XIX encontro nacional de pesquisa em ciência da informação
ENANCIB
// SUJEITO INFORMACIONAL E AS PERSPECTIVAS ATUAIS EM CIÊNCIA DA INFORMAÇÃO. //
22-26 OUTUBRO 2018
LONDRINA/PR
Universidade Estadual de Londrina

XIX ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO – ENANCIB 2018

GT-05 – Política e Economia da Informação

A POLÍTICA DE INFORMAÇÃO NA ARENA DA PRIVACIDADE DOS DADOS PESSOAIS

Daniela Assis Alves Ferreira (Fundação Mineira de Educação e Cultura)

Rodrigo Moreno Marques (Fundação Mineira de Educação e Cultura)

Alexandra Natale (Fundação Mineira de Educação e Cultura)

INFORMATION POLICY IN THE ARENA OF PRIVATE DATA PROTECTION

Modalidade da Apresentação: Comunicação Oral

Resumo: O tema privacidade e proteção de dados pessoais têm ganhado relevância, principalmente diante de tantos escândalos de vazamento e venda de dados pessoais que têm sido noticiados. Neste artigo, adota-se a política de informação como eixo condutor de uma discussão que tem como objetivo analisar como o direito à privacidade e à proteção de dados pessoais tem sido tratado, tanto na esfera da União Europeia, quanto no Brasil. Com esse intuito, realizou-se uma pesquisa bibliográfica e documental sobre o tema. A pesquisa documental tomou os aparatos legislativos como objetos de investigação. São discutidas as leis que tratam da proteção de dados pessoais no Brasil e na União Europeia e, mais especificamente, o Marco Civil da Internet no Brasil, o Regulamento 2016/679 da União Europeia e a Lei de Proteção de Dados brasileira (Lei nº 13.709/2018). A análise revela que o direito à privacidade e à proteção de dados pessoais tem evoluído diante das mudanças socioeconômicas e tecnológicas em curso. Adicionalmente, observa-se que a sanção da Lei de Proteção de Dados Pessoais brasileira veio acompanhada de vetos que descaracterizaram o projeto de lei aprovado no Senado, o que pode levar com que a mesma seja considerada incompatível com o modelo europeu.

Palavras-Chave: Privacidade; Proteção de dados pessoais; Internet.

Abstract: Privacy and protection of personal data are increasingly relevant issues, especially in face of many personal data leaks and sales scandals that have been reported. In this article, the information policy is adopted as a guiding principle for a discussion that aims to analyze how the right to privacy and the protection of personal data has been treated within the European Union as well as in Brazil. Following this objective, a bibliographic and documentary research was conducted. The documentary research took the legislative apparatuses as objects of investigation. The article discusses the laws

that deal with the protection of personal data in Brazil and in the European Union and, more specifically, the Brazilian Civil Rights Framework for the Internet, the European Union Regulation 2016/679 and the Brazilian Personal Data Protection Law (Law Nº. 13.709/2018). The analysis reveals that the right to privacy and protection of personal data has evolved in face of the ongoing socio-economic and technological changes. Additionally, it is noted that the sanction of the Brazilian Personal Data Protection Law received some vetoes that mischaracterized the bill approved in the Senate, bringing the risk of incompatibilities with the European model.

Keywords: Privacy; Personal data protection; Internet.

1 INTRODUÇÃO

Em uma época em que escândalos de vazamento de dados e espionagem virtual têm sido uma constante nos noticiários, discutir o tema privacidade em ambientes de rede é imprescindível. Nota-se que, atualmente, essa temática está presente na mídia, nos meios acadêmicos, empresariais e políticos. Com isso, o tema privacidade e proteção de dados pessoais que circulam na Internet têm suscitado diversas discussões, assim como tem envolvido diferentes abordagens, sejam elas do ponto de vista tecnológico, econômico, social, cultural e legal.

