UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
CURSO DE GRADUAÇÃO EM DIREITO

JOSE IGOR ALVES FONTES

DADOS PESSOAIS DIGITAIS E SEU TRATAMENTO NO ORDENAMENTO JURÍDICO BRASILEIRO

NATAL/RN
2018

JOSE IGOR ALVES FONTES

DADOS PESSOAIS DIGITAIS E SEU TRATAMENTO NO ORDENAMENTO JURÍDICO BRASILEIRO

Monografia apresentada ao Curso de Graduação em Direito como parte dos requisitos para a obtenção do Título de Bacharel em Direito do Centro de Ciências Sociais Aplicadas da Universidade Federal do Rio Grande do Norte.

Orientadora: Profa. Ma. Anna Emanuella Nelson Dos Santos Cavalcanti Da Rocha.

NATAL/RN

2018

Universidade Federal do Rio Grande do Norte - UFRN
Sistema de Bibliotecas - SISBI
Catalogação de Publicação na Fonte. UFRN - Biblioteca Setorial do Centro Ciências Sociais Aplicadas - CCSA

Fontes, Jose Igor Alves.
Dados pessoais digitais e seu tratamento no ordenamento jurídico brasileiro / Jose Igor Alves Fontes. - 2018.
44f.: il.

Monografia (Graduação em Direito) - Universidade Federal do Rio Grande do Norte, Centro de Ciências Sociais Aplicadas, Departamento de Direito. Natal, RN, 2018.
Orientador: Profa. Me. Anna Emanuella Nelson Dos Santos Cavalcanti Da Rocha.

1. Direito Constitucional - Monografia. 2. Direito ao sigilo - Monografia. 3. Dados pessoais - Monografia. I. Rocha, Anna Emanuella Nelson Dos Santos Cavalcanti Da. II. Universidade Federal do Rio Grande do Norte. III. Título.

RN/UF/Biblioteca Setorial do CCSA CDU 342

Elaborado por Eliane Leal Duarte - CRB-15/355

MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO RIO GRANDE DO NORTE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE DIREITO PRIVADO

ATA DE DEFESA PÚBLICA DE CONCLUSÃO DO CURSO DE BACHARELADO EM DIREITO

Aos 04 (quatro) dias do mês de julho do ano de 2018, às 16h, no Auditório Varela Barca, foi instalada a Comissão Examinadora para a defesa oral e pública da monografia sob o título: "**DADOS PESSOAIS DIGITAIS E SEU TRATAMENTO NO ORDENAMENTO JURÍDICO BRASILEIRO**", como trabalho final de conclusão de curso, apresentado(a) pelo(a) aluno(a) **JOSÉ IGOR ALVES FONTES**, matrícula nº 2013028110, ao Curso de Direito da Universidade Federal do Rio Grande do Norte, como parte dos requisitos para obtenção do título de Bacharel em Direito. A comissão examinadora foi presidida pelo(a) professor(a)/colaborador(a) **ANNA EMANUELLA NELSON DOS SANTOS CAVALCANTI DA ROCHA**, matrícula nº 2474994, lotado(a) no DEPARTAMENTO DE DIREITO PRIVADO; 1º membro o(a) professor(a)/colaborador(a) **ÂNGELO JOSÉ MENEZES SILVINO**, matrícula nº 1246641, lotado(a) no DEPARTAMENTO DE DIREITO PROCESSUAL E PROPEDÊUTICA; e o 2º membro o(a) professor(a)/colaborador(a) **ANA CAROLINA GUILHERME COELHO**, matrícula nº x.x.x.x, lotado(a) no Colaborador externo, integrantes da referida comissão que emitiu o seguinte parecer: Pela aprovação. A comissão examinadora após a defesa oral e o cumprimento dos demais procedimentos considerou a monografia aprovada. A comissão decidiu atribuir à menção _____, atribuindo a nota: 9,5.

Comissão Examinadora

ANNA EMANUELLA NELSON DOS SANTOS CAVALCANTI DA ROCHA
Presidente

ÂNGELO JOSÉ MENEZES SILVINO
1º Membro

ANA CAROLINA GUILHERME COELHO
2º Membro

AGRADECIMENTOS

A expectativa de ser aprovado no vestibular se torna o sonho de entrar na faculdade. Nem imaginamos o caminho tortuoso que iremos traçar. Depois de altos e baixos durante o trajeto da graduação, é chegada a hora do fim.

Agradeço;

Principalmente, aos meus pais, por terem se dedicado tanto a darem uma educação de qualidade aos seus filhos, muitas vezes tendo que realizar sacrifícios, que no fim, valeram a pena. A graduação em Direito na UFRN, mais do que uma conquista pessoal, é um presente para eles.

Também, ao restante da família, irmãos, tios e primos, pelo apoio até aqui e pela certeza que um dia toda a expectativa em mim depositada seria transformada em realidade.

À companhia dos meus amigos que foram, muitas vezes, motivo determinantes para continuar esta jornada.

À Profa, Anna Emanuella, por ter concordado em orientar a construção desta pesquisa e contribuir para a minha formação acadêmica, e ao Prof. Ângelo Menezes e à Profa. Carol Coelho por participarem da ativamente na avaliação deste trabalho.

“*As pessoas sempre têm medo das mudanças. tinham medo da eletricidade quando foi inventada*.” (Bill Gates)

RESUMO

A crescente importância das relações virtuais e os escândalos de vazamento de dados dão ensejo a esta monografia. Verificou-se a necessidade de uma pesquisa da legislação brasileira sobre como o país lida com o tema de proteção a dados pessoais digitais, associada a pesquisa jurisprudencial das cortes superiores nacionais de modo a extrair seu entendimento sobre o assunto. Também se faz a comparação com legislações de outras partes do mundo em contraste com a brasileira e o estudo de um dos maiores acontecimentos no que diz respeito à sigilo de dados, com o objetivo de demonstrar a necessidade da regulamentação. Com esta publicação, espera-se comprovar, quantitativa e qualitativamente, a existência de legislação, assim como interpretação jurídica, a favor da proteção de dados pessoais no Brasil.

Palavras-chave: Direito constitucional; direito ao sigilo; direito digital; dados pessoais.

ABSTRACT

The growing importance of virtual relationships and data leakage scandals gives rise to this monograph. It was verified the need for a research of the Brazilian legislation on how the country deals with the theme of protection of digital personal data, associated with the jurisprudential research of the national superior courts in order to extract their understanding on the subject. Also, comparisons are made with legislation in other parts of the world in contrast to the Brazilian law and the study of one of the major events regarding data confidentiality, in order to demonstrate the need for regulation. With this publication, it is hoped to prove, quantitatively and qualitatively, the existence of legislation, as well as legal interpretation, in favor of the protection of personal data in Brazil.

Keywords: Constitucional right; right to secrecy; digital rights; personal data.

SUMÁRIO

1 INTRODUÇÃO 8
2 ANÁLISE LEGISLATIVA SOBRE A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL 11
2.1 A CONSTITUIÇÃO FEDERAL de 1988 11
2.2 O CÓDIGO CIVIL, O CÓDIGO DE DEFESA DO CONSUMIDOR E O CÓDIGO PENAL 13
2.3 O MARCO CIVIL DA INTERNET 14
2.4 O DECRETO Nº 8.771 DE 2016 17
2.5 OS PROJETOS DE LEI 4060/2012 E 330/2013..... 18
3 CORTES SUPERIORES: O ENTENDIMENTO JURÍDICO BRASILEIRO .. 20
3.1 O SUPREMO TRIBUNAL FEDERAL 20
3.2 O SUPERIOR TRIBUNAL DE JUSTIÇA 24
4 DADOS PESSOAIS PELO MUNDO: O TEMA EM DIFENRENTES PAÍSES 29
4.1 ESTADOS UNIDOS 29
4.2 UNIÃO EUROPEIA 30
4.3 JAPÃO 31
4.4 ARGENTINA 32
4.5 MÉXICO 33
5 ESTUDO DE CASO: CASO *FACEBOOK & CAMBRYGE ANALITCA* E O PERIGO DA FALTA DE REGULAMENTAÇÃO 34
6 CONCLUSÃO 39
7 REFERÊNCIAS 41

1 INTRODUÇÃO

O direito tende a acompanhar as transformações sociais e adequar-se a elas, de modo que os conflitos resultantes estejam assegurados dentro das normas e legislação do país. Segundo a teoria tridimensional do direito[1], o fato precede a norma, que é gerada através de um valor sobre aquele.

Nessa esteira, nasce a teoria dos direitos fundamentais configurando-se como um dos principais pontos quando se trata de relações humanas, pois foi a partir do surgimento do Estado e de suas mais diversas formas de atuação que as gerações de direitos fundamentais se estabeleceram. Primeiramente, os direitos de resistência, como liberdade, privacidade, assim como os direitos civis e políticos. Com a emergência do Estado social, e, principalmente, com a constituição de Weimar, na Alemanha, nasceram os direitos de segunda geração, os chamados sociais ou prestacionais, constituindo obrigação estatal, como a educação, saúde, trabalho e lazer. E, por fim, os direitos fundamentais de terceira geração correspondem aos direitos coletivos (difusos, coletivos *stricto sensu* e individuais homogêneos), percebidos na modernidade nos movimentos neoconstitucionalistas, que tendem por abranger cada vez mais aspectos da vida humana sob a tutela constitucional. São exemplos: o direito ao meio ambiente e ao patrimônio comum da humanidade. Atualmente já se fala, inclusive, de direitos de quarta geração, aqueles advindos da pluralidade e da democracia, como o respeito às minorias e o direito de comunidades globais.

Influenciado por esse dinamismo social, a revolução digital ocorrida no início do sec. XXI trouxe novas maneiras de interação social, principalmente com as redes sociais, que criaram um novo horizonte de comunidade (virtual), quebrando as barreiras que antes pensava-se existir. Pessoas de todo o mundo se conectam reciprocamente. Hoje vivemos numa sociedade de rápida transmissão de dados, com diversas fontes e usuários, que recebem e enviam informações mutuamente de uma maneira há pouco tempo inconcebível. Devido a esse rápido desenvolvimento dos meios de troca de dados digitais, vários aspectos necessários para sua dinâmica ficaram de lado, um deles, e

[1] REALE, Miguel. Teoria Tridimensional do Direito. 5ª ed., Editora Saraiva, São Paulo, 2003.

objeto desse estudo, é a privacidade e sigilo dos dados transmitidos entre pessoas.

Recentes escândalos envolvendo vazamento de dados de uma famosa rede social[2] colocaram o mundo em alerta sobre o perigo que envolve o uso de dados digitais para fins diversos dos quais foram destinados. A capacidade de tais dados influenciarem no resultado de uma eleição presidencial de uma das maiores potências mundiais demonstra que há muito o que o direito ainda deve proteger. O uso indiscriminado e desenfreado da internet dá, àqueles que sabem atirar, a arma para cometer as mais diferentes infrações. O problema fica evidente em casos como o de vazamento de dados do governo americano pelo site *Wikileaks*, comprometendo a segurança nacional, como também o caso da *PSN Sony*, onde dados financeiros, como números de cartões de crédito, de diversos clientes foram postos a público[3].

