quê, quando e com que motivo sabe alguma coisa sobre ele."* (CASTRO, 2005, p. 29).

O que mais importa para uma efetiva proteção dos dados pessoais – e de seus titulares – é uma lei aplicável, que evite vazios legais ou a ‘*’sobreposição de legislações de diferentes países’’*(CASTRO, 2005, p. 53).

Portanto, conforme exposto nos dois últimos tópicos, a história dos direitos da privacidade e intimidade, seu avanço para um entendimento que compactue com a realidade atual, e resulte no direito de proteção de dados pessoais como autônomo, demonstra ainda mais a necessidade de lei específica no Brasil.

2 DADOS PESSOAIS COLHIDOS NA INTERNET: SUAS APLICAÇÕES E MECANISMOS

A utilização da internet se revela em números expressivos, sendo que atualmente excedeu a metade da população, isto é, mais de 4 bilhões[12] de pessoas fazem uso da mesma. Ao se debruçar sob a perspectiva do país observa-se que os brasileiros também acompanham: estima-se que 64% utilizam a internet, isso é, uma média de 116 milhões de pessoas[13].

Não há mais como imaginar um futuro sem sua existência, afinal sua presença é constante: celulares, notebooks, computadores e assistentes digitais. Ainda, observa-se que sua serventia é praticamente ilimitada, vai desde propósitos profissionais ao uso pessoal.

Não se pode olvidar também para o fato que a internet é um meio de comunicação interativa, que dada a sua maneira de ser vem a tornar suas fronteiras cada vez mais indeterminadas (CASTELLS, p. 19).

Nesse sentido, através dos mais diversos meios - aplicativos, softwares, pela própria internet (www), e e-mails, para citar alguns – são despejados milhares de informações e dados pessoais. E são nesses rastros significativos que se vislumbram, posteriormente, diversas utilidades para os dados pessoais coletados, quais sejam: a comercial, a de propaganda politica, o uso voltado para a governança e a sua aplicação para a vigilância.

Em continuidade aos conceitos e à relevância dada à proteção dos dados pessoais na internet, é necessário, portanto, compreender as estruturas, mecanismos e as aplicações dos dados pessoais. Para fins didáticos, esse capítulo será separado em três tópicos, cada qual apresentando e discorrendo acerca das finalidades - mencionadas alhures -, bem como sua dinâmica de operação.

2.1 UTILIZAÇÃO NO ÂMBITO COMERCIAL E EM CAMPANHAS POLÍTICAS

Conforme a história do mundo transcorre, muitos aspectos se modificam, em especial a economia. Com o advento da internet, dos espaços sociais na mesma, das tecnologias de informação, de uma ideia de economia global[14], de economia informacional global[15],

[12]Conforme a notícia disponível em: https://www.tecmundo.com.br/internet/126654-4-bilhoes-pessoas-usam-internet-no-mundo.htm
[13]Conforme a notícia disponível em: https://g1.globo.com/economia/tecnologia/noticia/brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-ibge.ghtml
[14]Sobre o tópico especifico consultar CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 2016.
[15]Sobre o tópico especifico consultar CASTELLS, Manuel. A sociedade em rede. São Paulo: Paz e Terra, 2016.

vislumbra-se uma aplicação dos dados pessoais para fins comerciais, em particular nos campos da publicidade, propaganda e marketing.

Talvez o melhor exemplo disso seja o Google, a empresa multinacional, desenvolvida por Lawrence Edward Page e Sergey Mihailovich Brin, em 1998, enquanto ambos estavam fazendo doutorado na *Stanford University*. Apesar da conhecida fama por plataforma de pesquisas, a empresa vai muito além e presta diversos outros serviços *online* – tais como o *Google Maps, Gmail, Google Apps*, Google Tradutor, é detentora do *Youtube*[16], entre outros –, bem como desenvolve softwares.

Com a sua expansão para além de uma ferramenta de busca, a empresa se reorganizou, em 2015, no formato de *holding*, sob o nome de *Alphabet Inc*. Sendo os serviços de anúncios da plataforma sua principal renda (MATTIUZZO, 2018, p.180 e 181).

Nessa esteira, foi criado o *AdWords*, que é a plataforma que desempenha, através de uma espécie elaborada de leilão, a publicidade para os anunciantes. A forma adotada é a venda de espaço publicitário, o qual varia conforme a escolha do anunciante, podendo ser divulgado nos próprios resultados de pesquisas do *Google Search* ou mesmo em qualquer site pago pelo Google que faça parte do *Display Network* (MATTIUZZO, 2018, p. 182).

Para tanto, a expansão da empresa só se concretizou em razão do aumento de dados pessoais colhidos dos usuários nos diversos serviços oferecidos pelo Google. Observa-se, nesse sentido, que seus serviços são singulares, uma vez que, combinam o comportamento online dos usuários com oportunidades de publicidade (MATTIUZZO, 2018, p. 184).

O eficiente sistema adotado pelo Google para conduzir suas publicidades emprega um algoritmo que calcula a relevância de uma publicidade para cada usuário diferentemente. De fato personaliza a busca de cada um, baseando-se na história de pesquisas anteriores, e também pelos dados colhidos dos usuários em sua navegação no *Youtube, Gmail*, e outros sites parceiros (MATTIUZZI, 2018, p. 186 e 187).

Como resultado da grande quantidade de informações obtidas pelo Google, por intermédio de seus serviços e outros parceiros, a empresa pode identificar desde dados pessoais de identificação de seus usuários – nome, endereço - à hora usual de dormir e sua condição médica (MATTIUZZI, 2018, p. 193 e 194).

O Google alega que o uso dos dados pessoais colhidos é somente para uso próprio das publicidades, não sendo vendido para terceiros, além de que o processo que efetua essa

[16]C.f.: https://www.bbc.com/portuguese/economia/story/2006/10/061009_googleyoutube.shtml

função é totalmente automatizado e não implica em qualquer envolvimento de pessoas (MATTIUZZI, 2018, p. 194).

Em relação às soluções para a proteção da privacidade, o Google adota uma postura de auto-regulamentação, em que cada usuário pode configurar na plataforma *MyActivity* conforme sua preferencia: consentindo ou não com o recolhimento de determinados dados pessoais e informações. Entretanto, ainda assim observa-se certa complexidade, uma vez que para proceder as configurações é exigido do usuário alto nível de conhecimento digital, da própria plataforma e seu engajamento espontâneo (MATTIUZZI, 2018, p. 196).

Outro exemplo relevante é a rede social Facebook, fundada por Mark Zuckerberg, Eduardo Saverin, Dustin Moskovitz e Chris Hughes em 2004. Tem-se que, assim como o Google, sua principal fonte de renda são os anúncios publicitários, conforme o próprio relato do CEO, em depoimento dado ao comitê de senadores dos Estados Unidos da América (BBC BRASIL, 2018).

Porém, diversamente do Google, seu funcionamento não está claro. O CEO da empresa assegura que os dados colhidos na rede social dos usuários não são vendidos, contudo, incoerentemente, confirma que toda movimentação e informações coletadas de quem faz uso da rede social são armazenadas (BBC BRASIL, 2018).

Ainda nesse contexto de desproteção dos dados pessoais e a desinformação acerca da rede social, atrela-se as notícias divulgadas, em março de 2018 – pelo *New York Times* e *The Guardian* –, que os dados pessoais de cerca de 87 milhões de usuários do Facebook foram repassados para a empresa de elaboração de campanhas politicas Cambridge Analytica. O ‘*’Brasil também aparece na lista, como o oitavo mais atingido, com 443.117 usuários’’* (G1, 2018).

O mais alarmante é que as informações coletadas não foram só dos usuários da plataforma, mas também de pessoas que não possuem perfis na rede social – conhecidos por ‘’perfis sombra’’. O CEO do Facebook, ‘*’na audiência da Comissão de Energia e Comércio da Câmara de Representantes dos Estados Unidos’’*, justificou a prática afirmando que se decorria por razões de segurança. Mark negou que a plataforma grave conversas pelo microfone do celular, e declarou que só utilizam para fins de publicidade os áudios contidos nos vídeos postados pelos próprios usuários na rede social. Além de que, com o argumento de fins de segurança e publicidade, confirmou que realizam a coleta de informações das *‘’atividades realizadas quando a pessoa não está logada na plataforma, como os sites visitados’’*. Quando questionado acerca da privacidade de seus usuários replicou que ‘*’a*

proteção está na capacidade dos usuários de escolherem o que e para quem compartilham conteúdos'' (ÉPOCA NEGÓCIOS, 2018).

Não fosse só isso, descobriu-se também que a gigante da mídia social possui parcerias de compartilhamento de dados com pelo menos 60 empresas, as quais citam-se Lenovo, Oppo, TCL, Amazon, Apple, BlackBerry, Samsung e Huawei – empresa que foi apontada como ameaça à segurança nacional pela agência inteligência americana (DANCE; CONFESSORE; LAFORGIA, 2018).

Isso significa que o Facebook dispõe às empresas parceiras os dados pessoais colhidos de seus usuários – que supostamente concordam com alguns termos de privacidade – e dos amigos de seus usuários. Ainda, confirmou-se que os referidos acordos datam do ano de 2007, há mais de uma década. Por fim, já que muitos aparelhos eletrônicos e celulares não conseguiam executar perfeitamente o aplicativo do Facebook, a justificativa dada pela empresa de mídia social foi que os acordos celebrados se deram a fim de possibilitar o pleno funcionamento do seu serviço em forma de aplicativos nos mais variados produtos – todos os tipos de celulares, *smart Tvs* e videogames (DANCE; CONFESSORE; LAFORGIA, 2018).

Outra adversidade acerca da privacidade e proteção dos dados pessoais se presenciou quando um defeito técnico da plataforma configurou todas as publicações – disparadas entre 18 a 27 de maio – como no modo ‘’pública’’, apesar da configuração pessoal de cada usuário –. Estima-se que as publicações de aproximadamente 14 milhões de pessoas foram atingidas. (MORSE, 2018).

Soma-se a essa conjuntura que o Facebook comprou o *WhatsApp* e o *Instagram*, outras redes sociais amplamente utilizadas mundialmente (GUILHERME, 2014).

O professor Tim Wu, da *Columbia Law School*, antigo conselheiro da Comissão de Comércio Federal dos Estados Unidos, afirma que o Facebook busca se tornar uma ‘*’gigante da publicidade*’’, a maior empresa do mundo enquanto trata com as informações sensíveis dos seus 2 bilhões de usuários. Também assevera que a empresa não lida com os dados pessoais de seus usuários com o zelo devido. E quanto à necessidade de proteção aos dados pessoais colhidos, adverte que o seu armazenamento se compara ao manuseio de ‘’*resíduo radioativo''*, tamanha a seriedade (BURCH, 2018).

Em relação à falta de transparência do funcionamento da empresa, Tim Wu alerta (BURCH, 2018)[17]:

[17]Texto original: *“There’s a number of abusive apps and they dig a lot more of your data than you thought they were. One of the big problems is Facebook gave you the impression you could control your own privacy by*

> Há um número abusivo de aplicativos e que buscam por dados pessoais muito mais do que se pensa. Um dos maiores problemas é que o Facebook deu a impressão que se podia controlar a própria privacidade, definindo suas configurações de certas maneiras – porém, essas configurações não alteraram nada. Elas se tratavam de falsos botões. (tradução nossa).

Nessa conjuntura, tem-se que são poucas empresas – multinacionais – que detém o controle sobre a maioria dos dados pessoais da população mundial (MATTIUZZO, 2018, p.177).

Ainda, nesse sentido, a empresa Uber em breve utilizara em sua plataforma, através de inteligência artificial a ferramenta que possibilita ao motorista do carro saber se a pessoa que solicitou o serviço está em "estado normal ou anormal'' (TRINDADE, 2018). Ou seja, será mais um dado pessoal coletado acerca dos usuários do aplicativo.

Consoante as reflexões feitas alhures, soma-se que horas após a entrada em vigor da Lei de Proteção de Dados Pessoais Europeia, em 25 de maio de 2018, foram realizadas denúncias contra o Facebook, o WhatsApp, o Instagram, e o Google, sob o fundamento de compelir os usuários às suas políticas de privacidade para conseguirem fazer uso de seus serviços (FOXX, 2018).

No mais, outra modalidade de uso comercial dos dados pessoais constitui-se na sua aplicação para fins de campanhas políticas – entende-se aqui por modalidade comercial, uma vez que os dados pessoais colaboram na elaboração de publicidade de partidos e candidatos de forma personalizada. Essa última categoria, no entanto, traz consigo consequências que ultrapassam a proteção de dados pessoais e ingressam na seara do estado democrático de direito.

As agências de marketing político observaram que a utilização de meios diversos das mídias tradicionais de massa se mostrou uma vantagem, já que os provedores de aplicação *''influenciam na formação da opinião publica e podem propiciar mudanças de comportamento politico dos eleitores por meio de seus algoritmos''*, bem como, *''o big data contribui para que as pesquisas de opinião sejam mais efetivas''* (SANTOS, 2018, p. 1).

Para ilustração, cita-se a campanha do então candidato à presidência dos Estados Unidos da América Barack Obama, em 2008, em que sua *''equipe de marketing captou diversos dados pessoais sensíveis a ponto de obter um histórico de preferencias, interesses e comportamento de seus eleitores, a fim de viabilizar o envio de e-mails personalizados''* (SANTOS, 2018, p. 12).

Complementa-se, em relação ao caso supracitado (SANTOS, 2018, p. 12):

---

setting your settings in certain ways — but those settings didn't do anything," said Wu. "They were like fake buttons."

> [...] os dados eram coletados de forma variada – redes sociais, sites, serviços de localização (gps), plataformas de doações. Acrescenta-se que a obtenção desses dados foi facilitada pela transferência indevida dessas informações entre provedores e empresas de marketing e publicidade, bem como demais parceiros comerciais, como instituições financeiras.

Como já apontado anteriormente, assim como o Google, o Facebook também personaliza o conteúdo mostrado aos seus usuários, o que não difere quando analisado sob a perspectiva de ações eleitorais, uma vez que o ‘*’perfil indica a um candidato quem é potencialmente mais receptivo às bandeiras e ideologias que ele representa’’* (NEIRA, 2018).

Portanto (NEIRA, 2018):

> Desta forma, a propaganda paga é direcionada com precisão, independentemente da qualidade da informação contida nela, que pode ser deturpada ou falsa. Além disso, o eleitor acaba entrando em uma espécie de bolha. Quanto mais ele navega, mais fornece suas preferências, que limitam o tipo de conteúdo recebido.
>
> Desta forma, a equipe de um candidato pode identificar não apenas preferências políticas, mas até mesmo as demandas de uma determinada região, de acordo com o comportamento dos usuários nas redes sociais.

Ao debruçar-se no contexto atual do Brasil, qual seja: das eleições do presidente, dos governadores, dos senadores, dos deputados federais, estaduais e distritais, todas a serem realizadas no final de 2018, vislumbra-se mais uma vez a urgência de lei específica que regularize o uso dos dados pessoais.

As opiniões de especialistas e estudiosos da área alertam que esse emprego de marketing político tem como resultado o prejuízo do ‘*’debate político em tempos de polarização e proliferação de candidaturas’’* e a fácil manipulação da opinião pública (NEIRA, 2018).

Outro fator que contribui para o uso dessa modalidade de publicidade eleitoral foi ‘*’a redução de 90 para 45 dias de campanha e o menor tempo disponível durante a propaganda eleitoral gratuita na televisão’’*, tornando-se assim a internet ‘*’como o melhor meio de exposição para candidatos, especialmente os menos conhecidos’’*(NEIRA, 2018).

Outro fenômeno que se revela é o impulsionamento de propagandas politicas, em plataformas como o Google e o Facebook. Trata-se da prática de ‘*’pagar para que um conteúdo alcance determinado público em redes sociais’’*, bem como em outras plataformas digitais. Esclarece-se que esse recurso foi legitimado pela Lei 9504/97, qual seja a Lei Eleitoral do Brasil (AFFONSO, 2018).

E, não para por aí, com o desenvolvimento extraordinário das técnicas de informática, os *boots* – já abordados mais profundamente no capítulo primeiro – também auxiliam no marketing eleitoral, e inclusive em outras questões políticas notórias.

Seus impactos são perceptíveis, porquanto ‘*’bots contribuíram para direcionar o discurso e o fluxo de informações de forma cirúrgica, influenciando eleitores’’*(DONEDA; CÓRDOVA, 2018).

Nesse sentido (CÓRDOVA; DONEDA, 2017):

> Sua atividade impacta diretamente porque, entre outros motivos, alguns dos métodos mais utilizados para medições e estatísticas em redes sociais envolvem metodologias quantitativas. Desse modo, se os bots existem em grande número, implicando elevado volume de informações, é possível que possam direcionar o fluxo dessas informações em redes sociais, pois algoritmos presentes em nessas plataformas geralmente priorizam o elemento quantitativo, não distinguindo entre bots e humanos. Desse modo também, muitas pessoas podem formar suas ideias e convicções – e decisões quanto ao próprio voto – a partir de direções que seus grupos sociais estão tomando, eventualmente influenciados por informação direcionada por bots.

No Brasil, verifica-se sua presença pelo menos desde as votações de 2010, o que alarma para suas consequências no debate democrático. No tocante à dimensão internacional, constatou-se que os bots tiveram papel fundamental em *‘’moldar o perfil do fluxo de informação no debate público em redes sociais, eventualmente influenciando concretamente no resultado de pleitos eleitorais como o norte-americano, o separatismo catalão ou a saída do Reino Unido da União Europeia’’*(DONEDA; CÓRDOVA, 2018).

Tal circunstância é incontestável, *‘’tanto é que existem diversas iniciativas legislativas que procuram restringir ou mesmo prescrever seu uso, ao mesmo tempo em que grandes plataformas anunciam modificações em seu modelo de publicidade na Internet para proporcionar maior transparência quanto ao financiamento da priorização de determinados assuntos em suas redes’’*(DONEDA; CÓRDOVA, 2018).