Um exemplo disso foi o Manifesto *Cypherpunk*, publicado em 1993 por Eric Hughes e apoiado por um grupo informal de ativistas interessados em discutir as políticas de privacidade e segurança na internet. Nos primórdios da rede mundial de computadores, não havia mecanismos eficientes que protegessem o acesso aos dados que por ela trafegados, sendo possível captar praticamente tudo que circulava, seja por empresas públicas ou privadas. No documento, afirma-se que:

> A privacidade é necessária para uma sociedade aberta na era eletrônica. Privacidade não é segredo. Um assunto privado é algo que não desejamos que o mundo inteiro saiba, mas um assunto secreto é algo que ninguém quer que ninguém saiba. Privacidade é o poder de se revelar seletivamente ao mundo (HUGHES, 1993).

Assim, a ideia deste manifesto foi alertar sobre a necessidade de garantir que cada pessoa revelasse somente o mínimo possível, devendo ter sua identidade preservada na rede, e somente revelada quando e somente quando for de seu desejo, sendo essa a essência da privacidade.

Partindo dessa problemática que merece ser pesquisada em seus diversos aspectos, o presente artigo adota a política de informação (BRAMAN, 2006) como eixo condutor da discussão ora apresentada. Nesse sentido, o objetivo deste trabalho é discutir como o direito à

privacidade e à proteção de dados pessoais tem sido tratado, tanto na Europa, quanto no Brasil[1].

A pesquisa se justifica pela vertiginosa expansão da prática de coleta massiva de informações dos usuários, que tem sido realizada por provedores de conteúdo e provedores de aplicações web (empresas que têm como fonte principal de receitas os anúncios publicitários veiculados no ambiente da Internet), bem como por órgãos ligados diretamente a esfera do Estado. A expansão desse tipo de prática suscita complexas questões de ordem ética, econômica, social e política (MARQUES; KERR PINHEIRO, 2014; SILVEIRA; AVELINO; SOUZA, 2016).

Neste artigo, considera-se que as leis e regulamentos que lidam com a privacidade dos dados dos internautas compõem na atualidade um dos subdomínios centrais das políticas de informação nacionais. Segundo Braman (2006), entende-se política de informação como todas as leis e regulamentos que lidam com os diversos estágios da cadeia de produção da informação, a exemplo da criação, processamento (cognitivo e algorítmico), armazenamento, transporte, distribuição, busca, uso e destruição. Em outros termos, política de informação é todo aparato jurídico aplicado ao "domínio da política de informação, comunicação e cultura" (BRAMAN, 2006, p.70).[2]

No artigo, apresenta-se inicialmente uma pesquisa bibliográfica acerca do tema privacidade de dados pessoais. Em seguida, adota-se uma pesquisa documental que tomou como corpus a Lei Geral de Proteção de Dados europeia (*General Data Protection Regulation* - GDPR) que entrou em vigor em maio de 2018, e a Lei Geral de Proteção de Dados (LGPD), sancionada no Brasil em 14 de agosto de 2018. Conclui-se que o direito à privacidade e à proteção de dados pessoais tem evoluído diante das mudanças socioeconômicas e tecnológicas em curso. Torna-se necessário resguardar a privacidade dos dados pessoais colhidos na internet por meio de legislação específica e, nesse sentido, mesmo tendo sido sancionada com vetos, a Lei Geral de Proteção de Dados representa um importante avanço da política de informação brasileira. No entanto, alguns vetos impostos ao projeto de lei, como o veto à criação da Autoridade Nacional de Proteção de Dados (ANPD) vinculada ao Ministério da Justiça e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, podem fazer com que a legislação nacional seja considerada incompatível com o modelo europeu.

[1] O artigo apresenta discussão teórica que compõe pesquisa de doutorado em andamento.
[2] Traduzido do original: "*domain of policy for information, communication, and culture*".