Dados digitais são todas informações, pessoais ou não, que são coletadas por um agente e armazenadas ou transferidas a outrem, por meio de mecanismos que utilizam linguagem computacional. A transmissão de informações é, e desde sempre foi, aspecto fundamental das relações humanas.

Agora estão presentes em todos os aspectos possíveis da vida contemporânea, desde a fabricação de alimentos, a educação, esporte, finanças, meio ambiente, mobilidade, saúde, segurança até as relações interpessoais.

---

[2] CADWALLADR, Carole; GRAHAM-HARRISON, Emma. Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. The Guardian. Disponível em: <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. Acesso em: 6 jun. 2018.
DE LLANO, Pablo; SANCHEZ, Alvaro. Vazamento de dados do Facebook causa tempestade política mundial. Disponivel em: <https://brasil.elpais.com/brasil/2018/03/19/internacional/1521500023_469300.html>. Acesso em: 6 jun. 2018.
ROSENBERG, Matthew; CONFESSORE, Nicholas; CADWALLADR, Carole. How Trump Consultants Exploited the Facebook Data of Millions. The New York Times. Disponível em: <https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html?rref=collection%2Ftimestopic%2FFacebook&action=click&contentCollection=business&region=stream&module=stream_unit&version=search&contentPlacement=233&pgtype=collection>. Acesso em: 6 jun. 2018.

[3] PRESSE, France. Ex-funcionário da CIA é acusado de vazar dados ao WikiLeaks. Globo. Disponível em: <https://g1.globo.com/mundo/noticia/ex-funcionario-da-cia-e-acusado-de-vazar-dados-ao-wikileaks.ghtml>. Acesso em: 6 jun. 2018.
ROHR, Altieres. Caso da PSN mostra despreparo para lidar com questões de segurança. Globo. Disponível em:<http://g1.globo.com/tecnologia/noticia/2011/05/caso-da-psn-mostra-despreparo-para-lidar-com-questoes-de-seguranca.html>. Acesso em: 6 jun. 2018.

O direito que nos interessa aqui é o de sigilo de dados pessoais, sendo um aspecto do direito à privacidade e dos direitos da personalidade, que, por sua vez é a expressão do direito de liberdade, no momento em que o indivíduo é livre para mostrar ao mundo aquilo que ele pensa necessário ou adequado, preservando aquilo que julga vergonhoso, desonroso ou simplesmente de interesse estritamente particular.

Desse modo, esta pesquisa visa reunir informações acerca das legislações que tratam sobre a proteção de dados pessoais digitais no Brasil, comparando-as com outros países no mundo, a partir de análise de caso e revisão bibliográfica, legislativa e jurisprudencial, por meio de pesquisa exploratória qualitativa e do método dedutivo, para responder à pergunta: no Brasil, há proteção legislativa ou jurídica para dados pessoais digitais? Se sim, de qual maneira ela se desenvolve?

Assim, para os fins que se prestam este trabalho, por se tratar de uma revisão legislativa, se utilizará o conceito de dados pessoais estabelecido no art. 14[4] do decreto nº 8.771/16, que regulamenta a lei nº 12.965/14, Marco Civil da Internet.

[4] Art. 14. Para os fins do disposto neste Decreto, considera-se:
I - dado pessoal - dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa;
II - tratamento de dados pessoais - toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

2 ANÁLISE LEGISLATIVA SOBRE A PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

2.1 A CONSTITUIÇÃO FEDERAL DE 1988

A constituição federal brasileira estabelece, em seu art. 1º, III[5], que um dos fundamentos do Estado brasileiro é a dignidade da pessoa humana. Sendo, como já exposto, o direito ao sigilo de dados, aspecto do direito da personalidade e, portanto, componente do conceito de dignidade humana, esta é a primeira referência constitucional a ser enfocada em relação ao tema aqui tratado.

Logo após, em seu art. 5º, X[6], defende a inviolabilidade da intimidade, da vida privada, da honra e da imagem da pessoa, todos aspectos relacionados à convivência social e, portanto, também digital, uma vez que as relações *on-line* são espelho das relações sociais no mundo real. Assim, do mesmo modo que a Constituição garante a privacidade da residência, por exemplo, também o faz para os dados que qualquer pessoa insere na rede, não obstante serem aspectos de um mesmo direito, qual seja, o da inviolabilidade.

Mais especificamente, traz, em seu art. 5º, XII[7], o direito fundamental ao sigilo, dessa vez, fazendo menção expressa aos dados, mas deixando em aberto que tipo de dados são esses. A partir de uma interpretação teleológica[8], depreende-se que todos e quaisquer dados, sejam aqueles em posse dos

---

[5] Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
(…)
III - a dignidade da pessoa humana;

[6] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(…)
X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[7] *Ibidem*
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

[8] BARROSO, Luís Roberto. Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo. 3ª ed. – São Paulo: Saraiva, 2011.

arquivos estatais, como aqueles em posse dos provedores e canais de comunicação digital, merecem a devida proteção constitucional.

Pela análise do trecho, podemos ver que o constituinte estabeleceu diferentes graus de violabilidade: primeiramente temos as correspondências, comunicações telegráficas e dados, os quais têm inviolabilidade absoluta. Na circunstância das comunicações telefônicas, a inviolabilidade é relativa, pois, nos casos previstos de investigação criminal ou instrução penal, o sigilo dessas comunicações pode ser quebrado desde que atenda a um interesse público maior, qual seja o fim da ação penal[9].

Vale ressaltar, ainda, que a carta magna, em seu art. 136[10], quando institui a possibilidade da decretação do estado de defesa, abre a oportunidade para a restrição do direito ao sigilo, podendo esse ser relativizado em nome do interesse nacional durante tempos de crise.

Apesar das técnicas de interpretação constitucional que possuímos, capazes de, em certos casos, conferir novo significado às normas constitucionais, consideramos necessária a expressão previsão de regras de proteção de dados pessoais, devido à importância do tema, sendo indispensável a atuação do Congresso Nacional no processo de emenda à Constituição.

---

[9] LIMA NETO, José Henrique Barbosa Moreira. Da Inviolabilidade de dados: inconstitucionalidade da Lei 9296/96. (Lei de interceptação de comunicações telefônicas). Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 2, n. 14, 1 jun. 1997. Disponível em: <https://jus.com.br/artigos/197>. Acesso em: 5 jun. 2018.

[10] Art. 136. O Presidente da República pode, ouvidos o Conselho da República e o Conselho de Defesa Nacional, decretar estado de defesa para preservar ou prontamente restabelecer, em locais restritos e determinados, a ordem pública ou a paz social ameaçadas por grave e iminente instabilidade institucional ou atingidas por calamidades de grandes proporções na natureza.

§ 1º O decreto que instituir o estado de defesa determinará o tempo de sua duração, especificará as áreas a serem abrangidas e indicará, nos termos e limites da lei, as medidas coercitivas a vigorarem, dentre as seguintes:

I - restrições aos direitos de:

[...]

b) sigilo de correspondência;

c) sigilo de comunicação telegráfica e telefônica;

2.2 O CÓDIGO CIVIL, O CODÍGO DE DEFESA DO CONSUMIDOR E O CÓDIGO PENAL

O Código Civil Brasileiro limita-se a abordar o tema da proteção de dados pessoais de forma genérica, tratando dos direitos da personalidade. Em seus arts. 20 e 21[11], estabelece a proteção à intimidade e à vida privada, sem necessariamente citar os dados transmitidos por meios digitais.

Na mesma linha, segue o Código de Defesa do Consumidor, contando apenas com o art. 43[12], que faz menção aos bancos de dados e cadastros de consumidores mantidos pelos prestadores de serviço, estabelecendo diretrizes para sua instalação, como também conferindo o direito ao consumidor de ter acesso livre aos seus dados pessoais armazenados.

Já o Código Penal, possuí uma interessante inovação no assunto. Com a edição da lei nº 12.737/12, conhecida também como lei Carolina Dieckmann[13], atriz que teve suas fotos íntimas vazadas por invasores de dispositivos, que acrescenta os arts. 154-A[14] e 154-B ao texto do código, tipificando o crime de invasão de dispositivo informático, o Brasil adentra na sua primeira forma de proteção efetiva de dados pessoais digitais, posto que comina penas para aqueles que se utilizam de artifícios para invadir os dispositivos eletrônicos alheios e subtrair ou divulgar informações acerca dos indivíduos.

Verifica-se nesses três importantes dispositivos a falha legislativa em inserir regulamentação sobre proteção de dados, deixando lacunas patentes na

---

[11] Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

[12] 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.

[13] GLOBO. Lei 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor. Disponível em: <http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html>. Acesso em: 6 jun. 2018.

[14] Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

lei, contribuindo para o aumento de casos de vazamento de dados e de informações pessoais.

2.3 O MARCO CIVIL DA INTERNET

A lei nº 12.965/14, mais conhecida como o Marco Civil da Internet, apesar de uma grande conquista em termos de direito contemporâneo, mostrou-se muito aquém do que era esperado, tomando como base as legislações internacionais e a necessidade de regulamentação dos constantes novos meios de comunicação. Numa primeira análise, podemos notar que tal dispositivo consta apenas com trinta e dois artigos, o que se torna ínfimo dentro da variedade de situações possíveis de regulamentação dentro do ambiente virtual. Dito isso, ela se torna muito mais um arcabouço principiológico necessário do que um diploma que tem por objetivo esgotar o tema, assim como ocorre com os códigos civil e penal brasileiros.

De pronto, em seu art. 3º[15] estabelece os princípios a serem observados no uso da internet no Brasil, dentre eles, cabe destacar o princípio da proteção à privacidade e da proteção aos dados pessoais, enfoques da presente monografia. A alocação desses princípios logo no início do texto é importante pois cria as bases hermenêuticas e axiológicas em qual se sustentam todas as outras regras derivadas das normas sobre o tema.

Posteriormente, no art. 7º[16], ocupa-se em tratar, especificamente, do objeto de estudo aqui em foco, nos seus três primeiros incisos, a proteção dada aos dados pessoais. Nesse sentido, define como proteção a inviolabilidade em três etapas: (i) a inviolabilidade da intimidade e vida privada, (ii) do fluxo de comunicações e (iii) das comunicações privadas armazenadas.

---

[15] Art. 3ºA disciplina do uso da internet no Brasil tem os seguintes princípios:
(…)
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;

[16] 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;

A inviolabilidade da intimidade e da vida privada se dá por meio da segurança dos dispositivos domésticos e dos servidores que armazenam dados pessoais (senhas, *logins* etc), impedindo o acesso de terceiros mal-intencionados, garantido a indenização em casos de danos causados. A inviolabilidade do fluxo de comunicações ocorre pela livre expressão do pensamento e das ideias, sem mecanismos de censura ou de análise de conteúdo, onde todos sejam livres para ler e publicar, salvo por interesse público através de ordem judicial. A inviolabilidade das comunicações privadas armazenadas realiza-se por meio da restrição de acesso às informações privadas de terceiros, erguendo bloqueios que exijam a identificação pessoal para o acesso a dados sigilosos.