Para melhor aclarar a proporção de alcance dos bots salienta-se o estudo ‘*’publicado por Alessandro Bessi e Emilio Ferrara, do Instituto de Ciências Informacionais, da Universidade do Sul da Califórnia, um dia antes das eleições presidenciais americanas, de 2016, estimando a atuação de 400.000 (quatrocentos mil) bots no Twitter, ou seja, criando tweets, bem como retweetando’’*(BESSI; FERRARA, 2016 apud SANTOS, 2018, p. 19).

O estudo aponta que esses bots sociais foram capazes de dar a falsa impressão de grande contingente de eleitores adeptos a algum candidato, quando na verdade tratavam-se de ‘’opiniões’’ sinteticamente geradas pelos bots (BESSI; FERRARA, 2016 apud SANTOS, 2018, p. 19).

Ainda, acerca do elevado nível de desenvolvimento dos bots, o pesquisador Alessandro Bessi se deparou com complexidades na tarefa de discernir twittes reais ou gerados por bot, porquanto alguns perfis *''produziam cerca de 1.000 tweets por hora''* e ‘*''outros pareciam que ''iam dormir'' (ficavam off-line por um longo período de tempo no dia) e tweetavam cerca de 5, 10 ou 15 tweets em sequencia e, depois, nada por horas*’’(BYRNES, 2016 apud SANTOS, 2018, p. 20).

Sem deixar o âmbito político e eleitoral, testemunha-se também a disseminação de notícias falsas – ou *fake news* –, que tratam-se na verdade de um negócio lucrativo, uma vez que pode-se ganhar em publicidade online, e geralmente atuam contra algum candidato ao difundir historias fictícias (WENDLING, 2018).

Apesar de nunca ter se noticiado nenhuma ligação direta de candidatos ou partidos pagando para a circulação de *fake news*, nota-se que os responsáveis pelo financiamento das mesmas são pessoas ou algum grupo de interesse – pessoa física ou jurídica –, que contemplem alguma vantagem em sua propagação, como ocorreu no caso das eleições americanas, de 2016, em que se descobriu que empresas russas financiavam notícias irreais a respeito da então candidata Hillary Clinton (STEIBEL, 2018).

Nesse sentido, destaca-se a existência de uma espécie de ‘’fazenda de trolls’’ russa, denominada *Internet Research Agency* (IRA), que através de *bots* alastra notícias (frequentemente falsas) e opiniões de cunho político – com ideologias e doutrinas, geralmente polarizadas –, no intento de manipular os debates públicos (SALAS, 2017).

O relatório apresentado pela *Freedom House*[18], entidade americana que visa à promoção de direitos fundamentais, como liberdade e democracia, para sociedades repressivas, aponta a China, pelo terceiro ano consecutivo, como o governo que mais censurou a liberdade na internet.

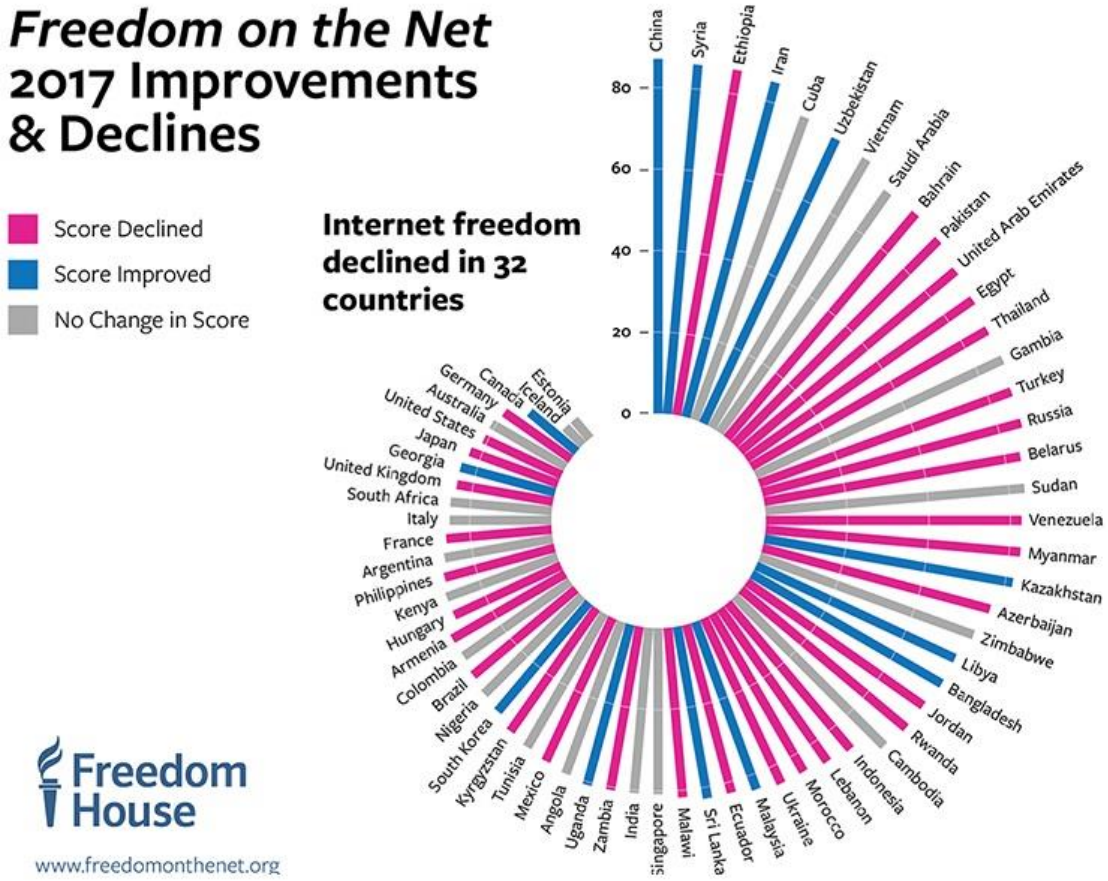
O estudo indicou que 30 países – entre eles Venezuela, Turquia e Filipinas – utilizavam uma espécie de ‘*’exército de formadores de opinião*’’, que eram pagos pelos governos para responder críticas e disseminar suas ideologias. Além disso, apurou-se que essas manobras políticas cresceram abundantemente, em razão da utilização de *bots, fake news* e algoritmos de pesquisa.

Os números são expressivos, tem-se que somente 23% dos usuários de internet pelo mundo não tem sua internet de alguma forma censurada, enquanto que 36% sofrem censura e 28% são parcialmente censurados.

[18] Disponível em: https://freedomhouse.org/report/freedom-net/freedom-net-2017

Da leitura de um dos gráficos apresentados no relatório (Figura 1) – gráfico de título *Freedom on the Net 2017 Improvements & Declines* – pode-se extrair a informação que o Brasil teve sua liberdade na internet reduzida, tal quais outros países sul-americanos.

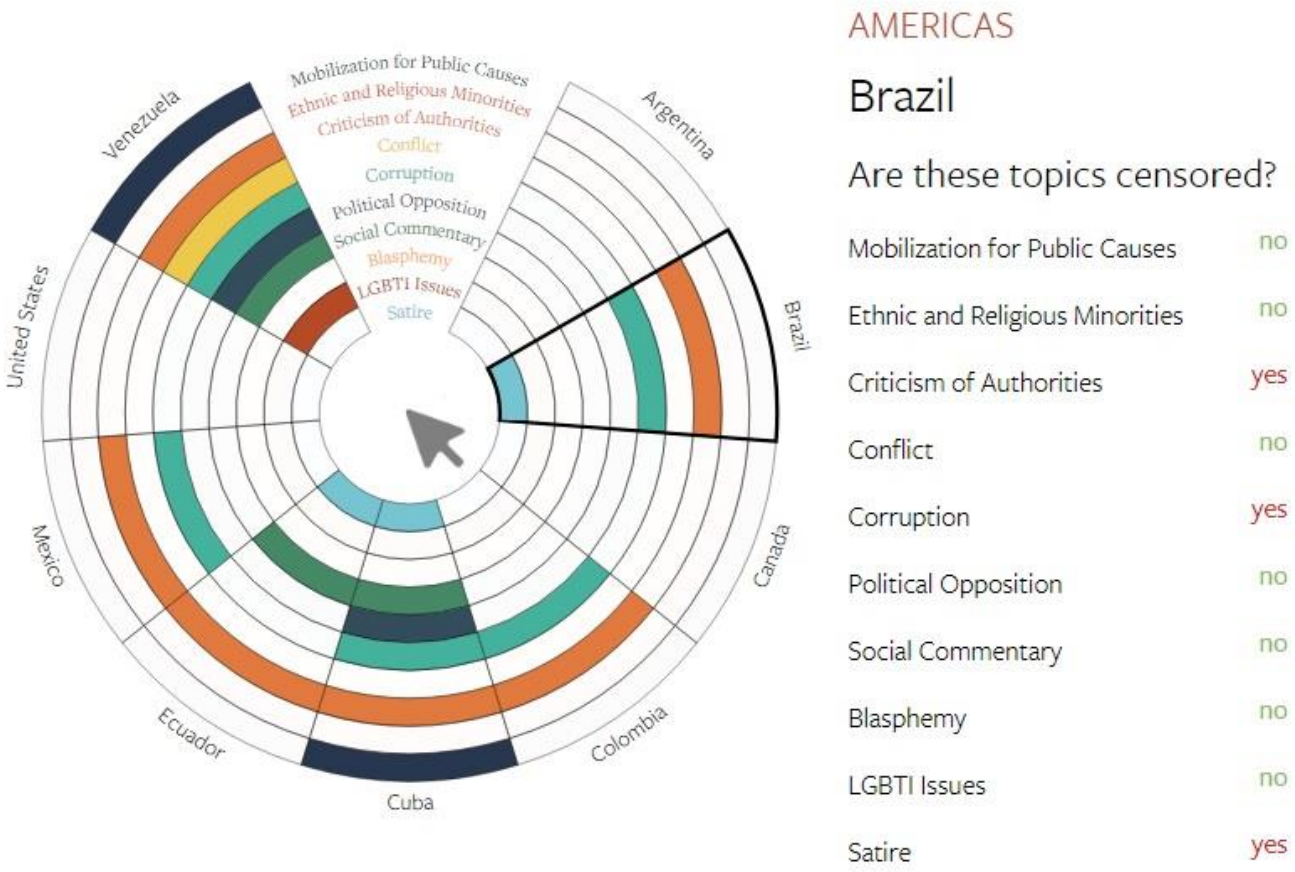
Figura 1: *Freedom on the Net 2017 Improvements & Declines*



Fonte: FREEDOM HOUSE, 2017.

E da leitura do gráfico (Figura 2) – de título *Censored Topics by Country* – conclui-se que os assuntos censurados pelo governo brasileiro foram: sátiras, corrupção e críticas a autoridades.

Figura 2: *Censored Topics by Country*



Fonte: FREEDOM HOUSE, 2017.

Em entrevista no programa Conversa com Bial[19], realizado no dia 02/05/2018, Ronaldo Lemos, Diretor do Instituto de Tecnologia e Sociedade do Rio (ITS Rio), alerta para o fato que as *fakes news* resultam em desinformação. Acerca das eleições brasileiras, afirma que a única vantagem em relação às eleições americanas (2016) é que na atualidade se há ciência desse problema. Ratificou o fenômeno exemplificando que as até ‘*’as empresas de tecnologia já estão tomando providencias: eliminando perfils falsos, exigindo mais transparência para quem compra anúncios*’’.

[19] Entrevista completa disponível em: https://www.youtube.com/watch?time_continue=214&v=lD8ZUWXZORc

O pesquisador e advogado, em relação à polarização presente no Brasil, informa que ‘’*não há terreno mais propício para a fake news do que um momento em que as pessoas estejam com medo ou com raiva. Sempre que se tem uma sociedade que está neurótica, que está com pensamentos de temor, imediatistas, com medo de segurança* [...] *Enfim, questões que falam a sentimentos muito básicos e elementares, essa sociedade fica vulnerável à manipulação’’.*

Ronaldo Lemos ensina que não se pode confundir opinião pública com a *timeline* das redes sociais, essa última não pode ser entendida como o retrato do ponto de vista popular. Nesse viés, preconiza a necessidade da promoção de educação de mídia para a sociedade.

Em vídeo explicativo, também transmitido no programa, Marcos Konopacki, Coordenador de Projetos do ITS, explica que os *bots* são ‘’*programas de computador, que interagem em redes sociais com fim específico de fazer uma ação repetitiva, uma interação programada para ser feita’’*. Ele alcunha os *bots* como *‘’a gasolina da desinformação’’*, e nesse sentido esclarece que são os *bots* que difundem, rapidamente, as informações falsas que são publicadas em perfis *fakes*. Ainda alerta que essas disseminações de *fake news* podem tornar uma eleição injusta e, assim, ameaçar a democracia.

Por fim, à luz desses conhecimentos, resta claro que a Internet, acompanhada de suas facilidades e o intento de ‘*’propiciar o fluxo de informações e permitir o compartilhamento do conhecimento*’’ ultrapassa essa concepção idealista e diante do monopólio de capacidade técnica e humana das empresas de provedores de aplicações de internet, e dos interesses em jogo – sejam políticos ou propriamente corporativos – transpõem-se para a noção de que não há equilíbrio entre os interesses dos usuários e os demais atores nessa relação (SANTOS, 2018, p. 23).

Ainda nessa toada, vale ressaltar que, apesar da ausência especifica de regulamentação, o Marco Civil da Internet empenha-se em uma tentativa de proteção aos dados pessoais quanto ao seu uso por provedores de conexão e provedores de aplicação.

Nesse sentido, destacam-se os arts. 14 e 16 da Lei 12.965/2014, que assim preconizam:

> Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.
>
> Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
> I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7o; ou
> II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Para a completa compreensão, tem-se que ‘’*provedor de conexão à internet é pessoa, física ou jurídica, que atribui endereços lógicos de acesso necessários aos usuários para se utilizarem das redes de informação e comunicação’’* (GONÇALVES, Victor Hugo, 2017, p. 131) e ‘*’provedor de aplicações de internet é a pessoa jurídica que presta serviços ou comercializa produtos nas redes de informação e comunicação que não envolvam acesso e conexão lógica de usuários’’* (GONÇALVES, Victor Hugo, 2017, p. 134).

A nova lei, portanto, ‘*’veda (i) a guarda de registros de acesso e aplicações da Internet por parte dos provedores de conexão e (ii) a guarda de acessos a outras aplicações de internet, sem consentimento do usuário’’* (KUJAWSKI; THOMAZ, 2014, p. 688).

Os mesmos autores acima mencionados destacam que (KUJAWSKI; THOMAZ, 2014, p. 688):

> A primeira vedação é absoluta, ou seja, não comporta exceção. Com efeito, não se antevê qualquer objetivo legitimo em se permitir que o provedor de conexão à internet conheça as informações relativas aos hábitos de seus clientes na utilização da internet. Seria como permitir que as empresas de telefonia tivessem acesso ao conteúdo das comunicações realizadas por seus usuários, simplesmente porque oferecem o meio pelo qual a comunicação se estabelece.

Dessa forma, tem-se que diante do acesso dos provedores de internet a informações e dados transferidos pelos seus usuários, o Marco Civil visa ‘’*proteger o usuário do vigilantismo dos provedores que, por ventura, tenham a intenção de monitorar os comportamentos de seus usuários na internet’’* (GONÇALVES, 2017, p. 132).

Ainda (COLNAGO, 2014, p. 767):

> [...] se o provedor de conexão dispuser da informação acerca de quais aplicações de internet são mais acessadas por seus clientes, aberto estará o caminho para que ele busque firmar acordos comerciais de acesso preferencial diretamente com os provedores de tais aplicações. Um meio ambiente digital sustentável, pois, pressupõe que todos possuam acesso igualitário à rede, sem o estabelecimento de escolhas preferenciais entre os grandes conglomerados econômicos que hoje contribuem para moldar a rede. Aí é que reside a instrumentalidade do dever previsto no artigo 14 para com a neutralidade de rede e, logo, para com a preservação do meio ambiente digital.

Em relação à vedação dada aos provedores de aplicações, o art. 16 concede garantias aos dados pessoais, porém com pouca efetividade, ‘*’já que não existe um órgão regulador de internet e defensor dos usuários’’* (GONÇALVES, Victor Hugo, 2017, p. 143).

Portanto, conforme o título desse tópico trata-se mais de uma tentativa de proteção, rasa, com pouca efetividade, evidenciando assim mais uma vez a necessidade de regulação própria e específica para os dados pessoais.

2.2 APLICAÇÕES DOS DADOS PESSOAIS NA VIGILÂNCIA GOVERNAMENTAL

Verifica-se a utilidade dos dados pessoais também na manipulação por governos, num fenômeno mais conhecido por *surveillance.*

Surveillance vai além de sua tradução literal para o português, qual seja vigilância. Seu significado engloba vários outros aspectos e sua tradução simplória desconsidera seu novo entendimento – *new surveillance*. (MORAIS; NETO, 2014, p. 421).

Ressalta-se que essa utilização para os dados colhidos de usuários da internet se deu principalmente após o atentado terrorista de 11 de setembro de 2011, que ocorreu na cidade de Nova York, e desencadeou um estado de vigilância e monitoramento efetuado pela NSA-National Security Agency.

O conhecimento público dos procedimentos adotados pela agência de proteção estadunidense só se tornam possível graças às declarações e documentos prestados pelo seu ex-funcionário, o analista de sistemas Edward Joseph Snowden[20].

Nesse sentido, cita-se a colocação de José Luiz Bolzan de Morais e Elias Jacob de Menezes Neto (MORAIS; NETO, 2014, p. 425):

> Atualmente, um dos objetivos primordiais da surveillance é a previsão de comportamentos futuros, seja por parte do poder público – prever atitudes terroristas, por exemplo -, seja pela iniciativa privada – para prever quais as melhores formas de ganhar dinheiro com anúncios, exemplificativamente. O homem é um animal de hábitos, de maneira que, com a coleta de informações diversas durante período de tempo suficiente, é possível prever padrões de comportamento, deslocamento, preferencias e interação social.