2 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS: CONTEXTO HISTÓRICO

Privacidade de dados revela-se uma temática mais antiga que a própria rede mundial de computadores. É possível afirmar que os debates acadêmicos sobre o tema privacidade tiveram início em 1890 a partir do artigo intitulado "*The right of privacy*" (WARREN; BRANDEIS, 1890), quando os autores definiram que a proteção integral do indivíduo é um direito tão antigo quanto o direito comum. Assim, os autores apontam que diante de tantas mudanças políticas, econômicas, sociais e tecnológicas, "o direito à vida passou a significar o direito de aproveitar a vida - o direito de ser deixado em paz; o direito à liberdade assegura o exercício de amplos privilégios civis; e o termo 'propriedade' cresceu para abranger todas as formas de posses - intangíveis e tangíveis" (WARREN; BRANDEIS, 1890, p.193).[3]

Os autores alertavam na ocasião sobre os danos causados pela invenção da fotografia e que estava sendo utilizada pela imprensa como uma forma de expor a intimidade das pessoas, o que ensejava a criação de uma lei para proteger e assegurar a privacidade do indivíduo e de sua vida doméstica. Segundo os autores, os danos causados por essas invasões de privacidade podem causar dor e sofrimento mental, devendo ser considerados uma lesão legal. Mas o direito comum (*common law*) assegura o direito à privacidade ao permitir que cada indivíduo determine o quanto comunicar aos outros de seus pensamentos e intenções, não sendo permitido que nenhuma outra pessoa possa publicar sem seu prévio consentimento.

> Esse direito é totalmente independente do material sobre o qual o pensamento, sentimento ou emoções são expressos. Pode existir independentemente de qualquer existência corpórea, como nas palavras ditas, uma canção cantada, um drama representado. Ou, se expresso em qualquer material, como em um poema por escrito, o autor pode ter se separado do papel, sem perder qualquer direito de propriedade na própria composição. O direito só finda quando o próprio autor comunica sua produção ao público, em outras palavras, a publica (WARREN; BRANDEIS, 1890, p.199).[4]

---

[3] Traduzido do original: "*the right to life has come to mean the right to enjoy life, - the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term "property" has grown to comprise every form of possession - intangible, as well as tangible*".

[4] Traduzido do original: "*This right is wholly independent of the material on which, or the means by which, the thought, sentiment, or emotion is expressed. It may exist independently of any corporeal being, as in words spoken, a song sung, a drama acted. Or if expressed on any material, as a poem in writing, the author may have parted with the paper, without forfeiting any proprietary right in the composition itself. The right is lost only when the author himself communicates his production to the public, in other words, publishes it*".

Os autores indicam ainda a necessidade de considerar o direito à privacidade de propriedade intelectual e/ou sentimental dos indivíduos, pois já existiam à época bases legais na lei da calúnia e difamação e na lei da propriedade literária e artística que deveriam ser seguidas. Segundo argumentam, o direito à privacidade não deve proibir publicações de interesse público ou geral, mas sim proteger as pessoas de serem expostas contra suas vontades, devendo ser evitada e repreendida a invasão indevida da privacidade individual, necessitando, assim, receber proteção com uma lei criminal. Deste modo, os autores concluem que a proteção deve partir do reconhecimento dos direitos do indivíduo, sendo que cada um é responsável por seus próprios atos e omissões. Portanto, "o direito à privacidade cessa com a publicação dos fatos pelo indivíduo ou com o seu consentimento" (WARREN; BRANDEIS, 1890, p.218).[5]

Historicamente, ao longo do tempo foram criados vários instrumentos de direito internacional, com o intuito de proteger o direito à intimidade e à vida privada do indivíduo:

> Apenas a título exemplificativo, poder-se-ia citar a Declaração Universal dos Direitos do Homem (1948), a Convenção Européia dos Direitos do Homem (1950), o Pacto das Nações Unidas sobre Direitos Civis e Políticos (1966), a Conferência Nórdica sobre o Direito à Intimidade (1967) e a Convenção Americana dos Direitos do Homem, assinada em San José da Costa Rica (1969) (QUEIROZ, 2006).

Corroborando a ideia do direito à privacidade, Bezerra e Waltz (2014, p.162) afirmam que a "privacidade e a intimidade são direitos fundamentais presentes na Declaração Universal dos Direitos Humanos e na Constituição da República [Federativa do Brasil] de 1988".