Nos incisos seis a dez[17], apesar de o *caput* do artigo orientar uma relação de direitos, expressam muito mais deveres, principalmente para os prestadores de serviço, uma vez que os obriga a prestar informações claras sobre os contratos e o regime de proteção de dados, proíbe o fornecimento de dados pessoais dos usuários a terceiros (salvo expresso consentimento), exige clareza na coleta e armazenamento de dados pessoais e permite a exclusão desses dados a requerimento do usuário, coadunando com o direito ao esquecimento[18].

Adiante, a lei estabelece, em seu art. 8º[19], aspectos cíveis do uso da internet no país. Em primeiro plano, trata da nulidade das cláusulas contratuais

---

[17] *Ibidem*

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.

[...]

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.

[18] CONSALTER, Zilda Mara – Direito ao esquecimento: proteção da intimidade e ambiente virtual.

[19] 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.

que contrariem os princípios constitucionais adequados, como também os já expostos nos artigos iniciais do mesmo dispositivo, destacando o direito ao sigilo, sendo nula de pleno direito qualquer cláusula que atente por permitir que o provedor do serviço colete, utilize, armazene, trate ou publique dados pessoais do usuário sem sua expressa anuência.

Os arts. 10, 11 e 12[20], tratam de diferentes aspectos da proteção aos dados pessoais. Primeiramente, a vinculação judicial dos provedores de serviços de internet, em que esses ficam obrigados a disponibilizar as informações necessárias às autoridades competentes, desde que acompanhadas de ordem judicial e sob expressa fundamentação, pois se trata de uma forma de quebra de sigilo e invasão de privacidade do usuário. Posteriormente, trata de aspectos internacionais do tratamento de dados pessoais, como da competência e territorialidade, afirmando que o disposto nesta lei se aplica aos dados processados por empresas brasileiras, estrangeiras que possuem pelo menos uma filial no território nacional ou estrangeiras cujo processo de armazenamento e tratamento de dados se dê, em alguma etapa, em território brasileiro. Por último, estabelece sanções para o descumprimento das medidas acima, que vão desde advertência até a proibição do exercício da atividade, sendo um exemplo de normal penal incorporada ao texto da lei.

Finalmente, em seu art. 16, II[21], cria a proibição dos provedores do serviço de armazenar informações de dados pessoais dos usuários além daquelas necessárias à prestação do serviço, como, por exemplo, aplicativos de venda de ingressos que armazenam dados financeiros e sobre renda do usuário, extrapolando o seu direito a tais dados.

Mesmo com sua edição tardia, este dispositivo torna-se uma conquista necessária ao país para se enquadrar nas demandas urgentes em relação à tecnologia que surge dia após dia. O fato de o legislativo nacional se atentar para tal aspecto demonstra uma intenção da nação em fazer parte da

---

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.

[20] Lei 12.965/14. Marco Civil da Internet. Capítulo 3, seção 2.

[21] Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
[...]
II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

comunidade de países que prezam pelos direitos de seus cidadãos. Apesar disso, o diploma legal se mostra insuficiente diante da realidade, uma vez que, por exemplo, fica silente em relação à responsabilidade civil sobre o vazamento de dados, fato comum em nossa vida cotidiana e de grande prejuízo para a dignidade da pessoa lesada.

2.4 O DECRETO Nº 8.771 DE 2016

O decreto 8.771/16 surgiu como um modo de complementar e preencher as lacunas do Marco Civil da Internet. De fato, sua intenção é de regulamentar aspectos de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, medidas de transparência na requisição de dados cadastrais pela administração pública e parâmetros para fiscalização e apuração de infrações[22].

Neste momento, cabe destacar dois principais aspectos abordados por este documento, quais sejam: a regulamentação da requisição de dados pessoais por parte do poder público aos provedores de serviço e os protocolos de segurança envolvendo tais dados.

Em seu art. 11[23], o dispositivo elenca o procedimento que a administração pública deve adotar para requisitar dados pessoais de indivíduos juntos aos provedores de serviço que armazenam tais dados. A motivação é um desses elementos, devendo, as requisições, ser fortemente fundamentadas, tanto legalmente como casualmente, em que se mostre visivelmente o interesse público na obtenção da informação. Tal requisito é necessário pois o direito ao sigilo da vida privada não pode, nem deve, ser transpassado de maneira arbitrária ou desmedida, ainda mais quando se trata da administração pública, responsável por manter os princípios constitucionais de legalidade, impessoalidade, moralidade, publicidade e eficiência em sua atuação.

---

[22] Decreto 8.771/16. Ementa.

[23] Art. 11. As autoridades administrativas a que se refere o art. 10, § 3º da Lei nº 12.965, de 2014, indicarão o fundamento legal de competência expressa para o acesso e a motivação para o pedido de acesso aos dados cadastrais.

É nesse sentido que caminha no art.12[24] da referida lei. As requisições administrativas de dados devem ser contabilizadas e constar em relatórios anuais de acesso público, de modo a permitir uma maior transparência da atividade pública.

Em um segundo momento, a legislação estabelece diretrizes a serem seguidas pelos provedores de acesso e pelos responsáveis pela guarda dos dados. No art. 13[25], podemos ver listadas: o estabelecimento da responsabilidade subjetiva no que diz respeito às pessoas que trabalham com esses dados, ou aquelas que possuem acesso a eles de alguma maneira, como forma de assegurar a reparação em caso de danos aos usuários. Também exige que tais pessoas possuam sistema de autenticação, para que seja identificado ou identificável o responsável pelo trato dos registros, além do uso de tecnologia de criptografia[26] para dificultar o acesso aos dados por *hackers*.

A despeito da edição deste decreto, o Marco Civil da Internet ainda possui diversas normas de eficácia limitada, pois exigem a regulamentação de lei posterior. Sendo assim, espera-se que o legislador continue encontrando formas de regulamentar as dinâmicas de comunicação digital como forma de promover a maior segurança das relações e a estabilidade das trocas de informações entre os atores desta.

2.5 OS PROJETOS DE LEI Nº 4.060/2012 E 330/2013

Seguindo a tendência de regulamentação iniciada pelo Marco Civil da Internet e pelo decreto anteriormente estudado, temos dois projetos de lei em tramitação nas duas casas do Congresso Nacional. Ambos, o projeto de lei 4.060 de 2012 da Câmara dos Deputados, proposto pelo Dep. Milton Monti e o projeto de lei 330 de 2013 do Senado, proposto pelo Senador Antonio Carlos Valadares, trazem diversas contribuições para o tema.

---

[24] Art. 12. A autoridade máxima de cada órgão da administração pública federal publicará anualmente em seu sítio na internet relatórios estatísticos de requisição de dados cadastrais[...].

[25] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as [..] diretrizes sobre padrões de segurança.

[26] Conjunto de princípios e técnicas empr. para cifrar a escrita, torná-la ininteligível para os que não tenham acesso às convenções combinadas; criptologia.

A primeira delas é a conceituação de “dados pessoais sensíveis”[27], sendo aqueles que vão além de meros dados cadastrais como nome, profissão e residência. Os dados sensíveis são aqueles que revelam o perfil psicológico ou comportamental do indivíduo, como cor, orientação sexual, religião, preferências politicas e que podem ser usados como forma de manipulação de opinião. São esses os dados mais valiosos no comercio de informações, pois são eles os capazes de impactar positiva ou negativamente nas relações comerciais, como uma campanha de marketing de uma determinada empresa, por exemplo. A carência de regulamentação especifica sobre o tema permite que empresas mal-intencionadas se utilizem de meios, muitas vezes fraudulentos, para obter informações sensíveis dos usuários e utilizá-las como forma de obter vantagem na competição com outras empresas, por mercado e consumidores.

Outro reforço normativo dos projetos é a inserção, no texto, de disciplina sobre responsabilidade civil, nesse caso, dos provedores de acesso sobre o conteúdo dos dados. Aqui se estabelece a responsabilidade objetiva, ou seja, sem averiguação de culpa, sobre os prejuízos decorrentes do tratamento irregular ou ilícito dos dados. Também se estabelece a responsabilidade solidária, quando a função do tratamento é compartilhada por mais de um proprietário ou quando o processo se desenvolve em mais de uma etapa por diferentes gestores. Nessa feita, dá-se a implementação de sanções administrativas sujeita aos infratores, podendo ser de multa, suspensão temporária da atividade, intervenção ou total interdição e proibição do desenvolvimento da atividade. Tais sanções não impede aplicação de outras previstas nos demais dispositivos da legislação, como a obrigação de indenizar a vítima do dano.

Conforme constatamos, o Brasil ainda encontra-se aquém do padrão de proteção ideal no que diz respeito a dados pessoais, apesar dos esforços neste sentido. Esperamos que os projetos de lei em tramitação consigam êxito em sua aprovação, pela emergência da regulamentação do enunciado.

---

[27] Art. 7º. Para os fins da presente lei, entende-se como:
[...]
IV - dados sensíveis: informações relativas à origem social e étnica, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas do titular;

3 CORTES SUPERIORES: O ENTENDIMENTO JURÍDICO BRASILEIRO

3.1 O SUPREMO TRIBUNAL FEDERAL

O Supremo Tribunal Federal (STF) em diversas oportunidades julgou casos referentes a direito digital e às relações virtuais. Destacaremos quatro deles para tentarmos retirar um entendimento do tribunal em relação ao tema.

O primeiro trata de repercussão geral[28] extraída do agravo 660.861/MG, de relatoria do Min. Luiz Fux[29]. Neste recurso, a recorrente *Google* questiona a sua condenação em danos morais por indenização devido ao conteúdo ofensivo publicado por terceiros em *sites* de seu domínio. Como argumento de defesa, a empresa se utilizou dos princípios da liberdade de expressão e da proibição de censura prévia, alegando que não seria razoável proceder a fiscalização do conteúdo que seus usuários publicam em seus *sites*, sob pena de afrontar tais princípios e, portanto, não poderia ser responsabilizada pelos danos causados pelas publicações.

Por outro lado, o tribunal não atendeu ao pedido da recorrente, sustentando a tese defendida no Código de Defesa do Consumidor, qual seja, a responsabilidade objetiva do fornecedor do serviço[30]. Nas palavras do relator, a alegação da recorrente não deve prosperar pois o prestador de serviço do site de relacionamento não exerce nenhum controle, nem mínimo, sobre o conteúdo ali veiculado, permitindo que mensagens agressivas e conteúdos violentos sejam publicados em seu domínio. Portanto, deve ser responsável pelos danos causados pelos mesmos, por assumir os riscos inerentes à

---

[28] Trata-se de conceito estabelecido pela emenda constitucional nº 45/2004, determinando a competência do STF, no julgamento de recursos extraordinários, às questões constitucionais com relevância social, política, econômica ou jurídica, que transcendam os interesses subjetivos da causa, auxiliando de forma que o tribunal não necessite julgar múltiplos casos sobre a mesma questão constitucional. Disponível em: <http://www.stf.jus.br/portal/cms/verTexto.asp?servico=jurisprudenciaRepercussaoGeral&pagina=apresentacao>. Acesso em: 5 jun. 2018.