Trata-se, portanto, de mais uma forma de categorização dos indivíduos, de forma pouco ou nada democrática, podendo levar, nesses casos específicos, à violação não só da proteção aos dados pessoais, mas de outros direitos fundamentais (MORAIS; NETO, 2014, p. 419).

A título de exemplo, citam-se as *no-flight lists*, isto é, listas - criadas e mantidas pelo governo dos Estados Unidos - que contêm nomes de pessoas impossibilitadas de viajar de avião por serem consideradas uma possível ameaça terrorista. (MORAIS; NETO; 2014, p. 437).

Uma tecnologia também usada pelos governos é a de reconhecimento facial, sabiamente na Rússia, China e Estados Unidos. A ferramenta pode ser aplicada em casos de

[20]Recomenda-se a leitura da notícia contida no link: https://observador.pt/seccao/mundo/edward-snowden/ , e o filme SNOWDEN: Herói ou Traidor. Direção de Oliver Stone. Produção de Moritz Borman, Eric Kopeloff, Philip Schulz-deyle, Fernando Sulichin. [s. I.]: Endgame Entertainment, Wild Bunch Krautpack Entertainment, Onda Entertainment, Vendian Entertainment, 2016. Son., color. Legendado.

terrorismo – para identificar o praticante – ou ainda para casos mais simplórios de multas quando algum cidadão atravessa a rua fora do local permitido (ELOLA, 2018).

De acordo com o diretor do *Law's Center on Privacy and Technology*, Álvaro Bedoya, acerca dos bancos de dados policiais americanos (ELOLA, 2018):

> Os bancos de dados de DNA e impressões digitais eram compostos por pessoas com antecedentes penais. Está sendo criado um banco de dados biométricos de pessoas que respeitam a lei.

E ainda que (ELOLA, 2018):

> Na Rússia ela [a tecnologia] é usada para identificar manifestantes. Nos EUA, também. Caminhamos para uma sociedade de controle. Pode-se identificar qualquer um, a qualquer momento, por qualquer motivo.

Em ações preventivas de policiamento o mecanismo é usado a fim de antecipar o lugar e o autor de um possível crime, mediante à analise de câmeras de seguranças instaladas em lugares públicos (ELOLA, 2018).

Nessa linha[21], a preocupação se estende para quem esses dados pessoais biométricos podem recair. Afinal, governos que tem '*'problemas de direitos humanos e restrições às liberdades"* teriam, dessa forma, *''um tremendo instrumento de perseguição de dissidentes''* (ELOLA, 2018).

Outra demonstração do alcance da *surveillance* na denúncia de Edward Snowden é de que há a '*'possibilidade de acesso remoto às câmeras e microfones que as pessoas possuem em seus ambientes privados e domésticos*'' (BEZERRA, 2018, p.27).

Alguns documentos expostos na rede por Julian Assange, por intermédio do Wikileaks, reiteram essas informações, deixando claro que a CIA (Agência Central de Inteligência dos Estados Unidos da América) possui um serviço secreto de hacking (SPUTNIK, 2017).

O conjunto de documentos – denominado ''Vault 7'' – vazou na rede diversos documentos oficiais da agência de inteligência que relatam '*'as táticas voltadas para invasão de celulares iOS, Android, computadores, roteadores e até televisores smart''* (PAYÃO, 2017).

Esses mesmos documentos revelaram que a requerimento da CIA, a Agência de Segurança Nacional (NSA) espionou a eleição presidencial francesa de 2012 – que teve como

[21] Nesse sentido recomenda-se a leitura da notícia disponível em: https://www.theguardian.com/technology/2017/nov/26/government-could-allow-firms-to-buy-access-to-facial-recognition-data

principais concorrentes o então presidente Nicolas Sarkozy e o candidato François Hollande – a fim de obter informações acerca de suas alianças, fontes de financiamento e interações políticas. Além disso, informaram que ‘*’no mesmo período os serviços secretos americanos espionaram o Palácio do Eliseu, realizando escutas telefônicas clandestinas a partir de um centro instalado no último andar da embaixada dos Estados Unidos em Paris’’*(NETTO, 2017).

Em um grupo distinto de documentos expostos pelo Wikileaks, emitidos ‘*’sob o nome da secretária de Estado americana, Hillary Clinton, pede que se coletem informações "biográficas e biométricas" - incluindo amostras de DNA, impressões digitais e biometria da íris - de funcionários-chave da ONU. Também foram pedidos dados de cartões de crédito, endereços de email, senhas e decodificadores usados em redes de computador em comunicações oficiais’’* (BBC BRASIL, 2010).

Nessa mesma perspectiva, em consideração ao manuseio pelos governos de dados pessoais, cita-se o recente caso em que se verificou a possibilidade de o governo brasileiro estar vendendo dados pessoais (LEMOS, 2018).

O Ministério Público do Distrito Federal está em investigações acerca de possíveis vendas de dados de identificação – nomes, endereços, CPF, data de nascimento, entre outros – além de situação fiscal, procedidas pelo Serviço Federal de Processamento de Dados (Serpo) à entidades privadas e a outros órgãos públicos (LEMOS, 2018).

Nesse sentido, destaca-se que (LEMOS, 2018):

> Se forem comprovadas as alegações do MP, o Brasil será o primeiro país do mundo a oficializar o vazamento de dados mediante pagamento. Enquanto outros países lutam para tornar suas bases de dados mais seguras e restritas, no caso brasileiro é só pagar para ter acesso a tudo.

Nessa toada, se torna mais nítido a necessidade de que a futura lei de proteção de dados pessoais brasileira também se aplique para o setor público, e, da mesma forma que para o setor privado. No entanto, tem-se que, por exemplo, um dos projetos de lei nesse sentido, institui a Controladoria Geral da União (CGU) como o órgão competente a fiscalizar o Estado, ao contrário de um órgão específico para tratar do assunto (LEMOS, 2018).

2.3 UTILIZAÇÃO DOS DADOS PESSOAIS PARA FINS DE GOVERNANÇA ELETRÔNICA

Primeiramente, importante esclarecer que a palavra governança, nesse tópico, não deve ser confundida com o conceito de ‘’governança da internet’’, que pode ser entendida por[22]:

> Governança da Internet é o desenvolvimento e a execução pelo governo, pelo setor privado e pela sociedade civil, em suas respectivas funções, de princípios, normas, regras, procedimentos decisórios e programas que moldam a evolução e o uso da internet (tradução nossa).

Na verdade, nesse caso, a expressão correta é ‘’governança eletrônica’’, qual seja[23]:

> [...] é uma expressão cujo significado remete à implementação, utilização e disseminação das tecnologias da informação e da comunicação — TICs — no âmbito do poder público, com vistas à melhoria da gestão pública, do monitoramento e da avaliação das políticas públicas e à ampliação do acesso do cidadão a todas as informações sobre os serviços públicos.

Tem se que, atualmente, as práticas sociais e as relações de cidadania devem ser incorporadas às tecnologias da informação e comunicação (TIC). Nesse sentido, a internet propícia aos governos seu uso a fim de promover a participação cidadã e o controle social (VAZ, 2005).

Acerca de seu funcionamento, cita-se[24]:

> Com o avanço das inovações em sistemas de informação e outras ferramentas digitais, a governança eletrônica é parte importante da administração de um governo, pois visa a facilitar e aprimorar a interação dentro do próprio governo, entre o governo e os cidadãos e entre o governo e a iniciativa privada. Para tanto, os governos atuam constantemente no desenho e na implementação de novos sistemas de informação e de comunicação, tendo como base a utilização da internet, de modo a melhorar, a cada dia, a acessibilidade a dados, informações e disponibilização de serviços públicos.

Importante mencionar alguns direitos que devem ser observados para sua realização, quais sejam: a) direito à informação de interesse particular; b) direito aos serviços públicos; c) direito ao próprio tempo; d) direito a ser ouvido pelo governo; e) direito ao controle social do governo; f) direito à participação na gestão pública, sendo que os três primeiros se referem a direitos individuais e os últimos a direitos coletivos (VAZ, 2005).

---

[22] Texto original: ‘*’Internet governance is the development and application by Governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures, and programmes that shape the evolution and use of the Internet’’*. Conforme o estudo disponível em: http://www.wgig.org/docs/WGIGREPORT.pdf

[23] C. f.: https://politicaspublicas.almg.gov.br/temas/governanca_eletronica/entenda/informacoes_gerais.html?tagNivel1=176&tagAtual=10260

[24] C.f.: https://politicaspublicas.almg.gov.br/temas/governanca_eletronica/entenda/informacoes_gerais.html?tagNivel1=176&tagAtual=10260

Observa-se que a governança eletrônica, exige o ‘*’uso intensivo da tecnologia da informação no interior das organizações estatais’’*, e proporciona ‘’*interação entre sociedade civil e governos, tanto nacionais como subnacionais’’* (VAZ, 2005).

Para aclarar sua dimensão, explica-se que[25]:

> Pode-se considerar como integrantes da governança eletrônica sistemas de ensino a distância, prestação online de serviços públicos, licitações e compras feitas por meio eletrônico (como, por exemplo, o pregão eletrônico), sistemas de monitoramento e avaliação de políticas públicas, sistemas de execução orçamentária e financeira, sistemas de convênios, sistemas de administração de pessoal, sistema de administração de material e patrimônio, entre outros.

Em relação específica ao Brasil, algumas medidas que se pode observar para a iniciativa de governança eletrônica foram: a instituição, em 1999, do Programa Sociedade da Informação; a criação, em 2000, do Comitê Executivo de Governo Eletrônico e, o lançamento, em 2001, da Política de Governo Eletrônico (BRAGA; ALVES; FIGUEIREDO, SANTOS, 2018, p. 10).

Além do mais houve a disponibilização de certificação digital; a implementação do Portal da Transparência e do Portal da Previdência Social; a concretização da votação eletrônica e a possibilidade de pregões eletrônicos (BRAGA; ALVES; FIGUEIREDO, SANTOS, 2018, p. 11).

Conforme já exaustivamente debatido nos capítulos anteriores acerca da internet e suas consequências, percebe-se que com o uso mais amplificado da internet pelo governo, a fim de promover e viabilizar a governança eletrônica, nosso dados pessoais também se encontram sujeitos a essa administração.

Um exemplo concreto de sua utilização é o *"Decreto Federal no 8.789/2016, que dispõe sobre o compartilhamento de bases de dados na administração pública federal’’* (CELLA; COPETTI, 2017, p 40).

Da mesma forma, tem-se que o cidadão, para cumprir seu exercício de forma plena necessita para a emissão do seu título de eleitor ‘’*fornecer informações de caráter pessoal – nome, filiação, data de nascimento, sexo, endereço residencial ou comercial, tempo de vínculo com o município, se possui ou não irmão gêmeo, telefones, escolaridade e profissão – tem sua assinatura coletada digital e fisicamente’’*(CELLA; COPETTI, 2017, p 41).

Nesse sentido, atenta-se (CELLA; COPETTI, 2017, p 43):

---

[25] C.f.: https://politicaspublicas.almg.gov.br/temas/governanca_eletronica/entenda/informacoes_gerais.html?tagNivel1=176&tagAtual=10260

> Quando um indivíduo fornece dados a uma determinada repartição pública ou é pessoalmente associado a informações, ele o faz para um determinado propósito, quase sempre vinculado a área de atuação daquela entidade. Ao quebrar as barreiras entre os diferentes órgãos e entidades do Estado e permitir o compartilhamento, dados podem ganhar novo propósito para além do que foram coletados inicialmente.

Nessa toada, portanto, observa-se que a manuseio pelo governo dos dados pessoais, apesar da *‘’iniciativa pretende[r] alcançar eficiência’’* deve ser tratada de forma cuidadosa e contemplar a proteção necessária (CELLA; COPETTI, 2017, p 41).

3 REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Ultrapassados o contexto histórico da temática, os conceitos necessários para seu entendimento e a efetiva aplicação dos dados pessoais colhidos, resta claro sua ampla utilidade e a necessidade de regulação dos dados pessoais.

Neste tópico será discutido o Regulamento 2016/679 da União Europeia (*General Data Protection Regulation* – GDPR), que é a lei com mais relevância no cenário internacional acerca do assunto.

Relativamente à situação legislativa brasileira atual acerca da proteção de dados ainda serão abordados o Marco Civil da Internet e o projeto de Lei n° 5.276/2016, o Projeto de Lei n° 4.060/2012, o Projeto de Lei do Senado n° 330/2013 e, por fim, o Projeto de Lei da Câmara n° 53/2018.

3.1 REGULAMENTO 2016/679 DA UNIÃO EUROPÉIA

O Regulamento, também conhecido por *General Data Protection Regulation* – GDPR, dispõe em sua ementa que é *‘’relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados’’* e ressalta que *‘’ revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados)’’.*

Aqui, importa aclarar que a versão utilizada é a portuguesa (Portugal), e que, conforme estabelece a lei, se tornou aplicável em 25 de maio de 2018.

Nesse sentido, explica-se o conceito de Regulamento, modalidade esta utilizada pela União Europeia (GUIDI, 2018, p. 87):

> [...] são normas vinculativas diretamente aplicáveis a todos os países, incluindo-se aí seus cidadãos e pessoas jurídicas, valendo como se direito nacional fosse.

Anterior ao Regulamento, a principal fonte de regulação do tema era a Diretiva 95/46, que também tutelava acerca dos dados pessoais, e tinha em sua ementa conteúdo igual ao do referido Regulamento. Nesse sentido, tinha-se que a proteção de dados pessoais era dada através de um ‘’sistema’’, que incluía ‘*’’diretivas, regulamentos, decisões vinculantes e orientações de diversos níveis hierárquicos, criando um quadro legal de diversas camadas que partem sempre de orientações gerais e estabelecem normas cada vez mais especificas sobre os direitos e obrigações relativos aos dados pessoais’’* (GUIDI, 2018, p. 88).

Entretanto, esse sistema *‘’sofreu grande alteração, em 2016, quando foi aprovada uma grande reforma gestada de 2010’’* e introduziu o Regulamento hoje vigente (GUIDI, 2018, p. 91 e 92).

Nessa esteira, a proposta do capítulo é analisar, de forma geral, como o Regulamento lidou com a problemática dos dados pessoais.

Para tanto, destaca-se as considerações abarcadas pelo advogado Guilherme B. de Campos Guidi (2018, 92 e 93):

> Em primeiro lugar, em relação aos direitos individuais, a forma de expressão do consentimento e a relevância do adjetivo ‘’informado’’ foram reforçados, exigindo-se que o titular dos dados tenha acesso facilitado às informações sobre o tratamento, expressas de modo simplificado (ao invés da linguagem geralmente hermética dos contratos), e que seu consentimento seja expressado de modo destacado – com igual facilidade para a sua revogação. Ainda para reforçar direitos dos titulares, os direitos de acesso e de eliminação dos dados (na forma do ‘’direito do esquecimento’’) são reelaborados e expandidos, dando maior segurança ao titular e ao mercado.
>
> No que toca o reforço das Autoridades de Proteção de Dados, podemos citar a especificação de sanções que podem ser impostas aos responsáveis por tratamentos de dados que não respeitem as regras do GDPR, a responsabilização também do agente processador dos dados e a nova obrigação de notificação de violações de segurança de dados. Assim, empresas que sofreram ataques para roubo de dados ou que tiverem dados pessoais de seus clientes vazados, por exemplo, deverão agora notificar os titulares dos dados e a Autoridade de Proteção de dados sobre tal fato.
> Ainda nessa esteira, o novo Regulamento cria diversas regras sobre procedimentos de avaliação de impacto em privacidade, os chamados *Privacy Impact Assessments*, ou simplesmente PIAs. Apesar de não haver uma obrigação de registro de tratamentos de dados, em certos casos é exigido do controlador ou responsável que elabore tal estudo, de modo a reduzir os riscos à privacidade dos titulares dos dados, podendo submetê-lo à aprovação da Autoridade de controle.
>
> Por fim, o regulamento também traz algumas práticas que servem como incentivo ao responsável pelo tratamento dos dados pessoais para que este zele pelo cumprimento do regulamento e pela garantia da privacidade dos titulares dos dados.
> A primeira mudança vem pela consolidação dos conceitos de *privacy by default* e *privacy by design* como obrigações do responsável pelo tratamento. Nesse sentido, o responsável deve sempre construir seus produtos, serviços e processos tendo em mente a preservação da privacidade e os princípios gerais da matéria, além de utilizar como padra de operação a escolha pela preservação da privacidade em detrimento da publicidade na ausência de um posicionamento expresso do titular de dados.

> A segunda mudança, de igual importância, vem na reafirmação dos programas de incentivo ao cumprimento do Regulamento, pela criação de selos e sistemas de certificação relacionados ao grau de zelo da empresa com a privacidade de seus usuários.

Outro aspecto que se vislumbra é a possibilidade de efetivar a proteção dos dados pessoais ‘*’por soluções tecnológicas’’* (VALENTE, 2018, p. 112).

Nesse sentido (VALENTE, 2018, p. 111):

> [...] discutir a possibilidade de proteção de dados por meio de dispositivos e aplicativos. Esse tipo de prática recebeu na literatura especializada o nome de ‘*’Privacy by Desig’’* (PBD). As tecnologias adotadas com essa finalidade foram denominadas ‘’*Privacy-Enhancing Technologies*’’ (PETs). Muitas vezes, os conceitos de confundem, mas no presente texto serão trabalhados de forma separada, sendo o primeiro relacionado à prática global de orientação de todo o processo de desenvolvimento e fabricação com o objetivo de assegurar a privacidade e a proteção dos dados do usuário e de coletividades e o segundo a denominação de toda a sorte de solução tecnológica que tem esta orientação em seu design.

Ainda, importa ressaltar que o Regulamento recorre para qualquer pessoa localizada na União Europeia, e não só a cidadãos europeus.