Assim, o artigo 12 da Declaração Universal dos Direitos Humanos, sinaliza que "ninguém será sujeito a interferências em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataques à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques" (UNESCO, 1948).

Já o artigo 5º da Constituição Federal brasileira de 1988 estabelece como garantia fundamental a proteção à intimidade e à vida privada do indivíduo. Além disso, a Magna Carta assegura o direito à indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

---

[5] Traduzido do original: "*The right to privacy ceases upon the publication of the facts by the individual, or with his consent*".

De acordo com Bezerra e Waltz (2014, p.162), a "privacidade refere-se a tudo o que o indivíduo não pretende que seja de conhecimento público, reservado apenas aos integrantes de seu círculo de convivência particular, enquanto a intimidade diz respeito única e exclusivamente ao indivíduo".

O artigo 21 do Código Civil brasileiro de 2002 também aborda o direito à privacidade, ao estabelecer que a "vida privada da pessoa natural é inviolável" (BRASIL, 2002). No entanto, segundo Polido *et al*. (2018), o mesmo não considera o amplo e complexo aspecto ligado à atual sociedade da informação ao não tratar a questão de proteção de dados pessoais.

O Marco Civil da Internet (MCI), Lei Nº 12.965, sancionada em 23 de abril de 2014, apesar de não ser um aparato legislativo especificamente voltado para o tema privacidade e proteção de dados, aborda essa temática em alguns dos seus artigos.

A divulgação do episódio de espionagem da presidente Dilma Rousseff pela Agência Nacional de Segurança dos EUA (*National Security Agency* - NSA) evidenciou a necessidade de uma legislação brasileira específica para regulamentar os princípios, direitos, deveres e as garantias dos usuários da internet no Brasil. Esse episódio foi um dos elementos que ensejou a promulgação do Marco Civil da Internet (MARQUES; KERR PINHEIRO, 2014; BEZERRA; WALTZ, 2014).

O texto do MCI foi resultado de uma série de discussões iniciadas em 2009, quando à época havia 26 propostas no Congresso Nacional a respeito do tema, e foi considerada uma das legislações mais avançadas do mundo na regulação da internet e na garantia da neutralidade da rede (MARQUES; KERR PINHEIRO, 2014).

Vieira (2016) destaca que os pontos que provocaram maiores discussões durante a tramitação da lei foram sobre liberdade, privacidade e neutralidade da rede. Bezerra e Waltz (2014, p.161) apontam acertadamente que o ponto mais polêmico dessa lei foi a questão da neutralidade da rede:

> Apesar de ter sido aprovado em tempo recorde pelo Senado Federal, e sancionado pela Presidente Dilma Rousseff no dia seguinte, durante a abertura do NETMundial, o projeto do Marco Civil permaneceu quase três anos emperrado na Câmara dos Deputados, principalmente por conta do lobby das grandes empresas de telefonia contra a chamada neutralidade da rede, isto é, a não-discriminação no trânsito da rede dos pacotes de dados em relação a seu conteúdo ou origem (BEZERRA; WALTZ, 2014, p.161).

Os temas privacidade e proteção dos dados estão presentes nos artigos 3º, 7º e 8º do Marco Civil da Internet. No seu artigo 3º, o Marco Civil da Internet estabelece os princípios da

proteção da privacidade e da proteção dos dados pessoais para o uso da internet no Brasil (BRASIL, 2014).

Já o artigo 7º estabelece os direitos e garantias dos usuários da Internet no Brasil, destacando que o acesso à internet é essencial ao exercício da cidadania, e ao usuário é assegurado o direito de inviolabilidade da intimidade e da vida privada, sigilo do fluxo de suas comunicações pela internet e de suas comunicações privadas armazenadas. O artigo 8º aponta que "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" (BRASIL, 2014).

Bezerra e Waltz (2014) indicam que os artigos 10º, 11º e 12º do Marco Civil da Internet versam sobre a proteção aos registros de conexão e de acesso a aplicações de internet, sem, no entanto, regular os usos desses registros.