[29] EMENTA: GOOGLE – REDES SOCIAIS – SITES DE RELACIONAMENTO – PUBLICAÇÃO DE MENSAGENS NA INTERNET – CONTEÚDO OFENSIVO – RESPONSABILIDADE CIVIL DO PROVEDOR – DANOS MORAIS – INDENIZAÇÃO – COLISÃO ENTRE LIBERDADE DE EXPRESSÃO E DE INFORMAÇÃO vs. DIREITO À PRIVACIDADE, À INTIMIDADE, À HONRA E À IMAGEM. REPERCUSSÃO GERAL RECONHECIDA PELO PLENÁRIO VIRTUAL DESTA CORTE.

[30] PEREIRA, Caio Mário da Silva. *Responsabilidade civil*. 9.ed. Rio de Janeiro: Forense, 2002.

atividade, tomando como parâmetro a responsabilidade objetiva prevista do Código de Defesa do Consumidor[31].

O segundo se desenvolve, também em repercussão geral, no agravo 652.777/SP[32], de relatoria do Min. Ayres Britto, em que o estado de São Paulo recorre de decisão que determina a retirada de informações de servidores públicos dos domínios eletrônicos de acesso público. Nesse caso, acontece o recorrente conflito entre interesse público e privado, assim como o de direitos fundamentais.

O acesso às contas públicas é condição para o exercício pleno da democracia, pois dá aos cidadãos o poder de fiscalizarem o uso de recursos públicos, como também a capacidade de investigar prováveis atos de corrupção. Já aos servidores é resguardado o direito ao sigilo de suas informações, como forma de proteção à intimidade e privacidade

Esta dinâmica ficou ainda mais conturbada com a edição da Lei de Acesso à Informação (Lei n.º 12.527/2011), que prevê, além da publicidade de nome, cargo, instituição e renda dos funcionários disponibilizados clara e publicamente para qualquer cidadão, a obrigação da administração pública proceder tal publicidade independentemente de demanda da população ou de prequestionamento. Neste terreno, a publicidade é a regra e o sigilo, a exceção.

O posicionamento do tribunal foi de que o interesse público, nesse caso, estava acima do interesse privado e as informações publicadas não excediam a competência do estado para tal, assim como assegura o relator: “[...]a remuneração bruta dos servidores, os cargos e funções por eles titularizados,

---

[31] Supremo Tribunal Federal. Acórdão de agravo provido para o reconhecimento da repercussão geral. Google Brasil Internet Ltda. e Aliandra Cleide Vieira. Repercussão geral no recurso extraordinário com agravo 660.861/Minas Gerais. Relator Ministro Luiz Fux. 22 de março de 2012. Disponível em: <http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=3058915>. Acesso em: 5 jun. 2018.

[32] EMENTA: CONSTITUCIONAL. ADMINISTRATIVO. DIVULGAÇÃO, EM SÍTIO ELETRÔNICO OFICIAL, DE INFORMAÇÕES ALUSIVAS A SERVIDORES PÚBLICOS. CONFLITO APARENTE DE NORMAS CONSTITUCIONAIS. DIREITO À INFORMAÇÃO DE ATOS ESTATAIS. PRINCÍPIO DA PUBLICIDADE ADMINISTRATIVA. PRIVACIDADE, INTIMIDADE E SEGURANÇA DE SERVIDORES PÚBLICOS.

os órgãos de sua formal lotação, tudo é constitutivo de informação de interesse coletivo ou geral”[33].

Passamos a análise do terceiro julgamento, sendo esse o *habeas corpus* 103.425/AM[34], de relatoria da Min. Rosa Weber. Aqui a questão aqui gira em torno do acesso a dispositivos de terceiros para obtenção de dados pessoais.

O recorrente defende que o acesso a dispositivos sem mandando judicial configura ilicitude pela violação do devido processo legal. A recorrida, em contrapartida, alega que as provas colhidas durante o processo se deram de forma legal, pois houve a anuência do proprietário do dispositivo para a coleta de tais dados e, uma vez publicados na *internet*, tais dados se tornam públicos.

O entendimento do tribunal acompanha o da recorrida, pois, uma vez que as informações coletadas estão disponibilizadas em dispositivo de uso comum, não cabe ao paciente direito sobre elas, não sendo proprietário desse dispositivo, sendo tratada como lícita a prova obtida por este meio. Não cabe igualmente ao paciente reclamar o direito à privacidade, uma vez que o mesmo disponibilizou o conteúdo questionado por sua própria vontade, tornando-o público. Afirma a Ex.ma Min. que não há que se falar em violação à privacidade uma vez que o paciente disponibilizou por vontade própria as comunicações com terceiros em foco, e esses agiram de forma a revela-las às autoridades, por seu teor criminoso, comparando a situação com o caso de alguém alegar violação à privacidade por carta enviada com ameaças a outrem, onde este comunicou-as às autoridades policiais[35].

---

[33] Supremo Tribunal Federal. Repercussão geral no recurso extraordinário com agravo 652.777/São Paulo. Município de São Paulo e Ana Maria Andreu Lacambra. Relator Ministro Ayres Britto. 29 de setembro de 2011. Disponível em:<http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=1902861>. Acesso em: 5 jun. 2018

[34] EMENTA: PROCESSO PENAL. HABEAS CORPUS. CRIME MILITAR. MENSAGENS CRIMINOSAS ENVIADAS PELA INTERNET. ACESSO AO CONTEÚDO DAS COMUNICAÇÕES DISPONIBILIZADO PELOS DESTINATÁRIOS. ACESSO AOS DADOS DE COMPUTADOR EM LAN HOUSE COM AUTORIZAÇÃO DO PROPRIETÁRIO JUDICIAL. INTERROGATÓRIO POR PRECATÓRIA. INVALIDADES NÃO RECONHECIDAS.

[35] Supremo Tribunal Federal. Habeas corpus 103.425/Amazonas. Efrain Santos da Costa e Defensoria Pública da União. Relatora ministra Rosa Weber. 26 de junho de 2012. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2541738. Acesso em: 5 jun 2018.

Por fim, o recurso extraordinário com agravo 756.917/SP[36], de relatoria do Min. Luiz Fux, se assemelha em partes ao julgado analisado anteriormente. Refere-se ao caso de publicação de fotografia contendo intimidade de pessoa alheia. O recorrente afirma que a prova obtida durante o processo é ilícita pela falta de anuência do produtor do conteúdo em disponibilizá-lo em juízo. Porém, como já mostrado, uma vez publicado o conteúdo em rede, a privacidade sobre aquele se torna nula. Assim considera o acórdão:

> [...]Fotografias que foram disponibilizadas voluntariamente pelos próprios autores na internet, permitindo-se o acesso irrestrito a todos os usuários da rede. Ausência de violação à intimidade e privacidade.[37]

Pela análise dos julgados apresentados, pode-se constatar que o Supremo Tribunal Federal se encontra em uma balança pendente: apesar de acertar em alguns casos, sua posição é de negar o direito à intimidade dos usuários da *internet* sobre seus dados pessoais, mesmo quando nitidamente esta proteção é devida. Por se tratar de um tribunal constitucional, tal posicionamento é esperado, uma vez que sua função é defender as bases constitucionais e principiológicas do Estado, uma função muitas vezes de manutenção do *status quo*. A recente judicialização de casos de conflitos envolvendo acesso a dados pessoais digitais ainda não foi capaz de causar uma mudança significativa no entendimento desta corte suprema, mas a expectativa é de que, no futuro, este tema seja levado mais a sério pelos guardiões da Constituição.

---

[36] EMENTA: AGRAVO REGIMENTAL NO RECURSO EXTRAORDINÁRIO COM AGRAVO. CIVIL. DANO MORAL. DIREITO DE IMAGEM. MATÉRIA COM REPERCUSSÃO GERAL REJEITADA PELO PLENÁRIO DO STF NO ARE Nº 739.382. CONTROVÉRSIA DE ÍNDOLE INFRACONSTITUCIONAL. SOBRESTAMENTO. PENDÊNCIA DE RECURSO NO SUPERIOR TRIBUNAL DE JUSTIÇA.

[37] Agravo Regimental no recurso extraordinário com agravo 756.917/São Paulo. Leonardo de Pinho Vieira, Marcus de Magalhães e Empresa Folha da manhã s/a. Relator ministro Luiz Fux. 29 de outubro de 2013. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=4872875. Acesso em: 5 jun 2018.

3.2 O SUPERIOR TRIBUNAL DE JUSTIÇA

No que concerne ao entendimento do Superior Tribunal de Justiça (STJ), vale, antes de tudo, ressaltar a notável decisão proferida no recurso especial nº 1.316.921/RJ[38], de relatoria da Min. Nancy Andrighi, na qual o tribunal equiparou os usuários da *internet* a consumidores, mesmo sem o caráter oneroso da relação. Nesta oportunidade, trataremos de quatro casos distintos envolvendo tráfego de dados na rede mundial de computadores, com o intuito de absorver algum entendimento concreto do tribunal, apesar da sua composição heterônoma.

De início, o recurso em mandado de segurança nº 55.019/DF[39], de relatoria do Min. Joel Ilan Paciornik, envolvendo a empresa *Yahoo* e o Ministério Público do Distrito Federal. O caso orbita em torno da obrigação da empresa em prestar informações que não estão sob sua guarda, uma vez que os servidores que armazenam informações de usuários que se encontram no exterior, ou seja, seria imprescindível a cooperação internacional neste caso, para a obtenção das informações requeridas, conforme a lei 12.965/2014 (Marco Civil da Internet).

No entanto, para o tribunal, o fato de a empresa possuir sede no Brasil, faz com que ela tenha a obrigação de se sujeitar às leis brasileiras e, portanto, a alegação de que a empresa situada no Brasil é apenas um braço de uma empresa maior situada no exterior, que possuí a simples função de alocar espaços publicitários e suportes de vendas, não a exime da obrigação de prestar informações solicitadas, até porque, como é sabido, tal tática de multinacionais que trabalham via *internet* visa burlar a carga tributária do país de origem e escapar de decisões judiciais que obriguem a prestação de informações. Uma vez possuindo sede no país, a multinacional submete-se a

---

[38] EMENTA: CIVIL E CONSUMIDOR. INTERNET. RELAÇÃO DE CONSUMO. INCIDÊNCIA DO CDC. GRATUIDADE DO SERVIÇO. INDIFERENÇA. PROVEDOR DE PESQUISA. FILTRAGEM PRÉVIA DAS BUSCAS. DESNECESSIDADE. RESTRIÇÃO DOS RESULTADOS. NÃO-CABIMENTO. CONTEÚDO PÚBLICO. DIREITO À INFORMAÇÃO.