Nesse sentido (SOPRANA, 2018):

> A GDPR passa a guiar como essas empresas, que lidam com vastos bancos de dados, precisam se comportar diante dos usuários. A regulamentação impõe uma série de normas que estimulam termos de uso mais compreensíveis, controles de privacidade simples, ferramentas que dão poder de gerenciamento aos usuários sobre suas informações, reforço de segurança cibernética e condutas internas que possam garantir conformidade legal com a proteção de dados.

Observa-se que a GDPR ‘*’incide sobre qualquer serviço, empresa e entidade que coleta dados na União Europeia, seja uma farmácia, um cinema ou o varejo’’* (SOPRANA, 2018).

Em relação às grandes empresas tem-se que (SOPRANA, 2018):

> Organizações que lidam com alto fluxo de dados tendem a sentir maior impacto, como redes sociais, lojas virtuais, data brokers (uma empresa que reúne e vende informações de consumidores na internet), instituições bancárias, de pesquisa, de saúde e serviços públicos, pois precisarão realizar adaptações sob risco de multas pesadas.

A lei estimula a transparência das empresas e organizações que lidam com os dados pessoais. Em seu teor obrigam-nas a estarem ‘*’aptas a comunicar sua responsabilidade sobre o ciclo de vida dos dados: coleta, tratamento, compartilhamento, armazenamento e descarte’’* (SOPRANA, 2018).

Tanto é, que após 25 de maio de 2018, os usuários residentes na Europa passaram a receber em seus e-mails diversos termos de atualização de serviços das diversas empresas e

organizações que lidam com seus dados. Um exemplo notório é o do Facebook, que disponibilizou, somente aos cidadãos europeus e pessoas lá residentes, sua nova e detalhada justificativa legal para a coleta de dados (OBRIEN, 2018).

O consentimento dos titulares dos dados pessoais, conforme já mencionado, é tido como de extrema relevância. Para garantir de fato esse direito tem-se que os antigos contratos de ‘’adesão’’ não são mais aceitos (SOPRANA, 2018).

Nesse toada (SOPRANA, 2018):

> A mudança prática para os cidadãos é: os novos modelos de contratos agora deverão vir com opt-in, um botão que expressa a vontade ou não de o usuário em aceitar fornecer seu dado. Opções pré-marcadas em termos de uso ou em questionários eletrônicos não servirão mais como consentimento.

De igual forma, ‘*’o compartilhamento de informações pessoais com terceiros (como outras organizações e empresas’’* não poderá ser mais como nos modelos anteriores, em que se apresentava aos usuários como pré-condição para utilizarem do serviço ofertado. Deverá, ainda, possibilitar ao usuário a revogação do compartilhamento no momento em que o mesmo desejar (SOPRANA, 2018).

No tocante às dúvidas recorrentes, após o já consentimento do usuário, aponta-se que (SOPRANA, 2018):

> Além do consentimento, outro pilar legal da GDPR é o legítimo interesse. Uma empresa pode julgar que será positivo para seu cliente se compartilhar seu dado pessoal com um terceiro, por exemplo. O farol ético, nesse caso, deve ser: isso quebra a expectativa do usuário? Se ferir qualquer outro direito fundamental dele, é provável que a decisão esteja errada. A dica às empresas é: ficou na dúvida na hora informar e pedir novo consentimento? Informe e peça.

Ademais, a lei oportuniza a portabilidade e a revogação dos dados pessoais, se assim requisitado pelo seu titular. Por exemplo, o cidadão pode solicitar que seus dados sejam transferidos de uma empresa para outra, ‘*’é como mudar de operadora e autorizar que todo o pacote de informações vá de uma marca a outra, com segurança’’*. A diferença é que se aplica para o Facebook, Google, e outras empresas afins (SOPRANA, 2018).

Especificamente às orientações estipuladas acerca da revogação, esclarece-se que (SOPRANA, 2018):

> Empresas terão um mês para entregar os dados de forma estruturada. Se um indivíduo decidir que não quer mais usar o aplicativo de corridas, pode requerer a devolução. Provavelmente receberá uma tabela com as localizações de GPS pelos lugares em que se exercitou.

Já acerca da prática de *profiling* – que trata-se de um modelo de negócio da publicidade –, a proteção é relativizada. O regulamento assegura que as pessoas que se

sentirem prejudicadas de alguma forma com essa técnica podem solicitar informações a respeito do processo (SOPRANA, 2018).

A fim de aclarar o que se compreende por profiling, menciona-se (SOPRANA, 2018):

> [...] dados pessoais passam por um processo de pseudoanonimização, em que são cruzados e agregados a outros dados. Assim, plataformas podem criar grupos de consumo específicos e otimizar o direcionamento de publicidade, sem que saibam quem são seus alvos.
> Por exemplo: se uma marca de esportes quiser anunciar a pessoas como "Júlia Silva, de 29 anos, que ganha R$ 20 mil, mora na rua X e corre no parque Y" na internet; alcança o grupo a qual pertence Júlia Silva: "mulheres na faixa de 30 anos, moradoras de determinada região de São Paulo, com alto poder aquisitivo e adeptas a um estilo de vida saudável".

E, ainda (MAILJET, 2018)[26]:

> [...] Profiling é definido por mais que a simples coleta de dados pessoais; inclui-se o uso de dados para avaliar certos aspectos relativos a um individuo. O objetivo é prever comportamentos dos indivíduos e fazer decisões sobre o mesmo. No contexto de publicidade via e-mails, afeta na escolha de mandar uma campanha dirigida a um alvo especifico ao invés de outra.
> Profiling pode ser definido por três tópicos específicos:
> - Implica em uma forma automatizada de processamento;
> - Se procede através do manuseio de dados pessoais; e
> - Seu propósito é prever comportamentos dos indivíduos e fazer decisões sobre o mesmo. (tradução nossa).

Nesse sentido, ainda ressalta-se que crianças não podem ser submetidas ao *profiling* (MAILJET, 2018).

A aplicação da territorialidade da lei pode alcançar empresas brasileiras. Estão sujeitas a lei: empresas brasileiras de data broker e de publicidade que terceirizem a empresas europeias a coleta e o tratamento de dados, e *''empresas brasileiras com filiais na União Europeia ou que estejam fora do bloco mas ofereçam serviços ao mercado europeu''*, além de qualquer empresa que colete, monitore, processe e trate dados de pessoas localizadas no bloco europeu (SOPRANA, 2018).

As empresas de e-commerce, quando direcionados ao publico europeu, também estão nessa seara. Já as pequenas *''lojas poderão fazer adaptações em relação ao ciclo de vida dos dados, mas dificilmente estarão sujeitas a multas''* (SOPRANA, 2018).

Frisa-se que a lei vale quando algum processamento ou a própria coleta dos dados se dá no referido continente, caso contrário, se a ação – seja ela qual for – concernente aos dados

[26] Texto original: ''*Profiling is defined by more than just the collection of personal data; it is the use of that data to evaluate certain aspects related to the individual. The purpose is to predict the individual's behaviour and take decisions regarding it. In the context of email marketing, it can be the choice to send a particular targeted email campaign instead of another one. Profiling can be defined by three specific elements: - It implies an automated form of processing; - It is carried out on personal data; and - The purpose of it is to evaluate certain personal aspects of a natural person to predict their behaviour and take decisions regarding it.''*

pessoais for de um cidadão europeu mas se dá fora da extensão europeia já não mais se aplica o GDPR (SOPRANA, 2018).

Em relação aos sujeitos e suas responsabilidades, cita-se (SOPRANA, 2018):

> O **processor data (processador de dados)** é a empresa ou organização que, claro, trata os dados. Ela responde ao controlador. Mas há responsabilidade solidária. Exemplo: uma cervejaria terceiriza o salário dos funcionários a uma empresa de pagamentos, que oferece o sistema de tecnologia e de armazenamento de dados dos trabalhadores. A cervejaria é o controlador e a terceirizada é o processador. Há situações em que uma entidade exerce as duas funções.
> **DPO é a sigla de Data Protection Officer**, um cargo dedicado a proteção de dados em casos de organizações, empresas ou entidades que tenham um grande fluxo de dados (mais de 5 mil registros de dados pessoais). É responsável por garantir a conformidade da empresa com a regulamentação. Pode ser uma pessoa, um escritório, alguém de dentro da organização e não precisa estar na UE. No entanto, deve trabalhar de forma independente.
> **DPIA é a sigla de Data Protection Impact Assessments**, uma avaliação de impacto no uso de dados pessoais que deve ser feita uma vez por ano. É uma função do DPO. Quando um tratamento utilizar novas tecnologias ou tiver uma natureza que possa resultar num risco elevado para direitos e liberdades de pessoas (como monitoramento de áreas públicas por drones ou de dados criminais), o responsável pelo tratamento precisa garantir um plano com medidas previstas para mitigar riscos, para assegurar a segurança, demonstrar a conformidade com a lei e levar em conta direitos e interesses legítimos das pessoas afetadas. Trata-se da elaboração e do preenchimento de questionários que envolvem diferentes setores da organização.

Além das multas incidirem sobre o uso indevido de dados pessoais, também recaem no caso de vazamentos de dados. Ainda, nesta última possibilidade a empresa ou organização deve notificar o incidente à Autoridade Europeia para a Proteção de Dados em até 72 horas, tal como todos os usuários lesados (SOPRANA, 2018).

No tocante às multas, determina (SOPRANA, 2018):

> As penas são de até € 20 milhões ou de 4% do faturamento global, o que for maior. No entanto, a Autoridade Europeia para a Proteção de Dados seguirá critérios de proporcionalidade, que envolvem diferentes categorias de danos e o histórico de cada organização.

Portanto, tem-se que o Regulamento 2016/679 da União Europeia (*General Data Protection Regulation* – GDPR) é um modelo de lei apropriado para se vislumbrar os direitos, os conceitos, e as direções para uma lei específica brasileira acerca da proteção dos dados pessoais. O Regulamento não só verte para a efetiva proteção dos dados pessoais, mas estabelece procedimentos claros e insere em seu conteúdo também soluções tecnológicas para tanto.

3.2 MARCO CIVIL DA INTERNET

A Lei nº 12.965/2014, mais conhecida como Marco Civil da Internet, se deu após consulta pública, na própria internet, em 2009. *''O projeto de lei passou pelo controle e revisão de diferentes setores da sociedade, entre empresas, organizações da sociedade civil, ativistas e comunidade técnica''* (SOUZA; LEMOS, 2016, p. 13).

Por tratar de assunto relativo a tecnologias, inovações e em que conceitos rapidamente se transformam, manteve em seu conteúdo *''o caráter principiológico para evitar uma caducidade precoce de seus dispositivos''* (SOUZA; LEMOS, 2016, p. 15 e 16).

Destaca-se que em sua tramitação – ainda como projeto de lei – apresentou caráter repressivo, se tratando de uma legislação criminal – que punia criminalmente diversas ações, como por exemplo, *''para quem transferisse músicas de um CD para outros dispositivos''* era previsto a pena de prisão de até quatro anos – porém, após diversas deliberações decidiu-se pela linha de marco regulatório civil (SOUZA; LEMOS, 2016, p. 17 a 19).

Na abertura da Conferência NetMundial – realizada no Brasil – foi sancionado o texto de lei pela então presidenta Dilma Roussef. *''A lei entrou em vigor em 23 de junho de 2014''* (SOUZA; LEMOS, 2016, p. 29).

Os autores, José Affonso Carlos e Ronaldo Lemos (2016, p. 30), que ajudaram na elaboração da referida lei – fizeram parte da execução da plataforma online para a realização da consulta pública – apontam que:

> Por ser uma lei principiológica, o Marco Civil não desceu (e nem deveria ter descido) em detalhes sobre a sua implementação. Essa é matéria típica para a regulamentação da lei, no caso para um decreto. O Decreto que por fim regulamentou o MCI foi editado em 2016, após a realização de quatro novas consultas sobre os seus termos: duas conduzidas pelo Ministério da Justiça, uma pelo Comitê Gestor da Internet e outra pela Anatel.

Ademais, observa-se que o Marco Civil da Internet versou acerca da responsabilidade civil dos provedores de conexão e dos provedores de aplicação, e da neutralidade da rede.

Em relação à neutralidade da net, destaca-se (SOUZA; LEMOS, 2016, p. 116 e 117).

> O Marco Civil da Internet definiu especificamente o que se entende por neutralidade da rede enquanto norma jurídica em nosso país. O ponto essencial da definição jurídica da neutralidade da rede (decorrente diretamente do objetivo de "manter a Internet aberta" - estrutura em ampulheta), é a **isonomia de tratamento entre os pacotes de dados**, que não podem ser discriminados injustificadamente, por exemplo, pelo operador da infraestrutura por onde trafegam, seja ele público ou privado. Sob essa perspectiva, a neutralidade da rede, tal como juridicamente definida no Brasil, aplica-se especificamente ao **tráfego** de dados sobre a rede.

Nesse sentido, após a breve explicação acerca do histórico da lei e o apontamento para a sua concepção mais principiólogica, discorrer-se-á acerca dos artigos que enfrentam

diretamente a problemática da proteção aos dados pessoais. Não se ocupará da responsabilidade civil dos provedores de conexão e dos provedores de aplicação, uma vez que não compete ao tema em estudo.

O Marco Civil preconiza alguns princípios em relação ao uso da internet no Brasil em seu art. 3º, que assim dispõe:

> 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;
> **II - proteção da privacidade;**
> **III - proteção dos dados pessoais, na forma da lei;**
> IV - preservação e garantia da neutralidade de rede;
> 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;
> VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
> VII - preservação da natureza participativa da rede;
> VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.
> 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. (grifo nosso).

Como se observa do texto da lei, *''o Marco Civil decidiu separar a privacidade de proteção dos dados pessoais''*, apesar da estrita ligação que têm. Tal cisão pode até ser interpretada com não constitucional (GONÇALVES, 2017, p. 32).

A referida lei, em seu art. 7º, apresenta os direitos dos usuários, que assim proclama:

> Art. 7o O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> **I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;**
> **II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;**
> **III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;**
> IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
> V - manutenção da qualidade contratada da conexão à internet;
> VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
> **VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;**
> **VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:**
> **a) justifiquem sua coleta;**
> **b) não sejam vedadas pela legislação; e**

> **c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;**
> **IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;**
> **X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;**
> XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
> XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
> XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet. (grifo nosso).

Da leitura dos incisos, ‘*’apesar da preferência do legislador pela defesa do usuário’’,* há a falta de transparência dos procedimentos das guardas dos dados pessoais pelas empresas de aplicação à internet, e o Marco Civil também não os estabelecem. Nesse seara, ‘*’não para se garantir direitos sem existirem regras claras e definidas sobre como funcionam os sistemas e tecnologias de informação e comunicação’’* (GONÇALVES, 2017, p. 59).

Outras críticas perspicazes ao artigo são (MORAIS; NETO, 2014, p. 428):

> [...] primeiro, a forma reducionista como vem sendo tratada a questão da privacidade, apenas como sinônimo de vida particular, ou seja, de intromissão nas comunicações privadas armazenadas (vide inciso III); segundo, os problemas oriundos da modernidade líquida não são resolvidos a partir de soluções dependentes da territorialidade, como é o caso do marco civil.

Indica-se, ainda, que o inciso VIII tem se que as finalidades apontadas – a, b, c – devem ser lidas como requisitos *‘’cumulativos e não alternativos’’,* a fim de assegurar ao máximo a proteção ao usuário (GONÇALVES, 2017, p. 72).

Em relação ao inciso X, se levanta a questão de como será feita a fiscalização para averiguar a prática recomendada pela lei nas empresas de aplicação de internet, afinal não há nenhum regulamento mais específico (GONÇALVES, 2017, p. 74).

O art. 8º da mencionada lei confere a possibilidade de anulação de cláusulas contratuais que violem os direitos de privacidade e liberdade de expressão nas comunicações, e assim dispõe:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
>
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

Nesse sentido, destacam-se as questões levantadas – e ainda não aclaradas – pelo advogado Victor Hugo Pereira Gonçalves (2017, p. 84), em que menciona que no referido artigo há problemas para a *''verificação técnico-jurídica''* da nulidade, já que o usuário não tem acesso aos mecanismos utilizados pelos aplicadores de internet e nem se há definido quem *''regulará as conformidades das cláusulas''*.

O art. 10 da Lei 12.965/2014 assim estabelece:

> 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.
>
> § 1o O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7o.
> § 2o O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7o.
> § 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.
> § 4o As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

A necessidade de cautela na guarda e manuseio dos dados de registros dos usuários decorre porquanto *''não é somente importante protegê-los formalmente, mas sim materialmente''* e sem os *''procedimentos de segurança não há segurança jurídica''* (GONÇALVES, 2017, p. 102).

O art. 11 da lei mencionada alhures, assim determina:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
>
> § 1o O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2o O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
> § 3o Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento

> da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
> § 4o Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Observa-se que o artigo acima reitera os preceitos do art. 7º da mesma lei (GONÇALVES, 2017, p. 113).

O art. 12 estabelece algumas sanções para serem aplicadas pelas autoridades judiciais ou extrajudiciais, a fim do cumprimento dos arts. 10 e 11, quais sejam: advertência, multa, suspensão temporária ou proibição das atividades empresariais (GONÇALVES, 2017, p. 118). Ademais, as referidas penalidades podem ser aplicadas de forma cumulativas ou isoladas, e não excluem a aplicação das sanções cíveis, criminais e administrativas (KUJAWSKI; THOMAZ, 2014, p.693).

Em complemento ao disposto nos artigos referentes à coleta de dados pessoais, ressalta-se que o Código do Consumidor aborda de maneira geral o tema em seu art. 43, caput, e pode assim, ser utilizado de forma complementar ao Marco Civil para as situações cabíveis, no âmbito da internet (KUJAWSKI; THOMAZ, 2014, p.689 e 690).

Nesse sentido, dispõe o art. 43 do CDC:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.