O artigo 10º indica que a guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet devem buscar preservar a intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas. Assim, somente mediante a alguma solicitação judicial o responsável pela guarda dos mesmos deverá disponibilizar esse tipo de registro do usuário.

Mas os autores ressaltam que, mesmo que "a lei proteja o usuário da divulgação imprópria de informações de caráter pessoal, não contempla o fato de que o uso comercial dessas informações em poder das empresas também poderia ser considerado uma violação de privacidade e da intimidade dos indivíduos" (BEZERRA; WALTZ, 2014, p.166).

Já o artigo 11º da Lei 12.965/2014, ao abordar a proteção dos registros, dos dados pessoais e das comunicações privadas, recomenda que:

> 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 (BRASIL, 2014).

O artigo 12º indica as sanções que devem ser aplicadas no caso de ocorrência de infrações às normas previstas nos artigos 10º e 11º, que podem ser advertência, multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, suspensão temporária das atividades e, até mesmo, proibição de exercício das atividades do infrator.

Nota-se que, mesmo que não estabeleça uma regulamentação específica sobre privacidade e proteção de dados, o MCI aborda em seus artigos 13º a 16º a guarda de registros de conexão, assim como a guarda de registros de acesso a aplicações de internet na provisão de conexão e de aplicações.

Segundo o artigo 13º da lei, os provedores e conexão à Internet devem guardar os registros de conexão sob sigilo, em ambiente controlado e seguro. O artigo 14º da lei não permite que empresas provedoras de conexão à Internet guardem registros de acesso a aplicações de internet, guarda essa que somente pode ser executada por empresas provedoras de aplicações de internet.[6] A decisão de vedar a captura de informações por parte dos provedores de conexão justifica-se pelo enorme poder que esse tipo de situação traria, uma vez os provedores de conexão têm acesso a todo o qualquer bit de informação digital enviado ou recebido pelos internautas que os contratam. Essa vedação pode ser apontada como um dos principais motivos para a oposição das empresas de telecomunicações ao projeto de lei que gerou o Marco Civil da Internet.

Diante desse marco legislativo brasileiro, Bezerra e Waltz (2014, p.169) concluem que:

> O Marco Civil [da Internet] constitui talvez uma das pedras fundamentais para a promoção da liberdade de expressão, combate à censura e promoção de direitos constitucionais da internet, mas não encerra o debate, uma vez que é preciso avançar em termos técnicos, políticos, legais e sociais. A efetividade de uma legislação para a rede depende que o governo produza, em curto prazo, uma série de regulamentações que instituirão os detalhes de como serão tratados temas centrais do novo arcabouço jurídico, como liberdade de expressão, segurança de dados e, especialmente, direitos de autor e copyright, que dependerão de leis ainda a serem criadas. Somente dessa forma será possível caminhar para que os avanços propostos pelo marco se tornem efetivos e as suas deficiências sejam superadas.

Corroborando o exposto anteriormente, o Relatório Final da Comissão Parlamentar de Inquérito destinada a investigar a prática de crimes cibernéticos, também conhecida como CPI dos Cibercrimes, foi publicado em 31 de março de 2016 e apontou o Marco Civil da Internet

[6] Provedor de conexão à internet é pessoa, física ou jurídica, que intermedia a conexão do usuário com a rede mundial de computadores, ou seja, fornece infraestrutura e equipamentos de transmissão (como modems ou linhas de telefonia móvel), além de endereços lógicos, para que o internauta possa navegar na *web*. São exemplos de provedores de conexão à internet as empresas Claro, GVT, NET, Oi, Telefónica, TIM, Vivo, dentre outras. Já o provedor de aplicações de internet é outro tipo de empresa que provê, para os usuários que já possuem conexão à internet, serviços ou produtos que envolvem conteúdos, dados e informações. São exemplos de provedores de aplicações de internet as empresas: Facebook, Google, Netflix, Twitter, Yahoo, dentre outras.

como uma das leis mais avançadas sobre o assunto, e que inspirou vários países a editarem suas próprias leis relacionadas a este tema.