[39] EMENTA: RECURSO ORDINÁRIO EM MANDADO DE SEGURANÇA. INQUÉRITO POLICIAL. QUEBRA DE SIGILO TELEMÁTICO. DESCUMPRIMENTO DE ORDEM JUDICIAL. ALEGAÇÕES DE AUSÊNCIA DE INDÍCIOS DE AUTORIA DELITIVA E DE VIOLAÇÃO A DIREITO DE TERCEIRO. NÃO CABIMENTO. APLICAÇÃO DE MULTA DIÁRIA. EMPRESA SITUADA NO PAÍS. SUBMISSÃO À LEGISLAÇÃO NACIONAL. MARCO CIVIL DA INTERNET. INCIDÊNCIA.

legislação brasileira, sendo, então, desnecessária a cooperação internacional para obtenção dos dados requisitados em juízo[40].

Nesse caso, dos dados pessoais dos usuários, mesmo que fisicamente armazenados no exterior, estariam sujeitos a jurisdição nacional, já que, além de o usuário emissor de tais dados se encontrar no Brasil, a empresa coletora é multinacional com filial instalada em solo brasileiro.

Para a segunda análise, temos o recurso em *habeas corpus* nº 75.800/PR[41], de relatoria do Min. Felix Fischer. Neste caso, o conflito se põe sobre a interpretação do art. 5º, XII da Constituição e sua abrangência para produção de prova penal. Segundo o relator, o direito ao sigilo não se estende aos dados armazenados em *smartphones* ou aparelhos celulares, pois a Constituição apenas protege a "comunicação entre dados, e não os dados em si, afastando também a incidência da lei 9.296/1996 (interceptação telefônica). Nas palavras do próprio, a Constituição Federal, em seu art. 5º, XII, não defende o sigilo das comunicações já armazenadas em dispositivos, mas tão somente aquelas em efetivo trânsito, o ato de comunicar-se. Na mesma feita, aduz que a lei 9.296/96 foi enfática na sua regulamentação do inciso acima em diferir a fluência da comunicação dos dados obtidos como consequência dos diálogos, onde apenas a integridade da conversação merece proteção e, por isso, não há vedação no conhecimento de material disponível em prova obtida de forma lícita, já que é facultado a cada interlocutor excluir tal material quando quisesse de seus dispositivos[42].

Neste momento percebe-se a patente visão positivista que muitos dos ministros presentes neste tribunal possuem, uma total ignorância à interpretação sistemática e axiológica da constituição, pondo mais valor no

---

[40] Superior Tribunal de Justiça. Recurso em mandado de segurança nº 55.019/Distrito Federal. Yahoo! do Brasil internet ltda., Distrito Federal e Ministério Público Federal. Relator ministro Joel Ilan Paciornik. 12 de dezembro de 2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1667238&num_registro=201702013432&data=20180201&formato=PDF. Acesso em: 5 jun 2018.

[41] EMENTA PROCESSUAL PENAL. OPERAÇÃO "LAVA-JATO". MANDADO DE BUSCA E APREENSÃO. APREENSÃO DE APARELHOS DE TELEFONE CELULAR. LEI 9296/96. OFENSA AO ART. 5º, XII, DA CONSTITUIÇÃO FEDERAL. INOCORRÊNCIA. DECISÃO FUNDAMENTADA QUE NÃO SE SUBORDINA AOS DITAMES DA LEI 9296/96. ACESSO AO CONTEÚDO DE MENSAGENS ARQUIVADAS NO APARELHO. POSSIBILIDADE. LICITUDE DA PROVA. RECURSO DESPROVIDO.

[42] Superior Tribunal de Justiça. Recurso em habeas corpus nº 75.800/Paraná. Ministério Público Federal. Relator ministro Felix Fischer. 15 de setembro de 2016. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2016/stj_50274979020164040000_15092016.pdf. Acesso em: 5 jun. 2018.

texto da norma do que na sua intenção, sem levar em conta o momento histórico em que foi elaborada. Além disso, por se tratar de peça constante da operação famosa conhecida como “Lava Jato”[43], vê-se o grande anseio punitivo da sociedade transcrito no voto do referido ministro, que não se freia em frente aos princípios constitucionais.

Numa terceira oportunidade, trazemos o recurso especial nº 1.660.168/RJ[44], de relatoria da Min. Nancy Andrighi. O caso se resume ao direito ao esquecimento, onde o autor almeja a retirada de termos de *sites* de pesquisa com o intuito de remover certo conteúdo ofensivo à sua honra dos domínios digitais públicos. O responsável pela pesquisa alega que não possui controle sobre o conteúdo dos endereços que aparecem na sua página, funcionando mais como um catálogo do que como um produtor de conteúdo em si, e que, portanto, não teria capacidade nem legitimidade para extrair tal conteúdo da rede.

Para a ministra, a exigência para que *sites* de pesquisa retirem conteúdo do ar é irrazoável, pois, não sendo eles detentores do domínio do mesmo, não há essa possibilidade. Caso feito, seria a instauração de um verdadeiro censor dentro do ambiente democrático digital. Para este efeito, seria necessário convocar os verdadeiros proprietários dos servidores em juízo, para que assim possa se pronunciar sobre a obrigação da retirada do conteúdo. Assim, defende que os provedores dos serviços devem agir de modo a resguardar o sigilo e a privacidade dos dados cadastrais dos seus usuários e das buscas por eles realizadas, assim como a manutenção do funcionamento do sistema, sendo desnecessária a filtragem de conteúdo das pesquisas feitas em seus domínios, já que esta não é uma obrigação inerente à atividade desempenhada. Acrescenta que o ordenamento brasileiro não prevê a possibilidade de imputar obrigação a terceiro sobre conteúdo pelo qual não tem

---

[43] Ação de investigação movida pela Policia Federal que investiga crimes de corrupção ativa, passiva, lavagem de dinheiro, entre outros, cometidos por políticos e associados de grande escalão no país.

[44] EMENTA: RECURSO ESPECIAL. DIREITO CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. 1. OMISSÃO, CONTRADIÇÃO OU OBSCURIDADE. AUSÊNCIA. 2. JULGAMENTO EXTRA PETITA . NÃO CONFIGURADO. 3. PROVEDOR DE APLICAÇÃO DE PESQUISA NA INTERNET . PROTEÇÃO A DADOS PESSOAIS. POSSIBILIDADE JURÍDICA DO PEDIDO. DESVINCULAÇÃO ENTRE NOME E RESULTADO DE PESQUISA. PECULIARIDADES FÁTICAS. CONCILIAÇÃO ENTRE O DIREITO INDIVIDUAL E O DIREITO COLETIVO À INFORMAÇÃO. 4. MULTA DIÁRIA APLICADA. VALOR INICIAL EXORBITANTE. REVISÃO EXCEPCIONAL. 5. RECURSO ESPECIAL PARCIALMENTE PROVIDO.

poder nem acesso, qual seja, cumprir a função de retirar as páginas com o conteúdo questionado da rede. Tal situação levaria a configuração de provedores sensores de conteúdo, decidindo quais informações deveriam ser ou não levadas a público, resultando numa situação perigosa ao direito devido à falta de regulamentação legal[45].

Apesar de acertada a decisão da ministra, seu voto foi vencido pelos demais, que, seja por falta de experiência com o tema, seja por desmedido apego ao texto das normas, se posicionaram a favor da parcialidade da *internet*. Dito isto, consideramos importante destacar o posicionamento do Min. Paulo de Tarso Sanseverino, no sentido de que o pedido não se trata de retirada de páginas da *internet* mas sim que, sendo feitas buscas pelo seu nome nos *sites* de pesquisa, o resultado ofensivo não seja o primeiro a aparecer como sugestão e que este seja colocado em posições de menor visibilidade para garantir o direito da autora de que aquela informação passada, não afete a sua vida no presente[46]. Traz uma inovação para a presente discussão, considerando a hipótese de que a autora na verdade não almejava a retirada do conteúdo dos *sites* em questão, mas sim do filtro da pesquisa, que mostrasse tais *sites* em posições menos favoráveis, e não como primeiros resultados, como vem acontecendo.

Em última análise, falaremos do recurso especial nº 1.348.532/SP[47], de relatoria do Min. Luis Felipe Salomão. Neste recurso, analisa-se a prática recorrente no meio financeiro, principalmente pelos bancos, de compartilhar dados pessoais de seus clientes com outras entidades financeiras, inclusive incluindo esta cláusula permissiva em seus contratos de adesão.

A possibilidade de compartilhar, ou não, seus dados pessoais com as instituições financeiras em si não caracteriza ilicitude, mas, a partir do momento em que o cliente se vê obrigado a aderir a um contrato com esta cláusula, sem

---

[45] Superior Tribunal de Justiça. Recurso Especial nº 1.660.168/ Rio de Janeiro. Yahoo! Brasil Internet ltda., Google Brasil Internet ltda. Relatora ministra Nacy Andrighi. 08 de maio de 2018. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2018/stj_02187678520098190001_08052018.pdf. Acesso em: 5 jun. 2018.

[46] *Ibidem*

[47] EMENTA: RECURSO ESPECIAL. CONSUMIDOR. CERCEAMENTO DE DEFESA. NÃO OCORRÊNCIA. CONTRATO DE CARTÃO DE CRÉDITO. CLÁUSULAS ABUSIVAS. COMPARTILHAMENTO DE DADOS PESSOAIS. NECESSIDADE DE OPÇÃO POR SUA NEGATIVA. DESRESPEITO AOS PRINCÍPIOS DA TRANSPARÊNCIA E CONFIANÇA. ABRANGÊNCIA DA SENTENÇA. ASTREINTES . RAZOABILIDADE.

a possibilidade de optar pelo compartilhamento ou pelo sigilo, fica configurado o abuso.

O entendimento do ministro relator é de que a impossibilidade da contratação do serviço sem a opção de não compartilhar seus dados pessoais é parte do problema. A vulnerabilidade advinda dessa coação expõe o consumidor de uma vulnerabilidade imensurável e improjetável, pois a partir da divulgação de seus dados abre-se uma janela para intromissões diversas em sua vida, conhecendo seus hábitos, sabendo de seus gastos e sua maneira de viver. Por isso é imprescindível a autorização espontânea para que tais dados sejam manipulados. Não suficiente, a cláusula é abusiva pois ela figura como condição para contratação do serviço, qual seja, a obtenção de crédito[48].

A posição do STJ acompanha a natureza da sua constituição, um tribunal essencialmente responsável por analisar a legalidade e os princípios infraconstitucionais, portanto, salvo exceções, estritamente legalista e limitado. Outro ponto que sustenta uma incoerência no entendimento do tribunal é a falta de uniformização das decisões das diferentes turmas que compõe o mesmo, tornando-o um tribunal mais subjetivo, quando deveria ser o contrário.