Lembra-se aqui, que os arts. 14 e 16 do Marco Civil já foram discutidos no capítulo dois. E nessa seara, somente se acrescenta (GODINHO; ROBERTO, 2014, p.740 e 741):

> O que cumpre questionar, todavia, é se o louvável propósito de se preservar a privacidade dos usuários da internet efetivamente terá sua devida eficácia, mormente diante da possibilidade de haver fraudes no manejo de dados de acesso dos usuários. Por mais que o texto legal tenha adequadamente estabelecido normas proibitivas acerca da cessão (seja gratuita ou onerosa) dos registros de conexão - e mesmo dos registros de acesso de aplicações de internet - armazenados pelos mais diversos tipos de provedores de internet, ainda é nebulosa a questão sobre o controle a ser eventualmente exercido sobre estas informações sigilosas, bem como acerca da fiscalização sobre seu destino, por não existir no Brasil uma Lei de Tratamento de Dados, que poderia ter sido elaborada e posta em vigor antes mesmo da aprovação do Marco Civil.

Em relação ao art. 23 do Marco Civil, que determina o sigilo das informações em juízo, tem se condizentes com os princípios expostos no decorrer da lei, uma vez que *‘’evitando-se a exposição indevida tanto do lesado, porventura ofendido em rede, e do ofensor, cujos dados permanecerão adstritos apenas ao uso para fins de instrução processual"* (GODINHO; ROBERTO, 2014, p. 745).

Em complemento, o Habeas Data, previsto no art. 5º, LXXII, da Constituição Federal e a Lei 9.507/1997 que o regulamenta, é utilizado para assegurar a proteção à privacidade, quando se trata de dados ou informações de caráter público, apesar de não mencionado no Marco Civil da Internet (GUERRA, 2014, p.410).

Nessa toada, cabe esclarecer novamente que nesse tópico foram discutidos somente os artigos da mencionada lei que pertinentes e relevantes de maneira direta ao assunto abordado nesse trabalho.

Assim, cita-se (MENEGUETTI; GIACCHETTA, 2014, p. 390):

> Ainda que o Marco Civil da Internet contenha alguns dispositivos e princípios esparsos e genéticos relacionados ao tema, a inexistência de um diploma legal especifico sobre a proteção de dados pessoais, é, frequentemente, um empecilho à efetividade do principio constitucional da intimidade e da vida privada (artigo 5º, inciso X, da Constituição Federal), assim como para a correta e clara delimitação das atividades e ações que são permitidas, desde que consentidas pelos usuários.

Dessa forma, temos que o Marco Civil traz em seu escopo algumas diretrizes e princípios relativos à proteção de dados, porém, não o regulariza da forma necessária. Há ainda – muitas – lacunas vazias, e para uma efetiva proteção estas devem ser preenchidas.

3.3 PROJETOS DE LEI NO BRASIL

Neste capítulo já se discorreu acerca do Regulamento 2016/679 da União Europeia – suas orientações e como serve de modelo para uma legislação efetiva na proteção dos dados pessoais – e, bem como, acerca do Marco Civil da Internet no Brasil – que apesar de declarar alguns direitos e instruir algumas direções acerca da proteção de dados pessoais, não tem em seu escopo tal objetivo, e, em verdade, ressalta mais ainda a necessidade de uma lei específica.

Com a crescente preocupação mundial acerca da circulação de dados pessoais, os escândalos envolvendo o Facebook e o Google, e até a venda de dados pessoais por órgãos públicos brasileiros, além da entrada em vigor da Lei Geral de Proteção dos Dados Pessoais Europeia, voltaram-se as pautas brasileiras para o já declarado tema.

Nessa toada, observou-se movimento no Senado Federal e na Câmara dos Deputados, os quais reavivaram projetos de lei referentes à proteção dos dados pessoais.

Nesse sentido, importa contextualizar a situação dos projetos de lei, qual seja (MANGETH; NUNES, 2018):

> Inicialmente, tramitavam três projetos de lei para a proteção geral de dados pessoais: o PL n° 330/2013, criado no Senado Federal, e os PLs n° 4.060/2012 e n° 5.276/2016, criados pela Câmara dos Deputados. Na semana passada, a Câmara

> finalmente votou e aprovou o PL n° 4.060, incorporando também a redação do PL n° 5.276/2016. E em regime de urgência regimental! Agora cabia ao Senado aprovar o PL. Mas…
>
> O PLS n° 330/2013, do Senado, permaneceu na Comissão de Assuntos Econômicos (CAE), ao invés de ser remetido à Câmara para votação. Com dois projetos versando sobre o mesmo tema no Senado, houve a saída de pauta do PLS n° 330/2013, que foi apensado ao PL n° 4.060/2012. Ambos se tornaram o PLC n° 53/2018, o que fez com que as iniciativas perdessem o regime de urgência regimental e voltassem para tramitação ordinária.
>
> Portanto, agora temos apenas o PLC n° 53/2018 (antigo PL n° 5.276/2016, apensado ao PL n° 4.060/2012 e, por fim, apensado ao PLS n° 330/2013), aguardando nova aprovação no Senado para, então, ser apreciado pelo Presidente da República.

Contudo, para fins didáticos antes de explicitar cada projeto de lei, um por um, convém assimilar as Recomendações Gerais aos Projetos de Lei, publicado pela ARTIGO19[27] – organização não-governamental inglesa de direitos humanos – disponível em seu relatório Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional [28].

Portanto (BANISAR; GUILLEMIN; BLANCO, 2017):

> 1. O projeto de lei deve estipular a criação de um órgão regulatório independente, inclusive do ponto de vista orçamentário. As funções do órgão em relação à proteção de dados pessoais devem ser a de fiscalizar e regular a implementação da lei e das práticas adotadas por responsáveis pelo tratamento de dados, para que os titulares não fiquem com o ônus da iniciativa, assim como diminuir o tempo necessário para a plena implementação da lei a partir das ações do órgão. Além disso, a ARTIGO 19 defende que esse órgão não se limite à proteção de dados, mas se destine também à regulação de temas mais amplos, relacionados à sociedade da informação como um todo.
>
> 2. A menção expressa à Lei nº 12527/2011, conhecida como Lei de Acesso à Informação (LAI)é necessária, pois o direito de acesso à informação eventualmente pode conflitar com o direito à proteção de dados pessoais em algumas situações específicas. Os projetos de lei não podem criar obstáculos aos avanços obtidos com a LAI e devem conter dispositivos que assegurem o acesso a dados pessoais quando o interesse público for maior que a necessidade de sigilo, como a divulgação de salários de servidores públicos, por exemplo.
>
> 3. Interpretações que possibilitem que o "direito ao esquecimento" possa ser reivindicado para o cancelamento dos dados pessoais devem ser evitadas. O direito ao esquecimento não deve ser alvo do texto de uma lei geral de proteção de dados pessoais, pois se trata de um tema diverso ao objeto da lei e que ainda necessita de um debate maior na sociedade. Dessa forma, os projetos de lei não devem permitir a solicitação de exclusão de informações que sejam de comprovado interesse público. Para isso, é necessário que eles tragam em seu texto uma ressalva explícita sobre a questão do interesse público quando se tratar do cancelamento dos dados pessoais.

[27] Para maiores informações acerca da organização, recomenda-se o link disponível em: http://artigo19.org/a-organizacao/

[28] Relatório disponível no link: http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf

> 4. Uma lei geral de proteção de dados pessoais deve se aplicar ao setor público como um todo, inclusive às forças de segurança. É importante que forças de segurança não sejam excluídas do escopo da lei, pois é notório que nos últimos anos têm crescido os programas de vigilância implantados por
> polícias estaduais, forças armadas e outros órgãos desta área, o que requer protocolos e garantias de proteção aos cidadãos que involuntariamente têm seus dados tratados.
>
> 5. Os projetos de lei devem especificar e delimitar o que se entende por pesquisa estatística, tendo em vista que essa atividade está prevista nos três projetos e não necessitaria do consentimento dos titulares dos dados para sua realização. Uma pesquisa estatística pode abarcar um número grande de tipos de pesquisa, feitas pelos mais diversos atores com variadas finalidades. Por essa razão, os projetos de lei, quando especificarem a exceção às pesquisas estatísticas, também devem oferecer uma delimitação dos tipos de atores e finalidades para que uma pesquisa seja considerada estatística.

Nesse mesmo sentido – apesar de poucas dissonâncias – posiciona-se o Anteprojeto de lei de proteção aos dados pessoas/Contribuição do ITS para o debate público, elaborado pelo ITSRio[29].

De maneira geral os diagnósticos obtidos para de uma regulamentação dos dados pessoais brasileira também apontam para: a) a aplicação material deve prever operações totais ou parcialmente automatizadas – não importando o local da sede do responsável ou operador –; b) em relação ao âmbito territorial, que a abrangência deve ser a mesma adotada pelo GDPR; c) em relação aos dados anônimos, que para a incidência ou não de lei se considere a ‘*’finalidade do tratamento de tal dado e os mecanismos utilizados para dificultar essa identificação’’*; d) que a autoridade fiscalizadora – no texto original utiliza-se a denominação ‘*’agência reguladora’’* – seja independente financeira e administrativamente, além de integrar outras competências, como os assuntos relativos à Lei de Acesso à Informação; e) em relação ao conceito de dados irrestritos – geralmente utilizados pelo poder público – apesar de seu caráter ilimitado, ainda assim, à luz do principio da finalidade, não deverão ser tratados com finalidade distinta da qual foi primeiramente tratado; f) que a lei não se concentre tanto na legitimação acerca do consentimento – uma vez que em certas situações online é inviável –, mas sim viabilize efetivamente maneiras de se garantir os direitos dos titulares dos dados pessoais; g) que seja previsto a hipótese de ‘*’tratamento de dados necessário ao atendimento dos interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados’’* (ITSRIO, 2015).

Ultrapassada essas ponderações iniciais, passar-se-á a analisar cada projeto de lei. Nesse sentido, convém aclarar que as informações aqui expostas tem por base o relatório

[29] Relatório disponível no link: https://itsrio.org/wp-content/uploads/2015/07/Consulta-APL-de-Dados.pdf

elaborado pelo ARTIGO19 mencionado alhures. Além de, ser fundamental mencionar os critérios levados em conta para as análises procedidas.

Portanto, os critérios abordados são[30]: 1) menção expressa à proteção da liberdade de expressão; 2) exceção à atividade jornalística e outras formas de expressão; 3) menção expressa à Lei de Acesso à Informação; 4) Cuidado com intepretações que possibilitem reinvindicações do direito ao esquecimento; 5) Órgão regulatório; 6) Mecanismo de participação e controle social; 7) Proteção aos dados sensíveis; 8) Graus de consentimento; 9) Consentimento do titular para compartilhamento a terceiros; 10) Proteção para transferência internacional de dados; 11) Proteção de dados em acesso público; 12) Adoção de medidas de segurança e de manuseio dos dados pessoais; 13) Aplicação ao setor público como um todo, incluindo forcas de segurança; 14) Delimitação de pesquisa estatística; e 15) Prazo para a lei entrar em vigor (BANISAR; GUILLEMIN; BLANCO, 2017, p. 17 a 24).

Para se ‘’quantificar’’ o cumprimento ou não dos requisitos aludidos acima foi estabelecido a seguinte classificação (BANISAR; GUILLEMIN; BLANCO, 2017, p. 17):

> SATISFATÓRIO
> O projeto de lei aborda o tópico de maneira adequada.
>
> PARCIALMENTE SATISFATÓRIO
> O projeto de lei aborda o tópico de maneira incompleta.
>
> AUSENTE
> O projeto de lei não aborda o tópico.
>
> INSATISFATÓRIO
> O projeto de lei aborda o tópico de maneira inadequada.

Dessa forma, exauridos os apontamentos necessários, é possível proceder a análise dos projetos de lei de forma singular.

3.3.1 Projeto de Lei n. 5276/2016

O Projeto de Lei n. 5276/2016, originado na Câmara dos Deputados, foi o que teve a maior participação social. O Ministério da Justiça, através de reuniões e consultas públicas, averiguou as posições de *‘’empresas, organizações da sociedade civil e representantes do poder público’’,* a fim de elaborar um projeto de lei completo. O texto foi disposto na

[30] Para um maior aprofundamento acerca dos critérios recomenda-se a leitura das páginas 17 a 24 do documento disponível em: http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Prote%C3%A7%C3%A3o-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf

plataforma online e-democracia para sua consulta pública, e recebeu mais de ‘’50 mil visitas e mais de 1.100 contribuições’’(BANISAR; GUILLEMIN; BLANCO, 2017, p. 25).

Relativamente acerca dos **aspectos satisfatoriamente preenchidos**, percebe-se que o PL em seu art. 2º, *‘’inciso II, insere as liberdades de expressão, de comunicação e de opinião como fundamentos da proteção de dados pessoais’’*, fazendo o correto balanço entre a proteção aos dados pessoais e o direito à liberdade de expressão e ao *‘’interesse público no acesso à informação’’*(BANISAR; GUILLEMIN; BLANCO, 2017, p. 26).

Já em seu art. 4º, inciso II, é conferido explicitamente exceção da aplicação da lei às *‘’atividades exclusivamente jornalísticas, artísticas, literárias ou acadêmicas’’*. Essa isenção é necessária, uma vez que as referidas atividades não visam um fim meramente econômico, mas, por vezes, *‘’podem ter uma função social de denúncia ou, ainda, de acúmulo de conhecimento’’*, ou ainda tratarem de liberdade de expressão de seus autores (BANISAR; GUILLEMIN; BLANCO, 2017, p. 26).

Nessa toada, complementa-se (BANISAR; GUILLEMIN; BLANCO, 2017, p. 26):

> Nesse ponto, seria bom esclarecer que a atividade deve ser exclusivamente para esses fins, não podendo ter impactos econômicos ou políticos. O projeto de lei, no parágrafo 3 do artigo 4, ainda confere ao órgão competente a função de emitir opiniões técnicas ou recomendações referentes às exceções previstas a essas atividades, o que visa evitar possíveis abusos e mau usos.

Verifica-se a menção expressa da Lei de Acesso à Informação, em seu art. 23, em seu art. 26, §1º, e no art. 44, §1º, todos em conformidade às diretivas da LAI (BANISAR; GUILLEMIN; BLANCO, 2017, p. 26).

O PL concede atenção especial aos dados sensíveis, exigindo o consentimento *‘’livre, inequívoco, informado, expresso e específico’’* para o seu tratamento. Ainda possibilita ao órgão competente a alternativa de estabelecer *‘’medidas adicionais de segurança e de proteção aos dados sensíveis’’* (BANISAR; GUILLEMIN; BLANCO, 2017, p. 27).

Para melhor exteriorizar a abordagem dos graus de consentimento no PL, menciona-se (BANISAR; GUILLEMIN; BLANCO, 2017, p. 27):

> O capítulo I, que aborda os requisitos para o tratamento de dados pessoais, dá ampla importância para o tipo de consentimento do titular sobre seus dados. O artigo 7 define que o processo só poderá ser realizado mediante um consentimento livre, informado e inequívoco. Tais qualificações reforçam os modos de permissão necessários.
>
> O parágrafo 1 do artigo 7 estipula que mesmo sendo permitido o tratamento de dados pela administração pública para o cumprimento de obrigações legais ou por conta da necessidade para execução de políticas públicas, esse tratamento deve ser informado ao titular. Sobre o mesmo ponto, o parágrafo 2 ainda exprime que a autoridade competente pode regular essa ação, estabelecendo diretrizes que protejam

> o titular. O artigo 8 dispõe que o acesso às informações do tratamento de dados deve ser facilitado e deve incluir pontos como:
> . a finalidade específica do tratamento
> . a forma e a duração do tratamento
> . a identificação do responsável
>
> Esses direitos garantem a transparência do processo de tratamento que poderá ser avaliado e supervisionado, além do órgão competente, pelos próprios titulares.
> No artigo 8, inciso VII, são descritos os direitos que o titular dos dados têm sobre o tratamento. Fica assegurado que ele pode:
> . acessar, retificar ou revogar seu consentimento para o tratamento de seus dados
> . denunciar possíveis atos em desacordo com essa lei
> . não oferecer o consentimento mediante o fornecimento de informações sobre as consequências da negativa
>
> O parágrafo 3 do mesmo artigo determina que em casos de coleta de dados continuada, o responsável pela operação deve informar periodicamente sobre a principais características do tratamento — prática conhecida como "consentimento granular" —, ou seja, deve haver prestação de contas em serviços duradouros, o que permite o acompanhamento regular e perene do titular sobre os seus dados.

Outro aspecto contemplado pelo PL é o consentimento do titular para compartilhar a terceiros, com exceção para manuseio pelo poder público quando for caso ‘*’finalidades específicas de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas’’*, conforme os arts. 40, 26 e 26, §1º (BANISAR; GUILLEMIN; BLANCO, 2017, p. 28).

Acerca da proteção conferida nas transferências internacionais, vislumbra-se que (BANISAR; GUILLEMIN; BLANCO, 2017, p. 28):

> Os artigos 33, 34 e 35 tratam da transferência internacional de dados. Atualmente, com a internet, grande parte do tratamento de dados pessoais de cidadãos de determinado país é realizada em um país estrangeiro. O artigo 33 prevê que essa transferência se dará somente junto a países que possuam um nível de proteção de dados semelhante, apresentando cinco critérios específicos de como será feita a comparação; quando o órgão competente autorizar a operação; e quando o titular tiver fornecido seu consentimento, com informação prévia e específica sobre o caráter internacional da operação. O artigo 35 ainda garante que tanto o responsável pelo tratamento quanto o operador respondam pelo tratamento de dados, independentemente de onde a operação se realize.

As adoções de medidas de segurança e de manuseio dos dados pessoais estão bem especificas em seu art. 6º, inciso VII, o qual preconiza que *"devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão"*. Também há previsão para a eliminação dos dados após o término do tratamento. E em relação ao manuseio dos dados pessoais pelo poder público estipula-se a elaboração de relatórios de impacto à privacidade referente às suas operações (BANISAR; GUILLEMIN; BLANCO, 2017, p. 28).