> A nova lei, tendo como fundamento a responsabilidade civil na internet, trouxe garantia da liberdade de expressão, privacidade, intimidade dos usuários e inviolabilidade das comunicações; vedação de divulgação de dados pessoais; obrigatoriedade de guarda dos registros de conexão por um ano e proibição de guarda dos registros de navegação; obrigação de retirada dos conteúdos infringentes; e garantia de neutralidade (BRASIL, 2016, p.83).

Bezerra (2016, p.241) aponta que o Marco Civil da Internet foi, na ocasião da sua promulgação, "o principal parâmetro legal para questões relacionadas à privacidade e à proteção de dados pessoais nas redes digitais". No entanto, conforme destaca o autor, o referido Relatório Final da Comissão Parlamentar de Inquérito cita oito projetos de leis que visavam reduzir o direito de privacidade dos usuários. Nota-se, portanto, o quão esse direito tem sido objeto de ataques.

O próximo tópico apresenta como a questão da proteção de dados pessoais tem sido tratada na Europa e os avanços na legislação brasileira diante da aprovação da Lei nº 13.709, de 14 de agosto de 2018.

3 REGULAMENTAÇÃO DA PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA E NO BRASIL

A Europa tem sido apontada como a protagonista do maior e mais recentemente avanço na questão de legislação específica sobre privacidade de dados após a aprovação do Regulamento nº 2016/679 pelo Parlamento Europeu e do Conselho, de 23 de abril de 2016, mais conhecido como Regulamento Geral de Proteção dos Dados Pessoais da União Europeia (*General Data Protection Regulation* - GDPR), que entrou em vigor em maio de 2018. Este regulamento é a lei mais relevante atualmente no cenário internacional e aborda a proteção das pessoas físicas em relação ao tratamento dos dados pessoais e a livre circulação desses. Tem como principal efeito ser de aplicação direta em toda a Europa, sem necessidade de ser incorporado pelo ordenamento jurídico de cada estado membro. Versa sobre os direitos de transparência, direitos de informação, direitos de acesso, direitos de retificação, direitos de eliminação ou direito ao esquecimento, limitação do tratamento dos dados, portabilidade dos dados e direito à oposição (UNIÃO EUROPEIA, 2016).

O regime jurídico de proteção de dados pessoais já se encontrava em vigor desde a Lei nº. 67, de 26 de outubro de 1998 (Lei de Proteção de Dados Pessoais), que resultou da transposição da Diretiva Comunitária nº. 95/46/CE, que teve como objetivo definir, harmonizar e promover igualdade no tratamento de dados pessoais pelos Estado-membros, por meio da definição de princípios para manipulação, tratamento de dados pessoais e estabelecimento de direitos básicos aos titulares dos dados (UNIÃO EUROPEIA, 1995).

A substituição da Diretiva nº 95/46/CE pelo Regulamento Geral de Proteção dos Dados Pessoais teve como objetivo unificar a proteção dos dados pessoais na União Europeia, uma vez que, sendo um regulamento, é possível sua aplicação direta junto aos 28 países que formam o bloco europeu.

O GDPR é composto por 11 capítulos e 99 artigos e se mostra bastante complexo. Ele buscou lidar com as novas e diversas questões trazidas pela economia digital e as novas tecnologias da informação e comunicação, de maneira abrangente e que atendesse aos diferentes países europeus.

A lei europeia apresenta em seu texto de abertura 173 considerações, sendo que a primeira reconhece como direito fundamental “a proteção das pessoas singulares relativamente ao tratamento de dados pessoais” (UNIÃO EUROPEIA, 2016, p.1). Além disso, o direito à proteção e ao tratamento dos dados pessoais deverá ocorrer independente da nacionalidade ou do local de residência das pessoas. Nos termos do regulamento,

> (4) O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística (UNIÃO EUROPEIA, 2016, p.2).