[48] Superior Tribunal de Justiça. Recurso Especial nº 1.348.532/ São Paulo. HSBC Bank Brasil s.a. e Associação Nacional de Defesa da Cidadania e do Consumidor – ANADEC. Relator ministro Luis Felipe Salomão. 10 de outubro de 2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1646430&num_registro=201202108054&data=20171130&formato=PDF. Acesso em: 5 jun. 2018.

4 DADOS PESSOAIS PELO MUNDO: O TEMA EM DIFENRENTES PAÍSES[49]

4.1 ESTADOS UNIDOS

Os Estados Unidos, como um país de história e essência liberal, prezam pela liberdade de seus cidadãos e isso se demonstra nas suas legislações. Apesar de não terem um diploma único que legisle sobre a proteção de dados pessoais, leis esparsas, federais e estaduais, nos dão uma ideia de como o assunto é tratado por lá. Neste país, a divisão entre o setor público e o privado, ou seja, entre as relações entre Estado e cidadãos e entre esses, é bem definida, de modo que as legislações aqui aplicadas seguem este mesmo modelo.

A primeira fonte que encontramos é o *Privacy Act* de 1974[50], que regulamenta de que forma as informações e dados sobre os indivíduos devem ser coletadas, armazenadas e tratadas pelas agências governamentais federais. Entre outras, esta lei estabelece que nenhuma agência poderia divulgar registros contidos em sistemas de registros por quaisquer meios de comunicação, a qualquer pessoa ou outras agências, exceto com um pedido escrito do proprietário dos dados, ou com o consentimento deste[51]. Além disso, tais agências são obrigadas a prestarem informações sobre quais dados possuem sobre determinado indivíduo, desde que o requerimento seja feito pelo próprio interessado. É possível notar o caráter eminente pessoal com que a matéria era tratada, ainda no século passado, dando total poder de decisão ao indivíduo. Existem algumas exceções a esta regra (como o uso desses dados para propósitos estatísticos), mas tal falto não fere a unidade do princípio posto.

---

[49] Dados colhidos em consulta ao *site* Pensando o Direito, em pesquisa realizada pela Divisão da Sociedade da Informação do Ministério das Relações Exteriores, componente do debate público sobre o projeto de lei de proteção a dados pessoais, da Secretaria de Assuntos Legislativos e da Secretária Nacional do Consumidor do Ministério da Justiça, disponível em: http://pensando.mj.gov.br/dadospessoais/. Acesso em: 5 jun. 2018.

[50] Estados Unidos da América. *Públic Law 93-579 - Privacy Act.* 31 de dezembro de 1974. Disponível em: https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf. Acesso em: 5 jun. 2018.

[51] *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains*.

No mesmo sentido disciplina o *Freedom of Information Act* de 1966[52], sendo esse uma lei de caráter mais regulamentar, especificando de que modo a divulgação de informações deve ser feita e propondo sanções para aquelas agências que não cumprirem com o ordenamento legal, pela instauração de um conselho especial que decidirá sobre qual processo disciplinar se instaurará contra o servidor ou empregado que foi responsável pela negativa[53].

No tocante às relações privadas, destaca-se a atuação da *Federal Trade Comission* (FTC) no sentido de fiscalizar a atuação das empresas nos mais diversos aspectos, inclusive no manejo dos dados pessoais de seus clientes. Sua fundação se dá pelo *Federal Trade Comission Act*[54] de 2006, que, dentre outros, estabelece a proibição de qualquer de seus empregados de divulgarem informações tanto de empresas quanto de indivíduos[55].

4.2 UNIÃO EUROPEIA

A comunidade europeia é, no ocidente, o primeiro lugar no quesito de proteção de dados pessoais. Como a vanguarda da vida contemporânea, a União Europeia está sempre à frente das evoluções sociais, principalmente no que diz respeito aos direitos humanos e direitos fundamentais.

Aqui, vemos a destacada posição da Diretiva nº 95/45/EC[56] de 1995, relativa a proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Este documento vem a estabelecer as bases do tratamento de dados no mundo e com ele a consagração do princípio do direito à privacidade, interpretado como um direito humano fundamental, de exímia rigidez e que as implicações de sua violação

---

[52] Estados Unidos da América. *Public Law 89-487 – Freedom of Information* Act. 04 de julho de 1966. Disponível em: https://catalog.archives.gov/id/299930. Acesso em: 5 jun. 2018

[53] *If agency personnel acted arbitrarily or capriciously with respect to the withholding, Special Counsel shall promptly initiate a proceeding to determine whether disciplinary action is warranted against the officer or employee who was primarily responsible for the withholding.*

[54] Estados Unidos da América. *Federal Trade Comission Act.* Disponível em: https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf. Acesso em: 5 jun. 2018.

[55] *No officer or employee of the Commission or any Commissioner may publish or disclose information to the public, or to any Federal agency, whereby any line-of-business data furnished by a particular establishment or individual can be identified.*

[56] Jornal Oficial das Comunidades Europeias. Directiva 95/46/CE do parlamento europeu e do conselho de 24 de outubro de 1995. 23 de novembro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 5 jun. 2018.

são tão severas quanto as dos demais direitos, como a vida, propriedade e liberdade, sendo necessária densa fundamentação para que seja restringido. Diferentemente do que acontece no Brasil, onde tal princípio, apesar de presente, possui uma menor relevância normativa e hermenêutica.

O capítulo sobre legitimidade do tratamento de dados é singular dentre as legislações sobre o tema no mundo. Quando muitos procuram dar fundamentação à violação da privacidade por meio do acesso aos dados pessoais, esta diretiva estabelece condições para que o tratamento de dados seja válido, caso contrário, deve se abster[57].

Nesta ocasião vale destacar também o art. 12[58] da Declaração Universal dos Direitos do Homem, que, apesar do título, se destina a todos os seres humanos. Nele, se estabelece o princípio universal do direito à privacidade, servindo de parâmetro para elaboração dos diversos diplomas legais aqui elencados.

4.3 JAPÃO

O país asiático segue o exemplo da União Europeia e possui uma densa legislação sobre o tema de proteção de dados pessoais de seus cidadãos. O ato nº 57 de 2003 (*Act on the Protection of Personal Information*) possui diversas semelhanças com a diretiva nº 95/45/EC, no que concerne ao estabelecimento de princípios no tratamento de dados, nos direitos dos usuários de sigilo e privacidade e a responsabilidade dos provedores de acesso.

---

[57] Os Estados-membros estabelecerão que o tratamento de dados pessoais só poderá ser efectuado se : a) A pessoa em causa tiver dado de forma inequívoca o seu consentimento; ou b) O tratamento for necessário para a execução de um contrato no qual a pessoa em causa é parte ou de diligências prévias à formação do contrato decididas a pedido da pessoa em causa ; ou c) O tratamento for necessário para cumprir uma obrigação legal à qual o responsável pelo tratamento esteja sujeito; ou d) O tratamento for necessário para a protecção de interesses vitais da pessoa em causa ; ou e) O tratamento for necessário para a execução de uma missão de interesse público ou o exercício da autoridade pública de que é investido o responsável pelo tratamento ou um terceiro a quem os dados sejam comunicados; ou f) O tratamento for necessário para prosseguir interesses legítimos do responsável pelo tratamento ou do terceiro ou terceiros a quem os dados sejam comunicados, desde que não prevaleçam os interesses ou os direitos e liberdades fundamentais da pessoa em causa , protegidos ao abrigo do n " 1 do artigo 1 " (vida privada).

[58] Artigo 12 Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques a sua honra e reputação. Todo o homem tem direito à proteção da lei contra tais interferências ou ataques.

No entanto, um ponto importante a se destacar nesta legislação é a cominação de multas em valores específicos como forma de sanção para aqueles que descumpram os preceitos estabelecidos neste documento. A multa tem um caráter não criminal e não pode exceder a quantia de 100.000 ienes (cem mil ienes, o equivalente a, aproximadamente, R$ 3.257,00 em 2018), tanto para as empresas quanto para os empregados[59].

Além disso, todas as empresas que tenham informações de mais de cinco mil pessoas ficam obrigadas por lei a comunicar os seus clientes sobre o armazenamento desses dados e sobre o deles, para os fins estabelecidos ou para fins diversos dos originais.

4.4 ARGENTINA

O país vizinho, ao contrário do Brasil, possui legislação específica sobre o tema. A lei 25.326 de 2000, de proteção a dados pessoais, cujo fim é o de regulamentar a proteção integral desses dados, disponíveis em arquivos, registros, bancos de dados públicos e privados para garantir a honra e a intimidade das pessoas. A Direção Nacional de Proteção de Dados Pessoais[60] (em espanhol, PDP), órgão vinculado ao Ministério de Justiça e Direitos Humanos argentino, é o ente responsável, desde 2003, pela aplicação dessa lei. A atuação da PDP é desvinculada da ação dos órgãos de defesa do consumidor, embora alguns casos, como utilização de dados pessoais para fins comerciais, possam criar situações para a atuação de órgãos pertencentes tanto à proteção de dados pessoais quanto à de defesa dos consumidores. A denúncia e as inspeções são os instrumentos utilizados pela PDP para certificar-se do cumprimento da lei. A Disposição 11/2006, da PDP, estabelece, ainda, medidas de segurança que devem ser seguidas para o tratamento e a conservação de dados pessoais contidos em arquivos, registros e bancos de dados públicos e privados.

---

[59] *Article 88 A person falling under any of each following item shall be punished by a non-criminal fine of not more than 100,000 yen.*
(i) a person who has violated the provisions of Article 26, paragraph (2), or Article 55
(ii) a person who failed to submit a notification or did falsely submit a notification under the provisions of Article 50, paragraph (1).

[60] *Dirección Nacional de Protección de Datos Personales.*

4.5 MÉXICO

A legislação mexicana é uma das poucas que contêm disposição sobre proteção de dados logo em sua lei originária. A Constituição Mexicana de 1917, em seu art. 6º, garante o direito de acesso às tecnologias da informação e comunicação, incluídos aí, o acesso a *internet*, radiodifusão e telecomunicação[61]. Já em seu art. 16, a proteção constitucional é prontamente estabelecida a partir do direito de todas as pessoas ao acesso, retificação e cancelamento de seus dados pessoais, assim como se opor ao seu uso em casos que não envolvam segurança nacional, saúde pública ou direitos de terceiros[62].

Adicionalmente, também possui legislação especial sobre o assunto, a *ley federal de protección de datos personales en posesión de los particulares*, que trata de regulamentar o art. 16 da Constituição citada anteriormente, estabelecendo os meios de exercício do direito, as exceções à validade do mesmo.

As legislações sobre dados no mundo formam um verdadeiro mosaico: porquanto os países da União Europeia contam com uma rigorosa normativa sobre o assunto, países como os Estados Unidos, palco dos acontecimentos retratados neste trabalho, resistem em dar atenção séria ao tema.