Em complemento (BANISAR; GUILLEMIN; BLANCO, 2017, p. 28 e 29):

> No artigo 40, fica expresso que a comunicação de dados pessoais entre responsáveis e operadores de direito privado dependerá do consentimento do titular tendo como ressalvas as hipóteses previstas em lei. No artigo 41, é designada a figura do encarregado. Já o capítulo VII inicia-se com o artigo 45, que determina que "o operador deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração de comunicação ou qualquer forma de tratamento inadequado ou ilícito."
> O artigo 46 complementa o anterior e estipula a obrigatoriedade de sigilo também aos responsáveis pelo tratamento de dados, mesmo após o fim do período da operação.

Agora, parte-se para a análise dos **aspectos parcialmente satisfatórios**, quais sejam: órgão regulatório, mecanismo de participação e controle social, proteção de dados em acesso público, delimitação de pesquisa estatística e prazo para a lei entrar em vigor (BANISAR; GUILLEMIN; BLANCO, 2017, p. 29 e 30).

Acerca do órgão regulatório, sua incompletude está na não criação do mesmo, apesar de mencioná-lo. Ademais, também se verifica que outras particularidades do órgão já poderiam estar dispostas, quais sejam: a criação também de um conselho nacional de proteção de dados pessoais, a eleição de seus membros, a ampliação de sua atuação – abrangendo ‘’todas as problemáticas relativas à constituição da sociedade da informação’’ –, e a independência orçamentária (BANISAR; GUILLEMIN; BLANCO, 2017, p. 29).

Apesar da referencia na lei a mecanismos de participação e controle social, o faz de forma tímida, e não estipula de fato os referidos mecanismos (BANISAR; GUILLEMIN; BLANCO, 2017, p. 29).

Relativamente a proteção de dados em acesso público, aponta-se que (BANISAR; GUILLEMIN; BLANCO, 2017, p. 29 e 30).

> O artigo 7, parágrafo 4º, supõe que o mesmo tratamento concedido aos dados em domínio priva- do deve ocorrer com dados tornados públicos. Ou seja, não há um relaxamento das normas por conta da origem dos dados pessoais, o que é um ponto positivo. Por outro lado, ao impor o mesmo processo para o tratamento de dados em acesso público, admite hipóteses nas quais o consentimento do titular não seja requerido no tratamento desses dados, como para o uso de forças de segurança e inteligência, que já praticam esse tipo de tratamento de dados em acesso público há algum tempo.

As deficiências encontradas acerca da delimitação de pesquisas estatísticas são: a não definição de ‘’pesquisas estatísticas’’, a não precisão de quais os sujeitos permitidos a realizarem tal pesquisa, e a falta de delimitação de quais finalidades se enquadrariam nesse contexto. Nesse sentido, esclarece-se que em seu art. 7, inciso IV, permite-se a realização de *‘’pesquisas estatísticas independentemente do consentimento dos titulares, impondo a*

condição de que sempre que possível os dados devem estar sob anonimato'' (BANISAR; GUILLEMIN; BLANCO, 2017, p. 30).

Pela urgência do assunto, confere-se a necessidade da entrada em vigor assim que publicada, o que não se observa nesse PL, tratando-se, porém, do projeto de lei com o maior lapso *''entre a publicação e sua entrada em vigor''*(BANISAR; GUILLEMIN; BLANCO, 2017, p. 30).

Por fim, entra-se na seara dos **aspectos insatisfatórios do projeto de lei**. Percebe-se que o PL aborda os requisitos de 1) evitar interpretações que possam ensejar reivindicações do direito ao esquecimento e 2) aplicação ao setor público como um todo, incluindo forças de segurança de forma inadequada.

A um, porquanto não prevê exceções nos casos de pedidos de retirada, exclusão ou alteração em situações que lidam com *''informações de utilidade pública e devem ser de acesso público'',* a fim de evitar abusos por autoridades ou pessoas públicas (BANISAR; GUILLEMIN; BLANCO, 2017, p. 30 e 31).

E a dois, pois (BANISAR; GUILLEMIN; BLANCO, 2017, p. 31):

> O artigo 4, inciso III, exclui da aplicação da lei o tratamento de dados pessoais "realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais."

Ante o exposto, tem-se que o referido PL observa em seu texto as principais diretivas e princípios internacionais acerca do tema. E ainda, contou com efetiva participação pública brasileira. De todos os projetos de lei se mostrou o mais satisfatório. (BANISAR; GUILLEMIN; BLANCO, 2017, p. 25).

3.3.2 Projeto de Lei de iniciativa do Senado n. 330/2013

O Projeto de Lei n. 330/2013, originado no Senado, tem seus alicerces muito similares ao do PL 5276/2016 (BANISAR; GUILLEMIN; BLANCO, 2017, p. 32). Nesse sentido, projeta-se a explicação de sua ementa[31]:

> Regula a proteção, o tratamento e o uso de dados das pessoas naturais e jurídicas de direito público ou privado. Define, para os efeitos da Lei: dado pessoal; banco de dados; tratamento de dados pessoais; gestor de banco de dados; gestor aparente; proprietário do banco de dados; titular de dados pessoais; usuário de banco de dados; dados sensíveis; interconexão de dados e dissociação. Dispõe sobre os princípios que se aplicam ao tratamento de dados pessoais. Define os casos em que os dados considerados sensíveis poderão ser coletados, armazenados, processados, transmitidos, utilizados, fornecidos a usuários ou divulgados. Estabelece que o

[31] Disponível no link: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947

> tratamento de dados pessoais para fins de segurança pública, investigação criminal ou instrução penal, administrativa ou tributária somente poderá ser feito por órgão da administração publica direta ou pessoa jurídica de direito público, limitando-se às seguintes hipóteses: a) exercício de competência prevista em lei; b) prevenção ou repressão de infração penal, administrativa ou tributária; c) compartilhamento de informações para fins de segurança do Estado e da sociedade; e d) atendimento dos termos de acordo, tratado ou convenção internacional de que o Estado brasileiro seja parte. Dispõe sobre os Direitos Básicos do Titular de Dados. Dispõe sobre os deveres do proprietário e do gestor de banco de dados, no tratamento de dados pessoais. Define as disposições especiais aplicáveis aos Bancos de Dados Públicos e aos Bancos de Dados Privados. Dispõe sobre: a segurança de dados, a interconexão de dados, da retificação e do cancelamento de dados. Dispõe sobre a Responsabilidade Civil; estabelece que qualquer pessoa que sofra prejuízo decorrente do tratamento irregular ou ilícito de dados possui direito à reparação dos danos, materiais e morais; dispõe que a responsabilidade do proprietário, do usuário, do gestor e do gestor aparente de banco de dados, quando houver, independe da verificação de culpa; define que o tratamento de dados realizado de forma associativa ou por qualquer outra forma, ainda que informal, acarreta a responsabilidade solidária e direta de todos os agentes envolvidos. Estabelece que as infrações às normas de proteção de dados pessoais ficam sujeitas às seguintes sanções administrativas, sem prejuízo das de natureza civil, penal e das definidas em normas específicas: a) multa; b) suspensão temporária de atividade; c) intervenção administrativa; e d) interdição, total ou parcial, da atividade exercida pelo proprietário ou gestor de banco de dados; dispõe que as sanções serão aplicadas pelas autoridades administrativas federal, estadual, do Distrito Federal ou municipal, no âmbito de suas atribuições, conforme disciplinadas em normas regulamentares. Estabelece que as penas serão aplicadas pela administração pública, mediante processo administrativo em que se assegure a ampla defesa. Dispõe que a produção, manuseio, consulta, transmissão, tratamento, manutenção e guarda de dados ou informações sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da administração pública federal, permanecerão regidos pela Lei nº 8.159, de 8 de janeiro de 1991, e pelo Decreto nº 4.553, de 27 de dezembro de 2002.

Conforme procedido no subtópico anterior, também se fará a análise do PLS n. 330/2013, sob o viés dos critérios apresentados no relatório elaborado pelo ARTIGO19.

Dessa forma, em relação aos **aspectos satisfatoriamente preenchidos**, observa-se preenchido os critérios para a proteção especial concedida aos dados sensíveis. O PLS em seu art. 15 proíbe o tratamento de dados pessoais sensíveis, e constitui sete razoáveis exceções (BANISAR; GUILLEMIN; BLANCO, 2017, p. 33).

Entretanto (BANISAR; GUILLEMIN; BLANCO, 2017, p. 33):

> Na quinta exceção, é necessária a delimitação das atividades consideradas como pesquisa jornalística, histórica ou científica, impossibilitando que práticas comerciais ou com outros fins não sejam enquadradas nessa exceção. Já na sexta exceção, é fundamental atenção e fiscalização sobre as atividades das pessoas jurídicas de direito público, já que o termo "atividades específicas" podem abarcar diversas ações e uma "decisão motivada" deve ser alvo de avaliação do órgão competente.

Quanto ao diferentes graus de consentimento, percebe-se que se dá da maneira devida, visto que aumenta seu grau em se tratando de dados sensíveis e porquanto seu art. 13 ‘*’define que o consentimento prestado de forma apartada do restante das declarações deve*

apontar uma finalidade legítima, específica e delimitada'' (BANISAR; GUILLEMIN; BLANCO, 2017, p. 33).

Já a previsão de consentimento do titular para compartilhamento a terceiros é prevista em seus arts. 13 e 20, e estabelece ainda que o ‘*'titular deve ter acesso a todas as informações relativas ao tratamento antes de dar sua autorização''* e que tal consentimento ‘*'deve ser específico e próprio do titular, ou por conta das exceções previstas nos incisos III a VI do artigo 12''* do PLS (BANISAR; GUILLEMIN; BLANCO, 2017, p. 34).

Posto que só poderá ser feito a transferência internacional de dados quando o titular obtiver informações de todos os aspectos da atividade, e consentir de forma especifica e própria, além da necessidade de o país que receber oferecer o mesmo grau de proteção de dados, tem-se satisfeito esse requisito (BANISAR; GUILLEMIN; BLANCO, 2017, p. 34).

Por estipular medidas sólidas para promover a segurança técnica e de manuseio durante o período de tratamento dos dados pessoais, como: impedir em certos casos o acesso não autorizado “aos equipamentos, instalações e suportes de tratamento de dados”, determinar a guarda dos dados sensíveis coletados em sigilo e previsão de multa no seu descumprimento, bem como impor a comunicação de incidentes de segurança ao órgão competente, tem-se, de igual modo, cumprido satisfatoriamente o critério (BANISAR; GUILLEMIN; BLANCO, 2017, p. 35).

Continuamente, aborda-se neste momento os **aspectos parcialmente satisfatórios ou ausentes no projeto de lei.** Nessa toada, verifica-se completamente ausente do corpo de texto do PL a menção expressa à proteção da liberdade de expressão, à Lei de Acesso à Informação e à proteção de dados em acesso público (BANISAR; GUILLEMIN; BLANCO, 2017, p. 35, 36 e 37).

Ainda, em relação à exceção à atividade jornalística e outras formas de expressão, observa-se que só faz jus no que concerne a atividade jornalística, não constando as atividades artísticas, literárias e acadêmicas de igual modo como não necessárias de consentimento (BANISAR; GUILLEMIN; BLANCO, 2017, p. 36).

Já quanto ao órgão regulatório sua redação é paradoxal porquanto designa ao poder público as competências referentes aos cuidados com os dados pessoais, e ao mesmo tempo, estabelece que *''será designado um órgão capaz de aprovar normas para lidar com o tema''* (BANISAR; GUILLEMIN; BLANCO, 2017, p. 36).

Acerca dos mecanismos de participação e controle social, depreende-se que (BANISAR; GUILLEMIN; BLANCO, 2017, p. 36):

> O PLS 330/2013 prevê a criação de mecanismos de participação do titular em um programa de governança em privacidade criado pelo responsável do tratamento em seu artigo 29, em especial no inciso I (e). Essa foi a maneira encontrada pelo legislador para fazer valer o principio estabelecido no inciso X, do artigo 4, sendo ele: "responsabilização e prestação de contas pelos agentes que tratam dados pessoais, de modo a demonstrar a observância e o cumprimento das normas de proteção de dados pessoais".

Também não se averiguou a delimitação do conceito de ''pesquisa estatística'' (BANISAR; GUILLEMIN; BLANCO, 2017, p. 37).

Conforme também apontado no subtópico anterior em relação ao PL 5276/2016, a necessidade da imediata vigência da lei impera (BANISAR; GUILLEMIN; BLANCO, 2017, p. 37).

Agora, abarcar-se-á os **aspectos insatisfatórios do projeto de lei**. Nessa toada, por estipular exceção da aplicação do PL aos bancos de dados mantidos pelo Estado para fins de defesa nacional e segurança publica, é, portanto, insatisfatório em relação ao quesito (BANISAR; GUILLEMIN; BLANCO, 2017, p. 38).

E, em relação às interpretações que possam ensejar reivindicações do direito ao esquecimento, tem-se insatisfatório visto que:

> O projeto de lei 330/2013 não faz referencia a situações nas quais o direito do titular de exclusão definitiva de dados pessoais —direito assegurado no artigo 6, inciso VII— entra em conflito com o direito de acesso a informação e ao de interesse publico, por exemplo. Uma lei de proteção de dados pessoais não pode dar margem a interpretações que permitam a institucionalização do direito ao esquecimento. Os artigos 8 e 9 da lei tratam dos casos nos quais podem ocorrer correção, bloqueio, cancelamento ou dissociação dos dados. Em nenhum momento se faz o contrapeso dessas ações com o interesse publico, o que e problemático, pois ha casos em que os dados pessoais publicitados tem efetivamente um grande interesse publico por trás, como em casos de denuncias de corrupção ou então de irregularidades em órgãos públicos.

Ante o exposto, o referido PL é o mediano entre os projetos de lei acerca do tema. Tem suas premissas similares ao do PL 5276/2016, e abarcar diversos aspectos necessários para a proteção de dados pessoais dos brasileiros.

3.3.3 Projeto de Lei n. 4.060/2012

O Projeto de Lei n. 4.060/2012, originado na Câmara dos Deputados, é o que menos corresponde aos critérios elaborados pelo ARRTIGO19, em vista do teor vago e por enfatizar mais os tratamentos concedidos aos dados pessoais que a sua própria proteção (BANISAR; GUILLEMIN; BLANCO, 2017, p. 39).

Nesse sentido, complementa-se que (BANISAR; GUILLEMIN; BLANCO, 2017, p. 39):

> A linguagem do texto do projeto não incorpora as discussões mais relevantes dos últimos anos sobre o tema e não assegura padrões mínimos de proteção aos titulares dos dados pessoais, em total desacordo com os padrões internacionais de direitos humanos.

O único **aspecto satisfatório do projeto de lei** é a exceção à atividade jornalística e outras formas de expressão, especificada em seu art. 6º (BANISAR; GUILLEMIN; BLANCO, 2017, p. 40).

Seguindo em frente, analisar-se-á os **aspectos parcialmente satisfatórios ou ausentes do projeto de lei.** Encontra-se ausente: menção expressa à proteção da liberdade de expressão, menção expressa à Lei de Acesso à Informação, mecanismo de participação e controle social, além de não estipular um ‘*’órgão competente para fiscalizar e implementar a proteção de dados pessoais’’* (BANISAR; GUILLEMIN; BLANCO, 2017, p. 40 e 41).

Em relação à proteção aos dados sensíveis observa-se que o cuidado devido não é concedido, porquanto discorre vagamente acerca do assunto (BANISAR; GUILLEMIN; BLANCO, 2017, p. 41).

A adoção de medidas de segurança e de manuseio dos dados pessoais não foi bem adequada, uma vez que (BANISAR; GUILLEMIN; BLANCO, 2017, p. 41):

> O texto não possui uma seção para lidar especificamente com o tema da segurança dos dados. A única disposição sobre o assunto está no artigo 11, no qual se estabelece que o responsável deve “adotar medidas tecnológicas aptas a reduzir ao máximo o risco da destruição, perda, acesso não autorizado ou de tratamento não permitido pelo titular.” O texto não prevê medidas específicas de proteção segurança dos dados, como fazem os outros dois projetos de lei. Não há menção sobre prevenção a acessos não autorizados, possibilidade de verificações periódicas dos dados tratados ou a garantia de que dados só serão acessados pelos usuários.

De igual forma ao apontado nos dois subtópicos anteriores a necessidade da imediata vigência da lei impera não foi contemplada (BANISAR; GUILLEMIN; BLANCO, 2017, p. 41).

Por último, minuciar-se-á os **aspectos insatisfatórios do projeto de lei**. nessa toada, verifica-se que o PL não evita interpretações que possam ensejar reivindicações do direito ao esquecimento, como é o caso do interesse público (BANISAR; GUILLEMIN; BLANCO, 2017, p. 42).

Outro elemento que lhe falta são os graus de consentimento, o PL sequer menciona o conceito de consentimento, e propõe princípios demasiadamente amplos e difusos, quais

sejam: boa-fé, lealdade e legítimos interesses (BANISAR; GUILLEMIN; BLANCO, 2017, p. 42).

Já concernente ao consentimento do titular para compartilhamento a terceiros, tem-se que (BANISAR; GUILLEMIN; BLANCO, 2017, p. 42):

> No artigo 14, permite-se aos responsáveis compartilhar os dados pessoais, inclusive para fins de comunicação comercial, com qualquer um que contribua direta ou indiretamente para a realização de tratamento de dados pessoais. Esse ponto é extremamente crítico. O que se autoriza a partir dessa disposição é, em seu extremo, a livre circulação de dados pessoais por uma rede enorme de empresas, órgão públicos ou qualquer um que tenha interesse em tratar dados pessoais, mediante a autorização e o consentimento do titular a um único responsável por tratamento de dados.

Não prevê proteção para transferência internacional de dados, em verdade, deixa-a à mercê para ser tratado da mesma forma que o *''compartilhamento realizado dentro das fronteiras brasileiras''* (BANISAR; GUILLEMIN; BLANCO, 2017, p. 42 e 43).

Em relação à proteção de dados em acesso público, percebe-se que o PL *''não se aplica a os dados que estejam em acesso público'*, bem como não estabelece o consentimento para a sua publicidade (BANISAR; GUILLEMIN; BLANCO, 2017, p. 43).