O GDPR também destaca o aumento significativo do intercâmbio de dados entre pessoas, associações e empresas decorrentes da evolução tecnológica e da integração econômica e social entre os Estados-Membros da União Europeia, o que criou novos desafios em relação à proteção de dados pessoais.

> As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas singulares disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global (UNIÃO EUROPEIA, 2016, p.2).

Assim, diante da facilidade de circulação e transferência de dados pessoais entre a União Europeia, países terceiros e organizações internacionais, é preciso assegurar a proteção dos dados pessoais, aplicar regras e gerar confiança para o desenvolvimento da economia digital. Com isso, o GDPR indica que as pessoas "deverão poder controlar a utilização que é feita dos seus dados pessoais" (UNIÃO EUROPEIA, 2016, p.2).

O regulamento europeu destaca que os princípios da proteção de dados não se aplicam a dados pessoais anônimos e de pessoas falecidas. As considerações iniciais do GDPR também indicam que "o consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito" (UNIÃO EUROPEIA, 2016, p.6).

O tratamento dos dados pessoais deverá ser feito de forma lícita, equitativa e de forma transparente, indicando para que finalidade serão recolhidos, utilizados e consultados. Assim, "o princípio da transparência exige que as informações ou comunicações relacionadas com o tratamento desses dados pessoais sejam de fácil acesso e compreensão, e formuladas numa linguagem clara e simples" (UNIÃO EUROPEIA, 2016, p.7). Desta forma, deverá ser informado o motivo e a finalidade do tratamento dos dados pessoais quando de seu armazenamento, devendo também ser estabelecido um prazo de conservação dos dados para posteriormente serem revistou ou apagados. "Os dados pessoais deverão ser tratados de forma a garantir a devida segurança e confidencialidade, evitando-se a utilização dos mesmos por pessoas não autorizadas" (UNIÃO EUROPEIA, 2016, p.7).

O capítulo I apresenta quatro artigos, sendo que neste último são apresentados diversos conceitos-chave que serão utilizados ao longo de todo regulamento para definição do escopo e aplicação de uma lei de proteção aos dados pessoais. O primeiro conceito definido foi o de 'dados pessoais', que, segundo o Regulamento 2016/679 da União Europeia em seu art. 4º, n. 1, entende que:

> «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 eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular (UNIÃO EUROPEIA, 2016, p.33).

Dentre um total de 26 termos conceituados, é possível destacar também a definição sobre 'tratamento', como sendo uma ou mais operações executadas para recolher, registrar, organizar, estruturar, conservar, alterar, recuperar, consultar, utilizar, divulgar ou apagar dados pessoais, de forma automatizada ou não; 'violação de dados pessoais', descrita como uma infração da segurança que gere a destruição, perda, alteração, divulgação ou acesso a dados pessoais, de forma acidental ou ilícito; e 'consentimento', como sendo uma manifestação de aceite de forma livre e explícita por parte do titular dos dados, "mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento" (UNIÃO EUROPEIA, 2016, p.34).

No artigo 4º também são diferenciados os termos dados genéticos, biométricos e relativos à saúde, assim como apresentados os conceitos de definição de perfis, tratamento transfronteiriço, empresa, grupo empresarial, organização internacional, responsável pelo tratamento, autoridade de controle, entre outros.

O capítulo II trata dos princípios relativos ao tratamento de dados pessoais: licitude, lealdade e transparência. Ou seja, o tratamento dos dados deve ser feito de forma lícita, leal e transparente quanto à finalidade de seu uso, mediante o consentimento livre do titular dos dados, além de permitir a revogação desse consentimento a qualquer momento. O capítulo III apresenta os direitos do titular dos dados, relativos à transparência das informações e regras para o exercício desses direitos, tais como: acesso, retificação, apagamento, portabilidade, limitação e oposição ao tratamento dos dados.