---

[61] *Artículo 6º El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios.*

[62] *Artículo 16 Toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de los mismos, así como a manifestar su oposición, en los términos que fije la ley, la cual establecerá los supuestos de excepción a los principios que rijan el tratamiento de datos, por razones de seguridad nacional, disposiciones de orden público, seguridad y salud públicas o para proteger los derechos de terceiros.*

5 ESTUDO DE CASO: CASO *FACEBOOK & CAMBRYGE ANALITCA* E O PERIGO DA FALTA DE REGULAMENTAÇÃO[63]

Em 17 de março de 2018, dois jornais mundialmente conhecidos, o americano *The New York Times* e o britânico *The Guardian*, publicaram longas matérias expondo o uso indevido de dados pessoais pela rede social *Facebook*, sob a suspeita de ter influenciado o resultado das eleições presidenciais dos Estados Unidos em 2016. A responsável pela coleta de tais dados foi a empresa *Cambridge Analytica*, a partir do uso de aplicativos de testes psicológicos. O responsável pela delação foi Christopher Wylie, ex-funcionário da empresa.

Neste caso, os usuários eram convidados a participar de testes de personalidade utilizando um aplicativo desenvolvido por Aleksandr Kogan, pesquisador da Universidade de Cambridge, e conectado ao perfil do *Facebook*, pedindo permissão para coleta de dados dos usuários para fins acadêmicos. Até o presente momento, não se constata nenhum ilegalidade no caso, pois é de comum hábito que dados sejam coletados pelas diferentes formas para fins estatísticos ou de estudo, desde que haja consentimento do interessado.

A grande questão está em como estes dados foram utilizados a partir da coleta: sem a permissão dos usuários, o aplicativo de Kogan teve acesso aos dados sobre amigos deles, que, por óbvio, não eram capazes de consentir com tal ação. Além disso, todo o material foi vendido à empresa *Cambridge Analytica*, que atua no mercado americano com marketing eleitoral, utilizando disso para promover mensagens personalizadas aos eleitores com base nas suas informações, com o intuito de convencê-los sobre a preferência de um candidato em detrimento de outro, nas eleições presidenciais dos Estados Unidos, e assim influenciar no seu resultado.

O *Facebook*, apesar de não ter tido envolvimento direto no caso, é também responsável por permitir que dispositivos de terceiros tenham acesso

[63] Globo. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml. Acesso em: 5 jun. 2018.

irrestrito aos dados de seus usuários, utilizando de brechas nos termos de adesão e permissão, que, por serem tão extensos, geralmente não são lidos. A empresa já enfrentava queixas anteriores de usuários que suspeitavam do uso indevidos dos seus dados armazenados.

Em 2011, *Facebook* e a *Federal Trade Comission* (FTC) realizaram um acordo em que a rede social se comprometia a ser mais transparente e honesta com seus usuários sobre como seus dados seriam armazenados, compartilhados e segurados, restringindo o seu acesso a terceiros. Os acontecimentos envolvendo a *Cambridge Analytica* revelaram a falta de esforços da empresa em cumprir com o acordo, o que pode levar a multas milionárias.

O choque na economia dos Estados Unidos foi sentido na diminuição do valor da empresa no mercado de ações, que chegou a marca de 95 bilhões de dólares nas semanas seguintes ao escândalo. As consequências desta mudança abrupta já foram sentidas no país, como também no mundo inteiro, na crise imobiliária de 2008.

A repercussão do caso foi tamanha que diversas empresas de tecnologia se viram obrigadas a alterar os seus termos de uso, de modo a deixa-los mais claros e acessíveis sobre como os dados dos usuários são coletados e tratados e para quais fins. Esta decisão, apesar de beneficiar os usuários com maior clareza nas informações, é uma forma de defesa das empresas contra possíveis ações judiciais futuras, cobrando indenizações sobre uso indevido de dados.

Destacamos a criação do projeto de lei do senado americano *Honest Ads Act*, que, dentro outros, estabelece uma maior transparência no uso de dados pessoais para veiculação de publicidade e marketing individualizado.

No Brasil, a atuação da *Cambridge Analytica* deu ensejo a instauração de um inquérito civil por parte do Ministério Público do Distrito Federal e Territórios (MPDFT)[64] para apurar o uso de dados pessoais de cidadãos brasileiros sem o seu consentimento e para fins comerciais, considerando este caso como um dos maiores incidentes de falha de segurança no mundo.

[64] Ministério Público do Distrito Federal e Territórios. Portaria 02/2018 MPDFT. Disponível em: http://www.mpdft.mp.br/portal/pdf/noticias/Mar%C3%A7o_2018/Instauracao_de_ICP_Cambridge_Analytica.pdf. Acesso em: 5 jun. 2018.

Nesse aspecto, a atuação do MPDFT se mostra avançada, pela criação de uma comissão de proteção de dados pessoais, a primeira no país a tratar especificamente sobre o assunto. Foi instituída pela portaria normativa nº 539 de 2018 e tem sete pilares básicos de atuação: (i) opinativo, sugerindo diretrizes para uma Política Nacional de Proteção dos Dados Pessoais e Privacidade; (ii) informativo, promovendo entre a população, empresas e órgãos públicos o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e privacidade, bem como medidas de segurança; (iii) estudos, promovendo estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade; (iv) cooperativo, incentivando ações de cooperação com autoridade de proteção de dados pessoais de outros países, de natureza internacional ou transnacional; (v) notificativo, recebendo comunicações sobre a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares dos dados; (vl) sancionador, propondo ações judiciais visando à aplicação das sanções previstas no artigo 12, da Lei nº 12.965/14 - Marco Civil da Internet, em conjunto com o promotor natural; e (vii) investigativo, instaurando procedimento preparatório, inquérito civil público e procedimento administrativo.

Aqui, assim como nos EUA, não há um órgão fiscalizador de atividades *online*. Caso o evento tivesse ocorrido em terras brasileiras, provavelmente seria tratado como um caso de direito do consumidor, sendo de reponsabilidade dos Programas de Proteção de Defesa do Consumidor (PROCON's) e do Ministério Público, por ser o legitimado para defender os interesses coletivos dos cidadãos.

Por enquanto, casos semelhantes são resolvidos em litigâncias esparsas pelo país. À título de exemplificação, temos a apelação cível 70074475153/RS[65], em que o autor pede indenização contra o *Facebook* por compartilhar suas informações com aplicativo externo. O aplicativo em questão

[65] EMENTA: APELAÇÃO CIVEL. REPONSABILIDADE CIVIL. PEDIDO DE IDENIZAÇÃO POR DANOS MORAIS. AÇÃO PROPOSTA CONTRA O FACEBOOK E LULUVISE INCORPORATION. DESISTÊNCIA DA AÇÃO EM FACE DE LULUVISE. INEXITÊNCIA DE ATO ILÍCITO COMETIDO PELO FACEBOOK. DADOS UTILIZADOS POR APLICATIVO SOBRE O QUAL O APELADO FACEBOOK NÃO POSSUÍ INGERÊNCIA. ALEGAÇÃO DE INDEVIDO COMPARTILHAMENTO DE DADOS QUE NÃO SE SUSTENTA. DADOS PÚBLICOS, NOS TERMOS DA POLÍTICA DE PRIVACIDADE DA REDE SOCIAL. AUTOR QUE NÃO LOGROU DEMONSTRAR OS REQUISITOS DA RESPONSABILIDADE CIVIL, ÔNUS QUE LHE CABIA. APELO NÃO PROVIDO.

era o *Lulu*, que coletava informações públicas dos perfis dos participantes e atribuía notas às suas características físicas e personalidade, permitindo aos usuários comentar os perfis de cada um, muitas vezes submetendo a pessoa a constrangimento público sem sequer o seu conhecimento.

O Tribunal de Justiça do Rio Grande do Sul não acolheu o pedido do autor, sob o fundamento de que se tratavam de informações públicas que o próprio disponibilizou na rede social, então não havia de se falar em vazamento, ignorando completamente o fato de que os dados disponibilizados tem um fim especifico e, neste caso, foram utilizados com fim diverso do original, atuando até mesmo contra o portados desses dados.

A análise deste caso nos mostra as consequências da inexistência de uma política de proteção de dados solidificada e a capacidade de eventos como este ultrapassarem as barreiras individuais e afetarem milhões de pessoas ao redor do mundo.

As informações sobre dados pessoais estão tomando o lugar do petróleo como mercadoria mais valiosa do mercado. É como no dito popular: não há almoço grátis. A oferta de serviços aparentemente grátis na *internet* esconde cláusulas contratuais e termos de serviço que exigem a permissão do usuário para comercializar seus dados. Pela continuidade do negócio, o interesse das empresas é coletar a maior quantidade possível de dados e fazer com eles o que bem entenderem.

Os riscos são inúmeros e afetam todos nós. O primeiro prejuízo da coleta, guarda e comercialização ou compartilhamento dos nossos dados pessoais de maneira desregulada é para a privacidade das/os cidadãos/ãs. O que está em jogo é o direito de escolher autonomamente o que queremos compartilhar e com quem. E não se trata de querer esconder algo, mas de poder decidir o que você quer divulgar ou não. Além disso, a coleta e venda desregulada dos dados pessoais é um perigo para a liberdade. Ao gerir nossos dados, as empresas ganham controle sobre nossas vidas. Com base nisso, ficamos expostos a inúmeras propagandas direcionadas, juntas de diversos “filtros” discriminatórios na hora de contratar um serviço ou acessar um direito e podemos ter a liberdade de expressão cerceada.

Proteger os dados pessoais é proteger as pessoas. Empresas e instituições não podem coletar ou comercializar seus dados sem

consentimento. As informações registradas não podem ser para além daquilo que foi pedido, e todos nós, usuárias e usuários, temos de ter disponíveis formas de saber quais dados são retidos e, a qualquer momento, desistir da permissão. Para isto, é preciso que haja uma autoridade pública que fiscalize essas garantias e evite violações e abusos.

6 CONCLUSÃO

Os resultados da pesquisa nos mostram que a posição que o Brasil ocupa no cenário de proteção de dados pessoais digitais no mundo é intermediária: apesar de possuir legislação no tocante ao tema, essa não aborda todos os pontos necessários para sua devida regulamentação.

A Constituição Federal carece de emenda constitucional que englobe o acesso aos meios digitais como direito fundamental, apesar de já ser possível retirar esta interpretação do texto constitucional. Assim como em outros assuntos de grande relevância, como no caso da união homoafetiva, é delegado ao Supremo Tribunal Federal o papel de preencher esta lacuna na norma originária.

A atualização das diversas leis também é imprescindível, pois em nenhum momento há a recepção das novas formas de interação social envolvendo meios digitais e, consequentemente, troca de dados. Por ser, hoje, a *internet*, o maior e mais abrangente meio de comunicação, com tendência de crescimento à medida que novas gerações surgem, não é prudente que o poder legislativo se escuse da sua função primordial, qual seja acompanhar as transformações sociais e os anseios da população.