Também é insatisfatório na aplicação ao setor público como um todo, incluindo forças de segurança, uma vez que exclui os bancos de dados de investigação criminal ou inteligência da sua incidência (BANISAR; GUILLEMIN; BLANCO, 2017, p. 43).

E, finalmente, a delimitação de pesquisa estatística também não se apresenta no PL (BANISAR; GUILLEMIN; BLANCO, 2017, p. 43).

Ante o exposto, o PL n. 4.060/2012 é que menos concede proteção aos dados pessoais e aos seus titulares, além de estar em desacordo com as normais internacionais de direitos humanos (BANISAR; GUILLEMIN; BLANCO, 2017, p. 39).

Após exauridos os projetos de lei minuciosamente, tem-se que o Projeto de Lei n. 5276/2016 foi o que melhor supriu os aspectos necessários para a efetiva proteção de dados pessoais brasileira, em conformidade com o gráfico (Figura 3) apresentado no relatório Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional (BANISAR; GUILLEMIN; BLANCO, 2017, p. 23). Nesse sentido, esclarece-se que a cor verde representa aspecto satisfatório, a cor laranja é parcialmente satisfatório, a cor goiaba verifica-se o aspecto ausente, e a cor vermelha (mais escura) aspecto insatisfatório.

Figura 3: Tabela Comparativa

ASPECTOS DA LEI	PL 5276/2016	PLS 330/2013	PL 4060/2012
Menção expressa à proteção da liberdade de expressão	🟢	🔴	🟡
Exceção à atividade jornalística e outras formas de expressão	🟢	🟡	🟢
Menção expressa à Lei de Acesso à Informação (LAI)	🟢	🔴	🔴
Evita interpretações que possam ensejar reivindicações do direito ao esquecimento	🔴	🔴	🔴
Órgão regulatório	🟡	🟡	🔴
Mecanismo de participação e controle social	🟡	🟡	🔴
Proteção aos dados sensíveis	🟢	🟢	🟡
Graus de consentimento	🟢	🟢	🔴
Consentimento do titular para compartilhamento a terceiros	🟢	🟢	🔴
Proteção para transferência internacional de dados	🟢	🟢	🔴
Proteção de dados em acesso público	🟡	🔴	🔴
Adoção de medidas de segurança e de manuseio dos dados pessoais	🟢	🟢	🟡
Aplicação ao setor público como um todo, incluindo forças de segurança	🔴	🔴	🔴
Delimitação de pesquisa estatística	🔴	🔴	🔴
PRAZO PARA A LEI ENTRAR EM VIGOR	180 dias	120 dias	90 dias

Fonte: ARTIGO19, 2017.

3.3.4 Projeto de Lei n. 53/2018

O Projeto de Lei n. 53/2018, originado na Câmara dos Deputados. Conforme já exposto no início desse tópico, trata-se da junção do antigo PL n° 5.276/2016, apensado ao PL n° 4.060/2012 e, por fim, apensado ao PLS n° 330/2013 (MANGETH; NUNES, 2018).

Ressalva-se que o PL n. 53/2018 não se trata inteiramente do PL 5.276/2016, mas tem, em fato, basicamente a mesma estrutura da lei – diretrizes, princípios, artigos – com poucas mudanças.

Uma vez que já analisado a efetividade da proteção aos dados pessoais da PL 5.276/2016, não é necessário repetir as mesmas ponderações.

Entretanto, convém expor a situação em que se encontra o referido PL, já que diante das perspectivas, tem-se como a promessa de concretizar a lei geral de proteção aos dados pessoais no Brasil.

Em respostas as manifestações que foram contra a aprovação do texto da PL ainda na Câmara, feitas pela FEBRABAN - Federação Brasileira de Bancos e outras organizações, ‘*’organizações como a Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação (Brasscom) e a Coalizão Direitos na Rede’’* resolveram publicar manifestos multissetoriais solicitando a imediata aprovação do referido PL e seu texto, porquanto entendem que foi resultado de *‘’uma posição mediada entre todos os setores envolvidos, numa efetiva demonstração de que processos participativos e democráticos produzem legislações equilibradas’’* (LUCA, 2018).

Nessa seara, citam-se trechos do Manifesto da Coalizão Direitos na Rede – rede independente de organizações da sociedade civil, ativistas e acadêmicos em defesa da Internet livre e aberta no Brasil –, que assim dispõe[32]:

> A proposta é o resultado possível e maduro de diálogo e negociação intensa entre diversos interessados na consolidação de uma moderna lei geral de proteção de dados pessoais, adequada ao atual contexto tecnológico, compatível com futuros avanços e compromissada com direitos fundamentais. Hoje, o mundo todo repensa a relação entre inovações tecnológicas e riscos coletivos gigantescos. E o Brasil pode dar um passo certo na direção de mais segurança jurídica e de uma economia de dados centrada no respeito a direitos.
>
> Participaram da construção do que agora é o PLC 53/2018 organizações de defesa de direitos na Internet, da infância e do consumidor, Procons, empresas de telecomunicações, representantes de plataformas digitais e do setor comercial e financeiro, universidades, centros de pesquisa, bem como agentes do poder público: Executivo (incluindo órgãos de segurança), Legislativo e Judiciário.
>
> Desde 2010, foram duas consultas públicas realizadas pelo Ministério da Justiça, gerando um anteprojeto de lei. Enviado ao Congresso Nacional, foram realizadas onze audiências públicas e dois seminários de grande porte, promovidos pela Comissão Especial designada para analisar a matéria. Houve ainda debates em outros fóruns, como no encontro anual promovido pelo Comitê Gestor da Internet no Brasil, e em eventos organizados por empresas, acadêmicos e pelo terceiro setor.

Ainda, acerca da pressão dos interesses particulares no referido PL, o Manifesto também se pronuncia[33]:

> **Infelizmente, setores insatisfeitos com o texto aprovado na Câmara se mostram incapazes de aceitar o equilíbrio entre as diversas partes envolvidas, e querem assegurar apenas o atendimento aos seus interesses particulares. Pressionam o**

[32] Disponível no link: https://medium.com/direitos-na-rede/pela-imediata-aprovacao-do-plc53-18-e50072b37713
[33] Disponível no link: https://medium.com/direitos-na-rede/pela-imediata-aprovacao-do-plc53-18-e50072b37713

> **atual relator do PLC 53/2018, senador Ricardo Ferraço, para que flexibilize as normas previstas tanto para empresas quanto para o setor público. Esse tipo de postura ameaça o processo legislativo democrático, desconsiderando o intenso esforço de equacionar a multiplicidade de interesses em prol do avanço do país.**
>
> **De um lado, o setor financeiro e as seguradoras pretendem modificar previsões sobre legítimo interesse, compartilhamento entre empresas e tratamento dos chamados dados sensíveis (por exemplo, biometria). De outro, o próprio Governo Federal tenta manter o Estado fora da lei, desobrigando o poder público de cumprir os princípios e regras do que deveria ser uma lei geral para o Brasil. Representantes do Executivo têm afirmado que a Advocacia Geral da União pedirá o veto de parcela fundamental do texto aprovado na Câmara, caso o projeto vire lei. Entre os pontos questionados está a criação da Autoridade Nacional de Proteção de Dados.** (grifo nosso).

A Brasscom – Associação Brasileira das Empresas de Tecnologia da Informação e Comunicação também expos em seu Manifesto as mesmas opiniões, apesar de mais comedida (LUCA, 2018).

E, destacou que[34]:

> **O Senado tem oportunidade** ímpar de conferir **protagonismo ao Brasil,** em termos de legislação de dados, passo fundamental para a inserção do País em foros internacionais bem como, de **proporcionar um ambiente de negócios seguro** que potencialize a **atração e materialização de investimentos na ordem de R$ 250 bilhões** (Brasscom e Frost & Sullivam) em tecnologias de transformação digital até 2021.

No Manifesto mencionado alhures, tem-se o apoio de diversas entidades, empresas, organizações, e até estudiosos da área, quais sejam: Data Privacy.br, FENAPRO – Federação Nacional das Agências de Propaganda, ITS-Rio – Instituto de Tecnologia e Sociedade do Rio de Janeiro, SaferNet – Associação Civil dos Direitos Humanos na Internet no Brasil, FecomercioSP – Federação do Comércio de Bens, Serviços e Turismo do Estado de São Paulo e do autor Danilo Donedo, para se citar alguns.

Em contraponto, a FEBRABAN é uma das poucas organizações que não de acordo com a redação do PL. *''A assessoria da Febraban retornou com o posicionamento oficial: "De forma geral, a FEBRABAN não comenta projetos de lei. Apenas leis já sancionadas"''* Ainda nesse sentido, ressalta-se que circulou em Brasília documento em que a FEBRABAN faz diversas sugestões ao PL. (LUCA, 2018).

Entretanto, observa-se que (LUCA, 2018):

> Na opinião de muitas das entidades que assinam os manifestos desta semana, e que têm entre seus associados os principais prestadores de serviços da cadeias de processamento de dados das instituições financeiras", os pleitos da Febraban são desatualizados.

[34] Disponível no link: https://brasscom.org.br/manifesto-pela-aprovacao-da-lei-de-protecao-de-dados-pessoais/

Ante o exposto, observa-se que o PL n. 53/2018, tem grande apoio da sociedade civil, de estudiosos, da comunidade acadêmica, de empresários, de entidades, e de organizações. Teve em sua concepção a participação democrática dos vários sujeitos relacionados ao tema, e principalmente, segue princípios e diretrizes necessários para a efetiva proteção dos dados pessoais.

Ainda, após por em pauta no Brasil a proteção dos dados pessoais, e obter em retorno tamanha participação da sociedade brasileira, o PL serviu como mais uma lembrança da urgência de lei para tratar do mencionado assunto. Por ora, o que resta é aguardar e conferir qual será o destino do PL 53/2018, na esperança de que cada dia mais se aumente a consciência pública da problemática dos dados pessoais.

CONCLUSÃO

O presente trabalho procurou abarcar a problemática dos dados pessoais, através da leitura aprofundada de artigos, doutrinas, relatórios e notícias, analisando o desenvolvimento dos direitos à privacidade e intimidade até o entendimento de proteção de dados pessoais como um direito autônomo e fundamental. Transcorreu também pelas suas aplicações e verificou a abordagem dada no Marco Civil da Internet, no Projeto de Lei n° 5.276/2016, no Projeto de Lei n° 330/2013, no Projeto de Lei n° 4.060/2012, no Projeto de Lei n° 53/2018 e, bem como, no Regulamento 2016/679 da União Europeia.

No primeiro capítulo, discorreu-se acerca do contexto histórico da problemática, o qual apontou uma dinâmica ímpar das relações sociais e da economia atual. Tratou-se também do desenvolvimento do direito à privacidade e intimidade, de onde, com o decorrer da história, e de novas necessidades, derivou o conceito de proteção de dados pessoais como um direito autônomo e fundamental. Ainda, estabeleceu definições de conceitos importantes para o tema, como: dados pessoas, internet, tratamento, *cookie, big data, bots,* algoritmos, metadados.

No segundo capítulo, investigou-se as aplicações dos dados pessoais, e se conclui que seus usos são variados, qual sejam: utilidade comercial, em campanhas políticas, são manuseados para fins de vigilância de governos e também para a governança eletrônica. E ainda, que o manuseio dos dados pessoais, em se tratando do Brasil, não estão acobertados por qualquer regulamento que defina limites, de que maneira e por quem podem se dar as aplicações dos dados pessoais nos âmbitos mencionados.

No terceiro capítulo, partiu-se para a análise do Regulamento 2016/679 da União Europeia, com apontamentos acerca da efetiva proteção dos dados pessoais. Bem como se discorreu acerca do Marco Civil da Internet e o que representou acerca da matéria. Por fim, esmiuçou-se os projetos de lei que cuidam dos dados pessoais no Brasil, qual sejam: o Projeto de Lei n° 5.276/2016, o Projeto de Lei n° 330/2013, Projeto de Lei n° 4.060/2012, e o Projeto de Lei n° 53/2018.

De todo o exposto, conclui-se que, apesar de o Marco Civil da Internet abordar a temática, é necessária uma lei específica que a regulamente. Isto é, para estabelecer os devidos direitos dos titulares dos dados, abordar as lacunas em relação aos agentes e as autoridades envolvidas, instituir uma autoridade fiscalizadora e possibilitar meios eficazes para a proteção dos dados pessoais. Nesse sentido, também se concluiu a necessidade de

prosseguimento do Projeto de Lei 53/2018, porquanto seu texto foi elaborado com a participação de diversos setores da sociedade – acadêmico, empresas, setor público –, além de oportunizar efetiva proteção aos dados pessoais.

Conforme exposto no segundo capítulo, a utilização comercial dos dados pessoais é um dos pontos que mais se deve proteger, porquanto de um lado há o interesse de diversas empresas e do setor público, que possuem vantagens técnicas e econômicas, e de outro, a sociedade civil como os titulares de dados pessoais. E, nesse aspecto o Projeto de Lei 53/2018 é certeiro, abrange os aspectos comerciais necessários, estabelece os princípios e direitos devidos, além de determinar mecanismos e procedimentos efetivos para a proteção dos dados pessoais e de seus titulares.

Ainda, outros apontamentos observados seriam a possibilidade de introduzir na lei meios tecnológicos de fazer o resguardo dos dados, e de importar da regulação europeia incentivos para que se alcancem os objetivos da lei, como são os casos dos selos medidores de privacidade.

REFERÊNCIAS

AFFONSO, Carlos. **Impulsionamento de propaganda eleitoral na Internet: perguntas e respostas.** Disponível em: <https://tecfront.blogosfera.uol.com.br/2018/05/29/impulsionamento-de-propaganda-eleitoral-na-internet-perguntas-e-respostas/>. Acesso em: 15 jun. 2018.

AIETA, Vania Siciliano. **Marco Civil da Internet**: marco civil da internet e o direito à intimidade. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

AMARAL, Fernando. **Introdução à Ciência de Dados: mineração de dados e big data**. Rio de Janeiro: Alta Books, 2016.

ARAÚJO, Luiz Alberto David; NUNES JÚNIOR, Vidal Serrano. **Curso de Direito Constitucional**. São Paulo: Saraiva, 2001.

ARAÚJO, Tarso. **Como surgiu o computador?** Disponível em: <https://mundoestranho.abril.com.br/tecnologia/como-surgiu-o-computador/>. Acesso em: 15 abr. 2018.

ARTIGO19. **Proteção de dados pessoais no Brasil:** ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL. 2017. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 15 jun. 2018.

BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. **Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional.** 2017. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 15 jun. 2018.

BBC BRASIL. **5 coisas que você talvez não saiba sobre o Facebook reveladas por Zuckerberg em depoimento.** 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43727418>. Acesso em: 15 jun. 2018.

BBC BRASIL. **Conheça as principais revelações feitas pelo site Wikileaks.** 2010. Disponível em: <https://www.bbc.com/portuguese/noticias/2010/11/101129_wiki_ponto_ji>. Acesso em: 15 jun. 2018.

BEZERRA, Arthur Coelho. **Privacidade em perspectivas**: Os Reflexos do Grande Irmão no Admirável Espelho Novo de Black Mirror. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

BRAGA, Lamartine Vieira; ALVES, Welington Souza; FIGUEIREDO, Rejane Maria da Costa; SANTOS, Rildo Ribeiro dos. **O papel do Governo Eletrônico no fortalecimento da governança do setor público.** Disponível em: <https://search.proquest.com/openview/e683eeaa069b662aed4a721ef686e187/1?pq-origsite=gscholar&cbl=2045880>. Acesso em: 15 jun. 2018.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Marco Civil Da Internet.** Brasília, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 15 jun. 2018.

BURCH, Sean. **Facebook Is 'Rotten,' Privacy Is Its 'Kryptonite,' Says Ex-FTC Advisor:** Social network's business model is at odds with protecting its users, according to one expert. 2018. Disponível em: <https://www.thewrap.com/facebook-privacy-kryptonite-ftc/>. Acesso em: 15 jun. 2018.

CABRAL, Rafael. '**A questão dos metadados tem sérias implicações para a privacidade**'. Disponível em: <http://revistagalileu.globo.com/Revista/Common/0,,EMI340880-17770,00-A+QUESTAO+DOS+METADADOS+TEM+SERIAS+IMPLICACOES+PARA+A+PRIVACIDADE.html>. Acesso em: 20 abr. 2018.

CABELLO, Marcos Antonio Assumpção**. Marco Civil da Internet**: Da guarda de registros de acesso a aplicações de internet. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

CASTELLS, Manuel**. A Galáxia Internet: reflexões sobre a Internet, negócios e a sociedade.** Rio de Janeiro: Jorge Zahar Ed., 2003. Tradução: Maria Luiza X. de A. Borges.

_____. **A sociedade em rede**. São Paulo: Paz e Terra, 2016.

CASTRO, Catarina Sarmento e. **Direito da Informática, Privacidade e Dados Pessoais**. Coimbra: Almedina, 2005.

CELLA, José Renato Gaziero; COPETTI, Rafael. **COMPARTILHAMENTO DE DADOS PESSOAIS E A ADMINISTRAÇÃO PÚBLICA BRASILEIRA.** Disponível em: <http://indexlaw.org/index.php/revistadgnt/article/view/2471/pdf>. Acesso em: 15 jun. 2018.

CHARLEAUX, João Paulo. **O que é o Vault 7, o 'maior vazamento da história da CIA', segundo o Wikileaks.** Disponível em: <https://www.nexojornal.com.br/expresso/2017/03/07/O-que-é-o-Vault-7-o-'maior-vazamento-da-história-da-CIA'-segundo-o-Wikileaks>. Acesso em: 15 jun. 2018.

COLNAGO, Cláudio Oliveira Santos. **Marco Civil da Internet**: Provedores de conexão e guarda de registros de acesso a aplicações de internet: o art. 14 do Marco Civil no contexto do dever fundamental de preservação do meio ambiente digital. São Paulo: Atlas, 2014.

CÓRDOVA, Yasodara; DONEDA, Danilo. **Um lugar para os robôs (nas eleições):** A utilização de APIs para o controle das informações que circulam em redes de bots. 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017>. Acesso em: 15 jun. 2018.

DANCE, Gabriel J.x.; CONFESSORE, Nicholas; LAFORGIA, Michael. **Facebook Gave Device Makers Deep Access to Data on Users and Friends:** The company formed data-sharing partnerships with Apple, Samsung and dozens of other device makers, raising new concerns about its privacy protections.. 2018. Disponível em: <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>. Acesso em: 15 jun. 2018.

_____. **Facebook's Device Partnerships Explained.** 2018. Disponível em: <https://www.nytimes.com/2018/06/04/technology/facebook-device-partnerships.html>. Acesso em: 15 jun. 2018.

DATA PRIVACY BRASIL. **A GDPR não aplica somente a dados de cidadãos europeus! Vamos acabar com esse mito!**Disponível em: <http://dataprivacy.com.br/a-gdpr-nao-aplica-somente-a-dados-de-cidadaos-europeus-vamos-acabar-com-esse-mito/>. Acesso em: 15 jun. 2018.

_____. **Esqueça as multas da GDPR! A sua real preocupação deve ser outra: contratos!** Disponível em: <http://dataprivacy.com.br/esqueca-as-multas-da-gdpr-a-sua-real-preocupacao-deve-ser-outra-contratos/>. Acesso em: 15 jun. 2018.

DONEDA, Danilo; CÓRDOVA, Yasodara. **Um lugar para os robôs (nas eleições):** A utilização de APIs para o controle das informações que circulam em redes de bots. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017>. Acesso em: 15 jun. 2018.

DOTTI, Renè Ariel. **Proteção Da Vida Privada e Liberdade de Informação.** São Paulo: RT, 1980.

ELIAS, Paulo Sá. **Algoritmos, Inteligência Artificial e o Direito.** Disponível em: <https://www.conjur.com.br/dl/algoritmos-inteligencia-artificial.pdf>. Acesso em: 15 jun. 2018.

ELOLA, Joseba. **O reconhecimento facial abre caminho para o pesadelo de George Orwell:** Tecnologia ameaça a privacidade das pessoas e abre as portas à distopia descrita no livro '1984'. Por outro lado, permite identificar em tempo recorde terroristas logo após cometerem atentados. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/01/05/tecnologia/1515156123_044505.html>. Acesso em: 15 jun. 2018.

ÉPOCA NEGÓCIOS, **Facebook admite que coleta dados de quem não tem conta na plataforma:** A revelação foi feita hoje pelo presidente da companhia, Mark Zuckerberg, durante audiência. 2018. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/04/facebook-admite-que-coleta-dados-de-quem-nao-tem-conta-na-plataforma.html?utm_source=facebook&utm_medium=social&utm_campaign=post>. Acesso em: 15 jun. 2018.

FARIAS, Edilsom Pereira de. **Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação.** Porto Alegre: Sérgio Antônio FOXX, Chris. **Google e Facebook são acusados de violar nova lei de proteção de dados da Europa.** 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-44259419https://www.bbc.com/portuguese/internacional-44259419>. Acesso em: 15 jun. 2018.

FURLANETO NETO, Mario; GARCIA, Bruna Pinotti. **Marco Civil da Internet**: Da guarda de registros de acesso a aplicações de internet na provisão de aplicações. São Paulo: Atlas, 2014.

G1. **Dados de 2,7 milhões de europeus no Facebook foram usados de forma 'inadequada' pela Cambridge Analytica:** Rede social admitiu que 87 milhões de usuários tiveram dados explorados por consultoria políticas, mas não listava cidadãos da União Europeia.. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/dados-de-27-milhoes-de-europeus-no-facebook-foram-usados-de-forma-inadequada-pela-cambridge-analytica.ghtml>. Acesso em: 15 jun. 2018.

_____. **EUA confirmam que Facebook é investigado por acesso não consentido a dados de mais de 50 milhões de usuários:** Rede social pode ser multada por não proteger informações pessoais e prejudicar consumidores.. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/eua-confirmam-que-facebook-e-investigado-por-acesso-nao-consentido-a-dados-de-mais-de-50-milhoes-de-usuarios.ghtml>. Acesso em: 15 jun. 2018.

GADELHA, Julia. **A evolução dos computadores.** Disponível em: <http://www2.ic.uff.br/~aconci/evolucao.html>. Acesso em: 15 abr. 2018.

GIACCHETTA, André Zonaro; MENEGUETTI, Pamela Gabrielle. **Marco Civil da Internet**: A garantia constitucional à inviolabilidade da intimidade e da vida privada como direito dos usuários no marco civil da internet. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

GODINHO, Adriano Marteleto; ROBERTO, Wilson Furtado. **Marco Civil da Internet**: A guarda de registros de conexão: o marco civil da internet entre a segurança na rede e os riscos à privacidade. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

GOMES, Rodrigo Dias de Pinho**. Privacidade em perspectivas**: Desafios à privacidade: Big Data, Consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de Dados Pessoais. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

GONÇALVES, Victor Hugo Pereira. **Marco civil da internet comentado.** São Paulo: Atlas, 2017.

GUERRA, Gustavo Rabay. **Marco Civil da Internet**: Direito à inviolabilidade e ao sigilo de comunicações privadas armazenadas: um grande salto rumo à proteção judicial da privacidade na rede. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

GUGIK, Gabriel. **A história dos computadores e da computação.** Disponível em: <https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 15 abr. 2018.

GUIDI, Guilherme Berti de Campos. **Privacidade em perspectivas**: Modelos Regulatórios para Proteção de Dados Pessoais. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

GUILHERME, Paulo. **Por que o Facebook comprou o WhatsApp e o Instagram? Este gráfico explica.** 2014. Disponível em: <https://www.tecmundo.com.br/facebook/60080-facebook-comprou-o-whatsapp-o-instagram-grafico-explica.htm>. Acesso em: 15 jun. 2018.

IGLESIAS, Daphne. **Privacidade em perspectivas**: Nudging Privacy: Benefits and Limits of Persuading Human Behaviour Online. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

ITAGIBA, Gabriel. **Fake news e Internet: esquemas, bots e a disputa pela atenção.** 2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/04/v2_fake-news-e-internet-bots.pdf>. Acesso em: 15 jun. 2018.

ITSRIO. **Anteprojeto de lei de proteção de dados pessoais:** Contribuição do ITS para o debate público. 2015. Disponível em: <https://itsrio.org/wp-content/uploads/2015/07/Consulta-APL-de-Dados.pdf>. Acesso em: 15 jun. 2018.

ITSRIO. **PegaBot:** Descubra se aquele perfil de rede social é bot. Plataforma em fase de testes.. Disponível em: <https://itsrio.org/pt/projetos/pegabot/>. Acesso em: 15 jun. 2018.

KUJAWSKI, Fábio Ferreira; THOMAZ, Campos Elias. **Marco Civil da Internet**: Da proteção aos registros, dados pessoais e comunicações privadas – um enfoque sobre o marco civil da internet. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

LAZARI, Rafael de. **Noções de Direito Constitucional**. Disponível em: <https://www.novaconcursos.com.br/media/wysiwyg/Retificacoes/2-Nocoes-de-direito-constitucional.pdf>. Acesso em: 15 abr. 2018.

LEMOS, Ronaldo. **Governo é acusado de vender dados:** Proteção de dados pessoais precisa valer também para o setor público. Disponível em: <https://www1.folha.uol.com.br/colunas/ronaldolemos/2018/06/governo-e-acusado-de-vender-dados.shtml?loggedpaywall#_=_>. Acesso em: 15 jun. 2018.

LIMA, Caio César Carvalho. **Marco Civil da Internet:** Garantia da privacidade e dados pessoais à luz do marco civil da internet. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

LUCA, Cristina de. **Manifestos pedem aprovação do PL de proteção de dados, sem mudanças.** 2018. Disponível em: <https://porta23.blogosfera.uol.com.br/2018/06/26/manifestos-pedem-aprovacao-do-pl-de-protecao-de-dados-sem-mudancas/?cmpid=copiaecola>. Acesso em: 27 jul. 2018.

MAILJET. **GDPR and Profiling.** 2018. Disponível em: <https://www.mailjet.com/gdpr/profiling/>. Acesso em: 15 jun. 2018.

MANGETH, Ana Lara; NUNES, Beatriz Marinho. **A proteção de seus dados pessoais está em jogo no Senado.** 2018. Disponível em: <https://feed.itsrio.org/senado-vs-câmara-seus-dados-pessoais-em-jogo-97d7b0cefc54>. Acesso em: 15 jun. 2018.

_____. **Seis pontos para entender o Regulamento Geral de Proteção de Dados da UE**. 2018. Disponível em: <https://feed.itsrio.org/seis-pontos-para-entender-a-lei-europeia-de-proteção-de-dados-pessoais-gdpr-d377f6b691dc>. Acesso em: 15 jun. 2018.

FREDOOM HOUSE. **Manipulating Social Media to Undermine Democracy.** Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2017>. Acesso em: 15 jun. 2018.

MATTIUZZO, Marcela**. Privacidade em perspectivas:** Business Models and Big Data: How Google uses your Personal Information. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

MAYER-SCHONBERGER, Viktor; CUKIER, Kenneth. Big Data: **A Revolution That Will Transform How We Live, Work, and Think**. New York. Houghton Mifflin Harcourt, 2013, p. 190 apud GOMES, Rodrigo Dias de Pinho. **Desafios à Privacidade: Big Data, Consentimento, Legítimos Interesses e Novas Formas de Legitimar o Tratamento de Dados Pessoais**, 2018, p. 236.

MENDONÇA, Renata. **Como os testes de Facebook usam seus dados pessoais - e como empresas ganham dinheiro com isso**. 2018. Disponível em: <http://www.bbc.com/portuguese/salasocial-43106323>. Acesso em: 25 abr. 2018.

MONTEIRO, Renato Leite. **A nova Regulação de Proteção de Dados Pessoais aprovada na União Europeia e sua influência no Brasil.** Disponível em: <https://renatoleitemonteiro.jusbrasil.com.br/artigos/273633610/a-nova-regulacao-de-protecao-de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil>. Acesso em: 2 abr. 2018.

MORAIS, José Luiz Bolzan de; MENEZES NETO, Elias Jacob de. **Marco Civil da Internet:** A insuficiência do marco civil da internet na proteção das comunicações privadas armazenadas e do fluxo de dados a partir do paradigma da surveillance. Organizadores: George Salomão e Ronaldo Lemos. São Paulo: Atlas, 2014.

MORSE, Jack. **Facebook bug affected 14 million people's privacy settings.** 2018. Disponível em: <https://mashable.com/2018/06/07/facebook-public-settings-14-million-bug/#Wnk.aQAXliqn>. Acesso em: 15 jun. 2018.

MOTTA, Sylvio; BARCHET; Gustavo. **Curso de direito constitucional: atualizado até a Emenda constitucional nº 53/2006**. Imprenta: Rio de Janeiro, Elsevier, Campus, 2007.
NEIRA, Ana. **País terá eleição sem proteção de dados na internet.** Disponível em: <https://politica.estadao.com.br/noticias/geral,pais-tera-eleicao-sem-protecao-de-dados-na-internet,70002345656>. Acesso em: 15 jun. 2018.

NETTO, Andrei. **NSA e CIA espionaram eleições francesas de 2012, diz WikiLeaks:** Agências de inteligência americanas queriam detalhes sobre as relações do ex-presidente Nicolas Sarkozy com assessores, seus meios de financiamento e detalhes de outros 'candidatos emergentes' ao Palácio do Eliseu. Disponível em: <https://internacional.estadao.com.br/noticias/geral,nsa-e-cia-espionaram-eleicoes-francesas-de-2012-diz-wikileaks,70001668941>. Acesso em: 15 jun. 2018.

O'BRIEN, Danny. **Why Am I Getting All These Terms of Service Update Emails?** 2018. Disponível em: <https://www.eff.org/deeplinks/2018/05/why-am-i-getting-all-these-terms-service-update-emails>. Acesso em: 15 jun. 2018.

PAYÃO, Felipe. **WikiLeaks vaza documentos: CIA vigia o seu Android, iPhone e smart TV.** Disponível em: <https://www.tecmundo.com.br/wikileaks/114808-wikileaks-vaza-documentos-cia-vigia-android-iphone-smart-tv.htm>. Acesso em: 15 jun. 2018.

PEREIRA, Ana Paula. **O que é algoritmo?** Disponível em: <https://www.tecmundo.com.br/programacao/2082-o-que-e-algoritmo-.htm>. Acesso em: 15 jun. 2018.

PERES-NETO, Luiz. **Privacidade em perspectivas**: Ética e Privacidade: Múltiplos Olhares e Partir do Campo da Comunicação. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

POLÍTICAS PÚBLICAS. **Governança eletrônica**. Disponível em: <https://politicaspublicas.almg.gov.br/temas/governanca_eletronica/entenda/informacoes_gerais.html?tagNivel1=176&tagAtual=10260>. Acesso em: 15 jun. 2018.

PROXXIMA. **Uso de algoritmos acontece na economia, política, entretenimento … e marketing:** Dados moldam produtos de empresas como Facebook, Google, Netflix e Amazon, mas também são utilizados em várias outras áreas da atividade humana. Veja Infográfico.. 2018. Disponível em: <http://www.proxxima.com.br/home/proxxima/how-to/2018/03/27/uso-de-algoritmos-acontece-na-economia-politica-entretenimento-e-marketing.html>. Acesso em: 15 jun. 2018.

RODOTÀ, Stefano. **A vida na sociedade da vigilância - a privacidade hoje.** Rio de Janeiro: Renovar, 2008. Tradução de: Danilo Doneda, Luciana Cabral Doneda.

SAFERNET. **O que são os Metadados?** Disponível em: <http://new.safernet.org.br/node/199.>. Acesso em: 15 jun. 2018.

SALAS, Javier. **Robôs e 'trolls', as armas que Governos usam para envenenar a política nas redesPelo menos 30 países sofrem a manipulação do debate público por meio de perfis falsos nas redes sociais:** Pelo menos 30 países sofrem a manipulação do debate público por meio de perfis falsos nas redes sociais. 2017. Disponível em: <https://brasil.elpais.com/brasil/2017/11/22/tecnologia/1511352685_648584.html>. Acesso em: 15 jun. 2018.

SANTOS, Andréia. **Privacidade em perspectivas:** O Impacto do Big Data e dos Algoritmos nas Campanhas Eleitorais. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

SANTOS, Coriolano Aurélio de Almeida Camargo; CRESPO, Marcelo. **Inteligência artificial, tecnologia e o Direito: o debate não pode esperar!** Disponível em: <http://www.migalhas.com.br/DireitoDigital/105,MI249734,41046-Inteligencia+artificial+tecnologia+e+o+Direito+o+debate+nao+pode>. Acesso em: 15 jun. 2018.

SCHINCARIOL, Fernando. **Privacidade em perspectivas**: Filtros Bolha, as Escolhas que Fizemos e as que Faremos: Considerações sobre como (Não) Regular a Internet. Rio de Janeiro: Lumen Juris, 2018.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 24. ed. São Paulo: Malheiros, 2005.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s: Redes digitais, privacidade e venda de dados pessoais.** São Paulo: Edições Sesc, 2017.

SOPRANA, Paula. **O que é a GDPR, a lei de proteção de dados europeia, e por que ela importa.** 2018. Disponível em: <https://gizmodo.uol.com.br/lei-proteca-dados-gdpr/>. Acesso em: 15 jun. 2018.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. **Marco civil da internet: construção e aplicação.** Juiz de Fora: Editar Editora Associada Ltda, 2016.

SPUTNIK. **Analista sobre recentes revelações do WikiLeaks: 'Não há dúvidas que alguém nos escuta'.** 2017. Disponível em: <https://br.sputniknews.com/americas/201703107860824-wikileaks-espionagem-cia-inteligencia-samsung/>. Acesso em: 15 jun. 2018.

STEIBEL, Fabro Boaz. **Quem financia fake news?:** Converter dinheiro em atenção é um modelo de negócio legítimo e antigo, mas, quando usado para impulsionar conteúdo falso, torna-se um problema. Disponível em: <https://gauchazh.clicrbs.com.br/colunistas/fabro-boaz-steibel/noticia/2017/11/quem-financia-fake-news-cj9inlgt8055y01ogmnchfv60.html>. Acesso em: 15 jun. 2018.

SUSSEKIND, Evandro. **COMO É FEITA A DISTRIBUIÇÃO DE PROCESSOS NO STF?** 2017. Disponível em: <http://www.politize.com.br/distribuicao-processos-stf/>. Acesso em: 15 jun. 2018.

TRINDADE, Rodrigo. **IA da Uber identificará passageiros bêbados que pedirem carros... - Veja mais em https://tecnologia.uol.com.br/noticias/redacao/2018/06/09/ia-da-uber-identificara-passageiros-bebados-que-pedirem-carros.htm?cmpid=copiaecola.** 2018. Disponível em: <https://tecnologia.uol.com.br/noticias/redacao/2018/06/09/ia-da-uber-identificara-passageiros-bebados-que-pedirem-carros.htm>. Acesso em: 15 jun. 2018.

VALENTE, Jonas. **Privacidade em perspectivas**: Promovendo a privacidade e a proteção de dados pela tecnologia: Privacy by Design e Privacy Enhancing-Technologies. Organizadores: Sergio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.

VAZ, José Carlos. **Desafios para a inclusão digital e governança eletrônica.** Disponível em: <http://www.polis.org.br/uploads/808/808.pdf>. Acesso em: 15 jun. 2018.

_____, José Carlos. **Governança eletrônica: para onde é possível caminhar?** Disponível em: <http://www.polis.org.br/uploads/745/745.pdf>. Acesso em: 15 jun. 2018.

WENDLING, Mike. **Como o termo 'fake news' virou arma nos dois lados da batalha política mundial.** Disponível em: <https://www.bbc.com/portuguese/internacional-42779796>. Acesso em: 15 jun. 2018.