Ademais, a legislação sobre uso da rede digital, nomeadamente o Marco Civil da Internet e posteriores regulamentações, não cumpre com o objetivo principal de sua criação que é conferir segurança jurídica para as relações virtuais e diminuir o efeito “terra de ninguém” que se atribuí à *internet*. É necessário o decurso do tempo e da judicialização de casos com fundamento legal nestes dispositivos para que sua eficácia plena seja analisada.

Quanto à posição das cortes superiores, vê-se uma lenta mudança na posição adotada por seus ministros. Talvez pela desconfiança nos meios digitais ou pela sua recente história, a tendência era de se desconsiderar os direitos daqueles que utilizavam este meio de comunicação. Porém, com o crescimento exponencial de usuários nos últimos anos, a relevância da comunicação por redes digitais se tornou forte o suficiente para transformar o pensamento dos juristas nacionais, de modo que, hoje, já é possível se falar em equiparação de direito a privacidade digital ao direito à inviolabilidade do domicílio, ambos de grande importância.

A renovação das legislações sobre dados pelo mundo, encabeçada pela União Europeia, segue uma inclinação internacional de adaptação às novas dinâmicas de comunicação. Atualmente, o cenário internacional encontra-se em transição: países com legislação concreta sobre proteção de usuários digitais, como é o caso da já citada, países que possuem legislação sobre dados, mas de maneira ineficiente, como é o caso do Brasil, e países que não possuem nenhuma legislação sobre o tema, como os Estados Unidos. Acreditamos que, pela observação da história, todos os temas de grande importância no mundo requerem tempo para serem incorporados aos valores de uma sociedade, então esperamos que no futuro este cenário seja diferente.

Não obstante, ainda temos o problema ético envolvido de como garantir o sigilo e a privacidade de dados pessoais, se os mesmos são publicados por vontade própria dos usuários O caso analisado nos mostra que este limite não está bem definido e que, antes de tudo, é necessário a discussão ampla sobre o tema.

REFERÊNCIAS

ALEXY, Robert. Teoria dos Direitos Fundamentais. Tradução de Virgílio Afonso da Silva. São Paulo: Malheiros, 2009.

Argentina. Lei 25.326. *Ley de Protección de los Datos Personales*. Disponível em: http://www.migliorisiabogados.com/wp-content/uploads/2012/06/LEY-25326.docx. Acesso em: 6 jun. 2018.

ASCENSÃO, José de Oliveira. Estudos sobre direito da Internet e sociedade da informação. Coimbra, 2001.

BARROSO, Luís Roberto. Curso de Direito Constitucional Contemporâneo: os conceitos fundamentais e a construção do novo modelo. 3ª ed. – São Paulo: Saraiva, 2011.

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

_____. Lei nº 12.965 de 23 de abr. de 2014. Marco Civil da Internet. Brasília, DF. abr. 2014.

_____. Decreto nº 8.771 de 11 de maio de 2016. Regulamenta a Lei nº 12.965. Brasília, DF. maio, 2016.

_____. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Brasília, DF. jan. 2002.

_____. Decreto-lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Brasília, DF. dez. 1940.

_____. Lei nº 8.078, de 11 de setembro de 1990. Código de Defesa do Consumidor. Brasília, DF. set. 1990.

_____. Lei nº 12.527, de 18 de novembro de 2011. Lei de acesso a informação. Brasília, DF. nov. 2011.

Câmara dos Deputados. Projeto de lei da câmara nº 4060/2012. Disponível em: http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra?codteor=1001750&filename=PL+4060/2012. Acesso em: 6 jun. 2018.

CONSALTER, Zilda Mara – Direito ao esquecimento: proteção da intimidade e ambiente virtual. Curtiba: Juruá, 2017.

Declaração Universal dos Direitos do Homem. Disponível em: http://pfdc.pgr.mpf.mp.br/atuacao-e-conteudos-de-apoio/legislacao/direitos-humanos/declar_dir_homem.pdf. Acesso em: 6 jun. 2018.

DIMOULIS, Dimitri; MARTINS, Leonardo. Teoria geral dos direitos fundamentais. 5. ed. rev., atual. e ampl. – São Paulo: Atlas, 2014.

Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. BBC. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 6 jun. 2018.

Estados Unidos da América. *Públic Law 93-579 - Privacy Act.* 31 de dezembro de 1974. Disponível em: https://www.gpo.gov/fdsys/pkg/STATUTE-88/pdf/STATUTE-88-Pg1896.pdf. Acesso em: 5 jun. 2018.

_____. *Public Law 89-487 – Freedom of Information* Act. 04 de julho de 1966. Disponível em: https://catalog.archives.gov/id/299930. Acesso em: 5 jun. 2018

_____. *Federal Trade Comission Act.* Disponível em: https://www.ftc.gov/sites/default/files/documents/statutes/federal-trade-commission-act/ftc_act_incorporatingus_safe_web_act.pdf. Acesso em: 5 jun. 2018.

Facebook stock drops after reports of FTC probe and UK summons of Zuckerberg in data scandal. CNBC. Disponível em: https://www.cnbc.com/2018/03/20/ftc-reportedly-to-investigate-facebooks-use-of-personal-data.html. Acesso em: 6 jun. 2018.

Japão. *Act* Nº. 57 de 30 maio de 2003. *Act on the Protection of Personal Information.* Disponível em: http://www.japaneselawtranslation.go.jp/law/detail/?printID=&ft=5&re=02&dn=1&gn=99&sy=2003&ht=A&no=57&x=58&y=14&ia=03&ky=&page=1&vm=02. Acesso em: 6 jun. 2018.

Jornal Oficial das Comunidades Europeias. Directiva 95/46/CE do parlamento europeu e do conselho de 24 de outubro de 1995. 23 de novembro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT. Acesso em: 5 jun. 2018.

Lei 'Carolina Dieckmann', que pune invasão de PCs, entra em vigor. Globo. Disponível em: http://g1.globo.com/tecnologia/noticia/2013/04/lei-carolina-dieckmann-que-pune-invasao-de-pcs-passa-valer-amanha.html. Acesso em: 6 jun. 2018.

LIMA, Glaydson de Farias. Manual de Direito Digital: fundamentos, legislação e jurisprudência. 1. ed. Curitiba: Appris. 2016

LIMA NETO, José Henrique Barbosa Moreira. Da Inviolabilidade de dados: inconstitucionalidade da Lei 9296/96. (Lei de interceptação de comunicações telefônicas). Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 2, n. 14, 1 jun. 1997. Disponível em: <https://jus.com.br/artigos/197>. Acesso em: 5 jun. 2018.

México. Constituição Mexicana. Disponível em: http://www.diputados.gob.mx/LeyesBiblio/pdf/1_150917.pdf. Acesso em: 6 jun. 2018. Acesso em: 6 jun. 2018.

_____. *Ley federal de protección de datos personales en posesión de los particulares* de 5 de jul. de 2010. disponível em: http://www.diputados.gob.mx/leyesbiblio/pdf/lfpdppp.pdf. acesso em: 6 jun. 2018.

Ministério Público do Distrito Federal e Territórios. Portaria 02/2018 MPDF. Disponível em: http://www.mpdft.mp.br/portal/pdf/noticias/Mar%C3%A7o_2018/Instauracao_de_ICP_Cambridge_Analytica.pdf. Acesso em: 6 jun. 2018.

MORAES, Alexandre de. Direitos humanos fundamentais: Teoria Geral. 4ªed. São Paulo: Atlas, 2002.

PEREIRA, Caio Mário da Silva. Responsabilidade civil. 9.ed. Rio de Janeiro: Forense, 2002.

REALE, Miguel. Teoria Tridimensional do Direito. 5ª ed., Editora Saraiva, São Paulo, 2003.

Senado Federal. Projeto de lei do senado nº 330/2013. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=2931559&ts=1529326765038&disposition=inline&ts=1529326765038. Acesso em: 6 jun. 2018.

Superior Tribunal de Justiça. Recurso em mandado de segurança nº 55.019/Distrito Federal. Yahoo! do Brasil internet ltda., Distrito Federal e Ministério Público Federal. Relator ministro Joel Ilan Paciornik. 12 de dezembro de 2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1667238&num_registro=201702013432&data=20180201&formato=PDF. Acesso em: 5 jun 2018.

Superior Tribunal de Justiça. Recurso em habeas corpus nº 75.800/Paraná. Ministério Público Federal. Relator ministro Felix Fischer. 15 de setembro de 2016. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2016/stj_50274979020164040000_15092016.pdf. Acesso em: 5 jun. 2018.

Superior Tribunal de Justiça. Recurso Especial nº 1.660.168/ Rio de Janeiro. Yahoo! Brasil Internet ltda., Google Brasil Internet ltda. Relatora ministra Nacy Andrighi. 08 de maio de 2018. Disponível em: http://www.omci.org.br/m/jurisprudencias/arquivos/2018/stj_02187678520098190001_08052018.pdf. Acesso em: 5 jun. 2018.

Superior Tribunal de Justiça. Recurso Especial nº 1.348.532/ São Paulo. HSBC Bank Brasil s.a. e Associação Nacional de Defesa da Cidadania e do Consumidor – ANADEC. Relator ministro Luis Felipe Salomão. 10 de outubro de 2017. Disponível em: https://ww2.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=1646430&num_registro=201202108054&data=20171130&formato=PDF. Acesso em: 5 jun. 2018.

Supremo Tribunal Federal. Acórdão de agravo provido para o reconhecimento da repercussão geral. Google Brasil Internet Ltda. e Aliandra Cleide Vieira. Repercussão geral no recurso extraordinário com agravo 660.861/Minas Gerais. Relator Ministro Luiz Fux. 22 de março de 2012b. Disponível em: < http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=3058915>. Acesso em: 6 jun. 2018.

Supremo Tribunal Federal. Acórdão de agravo provido para o reconhecimento da repercussão geral. Município de São Paulo e Ana Marcia Andreu Lacambra. Repercussão geral no recurso extraordinário com agravo 652.777/São Paulo. Relator Ministro Ayres Britto. 29 de setembro de 2011a. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=1902861. Acesso em: 6 jun. 2018.

Supremo Tribunal Federal. Agravo regimental desprovido. Leonardo de Pinho Vieira, Marcus de Magalhães e Empresa Folha da Manhã S/A. Agravo regimental no Recurso Extraordinário com Agravo 756.917/São Paulo. Relator Ministro Luiz Fux. Julgado em 29 de outubro de 2013b. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=4872875. Acesso em: 6 jun. 2018.

Supremo Tribunal Federal. Ordem denegada em Habeas Corpus. Efrain Santos da Costa e Superior Tribunal Militar. Habeas Corpus 103.425/Amazonas. Relatora Ministra Rosa Weber. 26 de junho de 2012c. Disponível em: http://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=2541738. Acesso em: 6 jun. 2018.

Supremo Tribunal Federal. Sobre a repercussão geral. Disponível em: http://www.stf.jus.br/portal/cms/verTexto.asp?servico=jurisprudenciaRepercussaoGeral&pagina=apresentacao. Acesso em: 6 jun. 2018.