O capítulo IV versa sobre a responsabilidade quanto ao tratamento, proteção, registro das atividades, segurança e violação dos dados pessoais. Também apresenta no seu artigo 37 a figura do encarregado da proteção de dados, ou *data protection officer* (DPO),[7] que deve ser designado pela empresa responsável pelo tratamento dos dados pessoais. Seu papel é aconselhar e aproximar os órgãos reguladores dos titulares dos dados pessoais e, entre outras, tem a função de controlar "a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do

[7] O termo "encarregado da proteção de dados" aparece na versão oficial em português como uma tradução de "*data protection officer*".

responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais" (UNIÃO EUROPEIA, 2016, p. 56). As empresas responsáveis ou subcontratadas para fazerem o tratamento dos dados em larga escala ou que processem grandes volumes de dados pessoais precisam contratar um responsável para atuar como encarregado da proteção de dados (*data protection officer* – DPO) por uma questão de *compliance.*[8]

O capítulo V regula a transferência de dados pessoais para países terceiros ou organizações internacionais. O GDPR não permite a transferência de dados de europeus para países que não tenham uma legislação adequada de proteção de dados ou que não estejam em conformidade com as normas do GDPR, sendo necessário oferecer garantias adequadas, como a adoção de códigos de conduta ou certificações consonantes à lei europeia. As empresas também devem comprovar que possuem autorização do usuário para o uso dos seus dados pessoais, e deve haver a possibilidade do usuário suspender seu consentimento a qualquer momento. Segundo o regulamento, ao usuário deve ser permitido obter uma cópia dos dados registrados e ele deve poder ainda movê-los facilmente para outro prestador de serviços. Adicionalmente, todas as empresas que tiverem acesso a qualquer tipo de dados pessoais de um residente da UE deverão se adequar ao GDPR, mesmo não estando em solo europeu. Assim, é possível perceber que este regulamento tem alcance global, visto que países que têm relações com a comunidade europeia ou pretendem participar desta economia digital devem adequar suas legislações de proteção de dados ao GDPR. Corroborando essa ideia, Rocillo *et al.* (2018) apontam que

> Esse extenso regulamento, produto da atividade política e normativa dos órgãos da União Europeia, repercutiu rapidamente em todo o mundo, resultando em alterações significativas nos termos de uso de diversas aplicações de internet. Em curto período, empresas de internet tiveram de se adequar às demandas estabelecidas pelo GDPR em torno de *compliance* com os padrões de proteção de dados e evitar as consequências de atuação em conflito com um dos maiores mercados digitais do mundo (ROCILLO *et al*., 2018).

No Brasil, os impactos do GDPR se fizeram sentir por meio da atualização de termos de uso de vários sites e aplicativos, tais como Facebook, Instagram, Google, Yahoo. Isso se deve ao fato que, mesmo sendo restrito à Europa, as empresas tiveram que se adequar à nova legislação para continuarem atuando nos países que compõe a União Europeia, o que levou à

[8] O termo *compliance* significa estar em conformidade com leis e regulamentos externos e internos (Tradução dos autores).

adoção de melhorias nas regras de outros países, inclusive do Brasil. Assim, as novas regras acabaram por afetar as transações referentes ao processamento de informações de cidadãos, não só da União Europeia, mas também de organizações localizadas fora da Europa.

Além disso, o GDPR não só serviu como inspiração, como também parece ter feito avançar no Brasil a aprovação da Lei 13.709/2018 (BRASIL, 2018b). No Brasil, a Lei de Proteção de Dados Pessoais estava em discussão pela sociedade civil desde 2010. Em maio de 2018 a Câmara dos Deputados aprovou o parecer referente ao PL 4.060/2012, que tratava da proposta de Lei de Proteção de Dados Pessoais, que foi enviado ao Senado.

Em julho de 2018, a Comissão de Assuntos Econômicos do Senado aprovou o Projeto de Lei da Câmara 53/2018, que dispõe sobre a proteção, o tratamento e o uso de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Dando prosseguimento em regime de urgência, o plenário do Senado aprovou o substitutivo ao PLC 53/2018. A proposta foi aprovada por unanimidade e manteve 43 emendas já deliberadas anteriormente, além de rejeitar os Projetos de lei PLS 131/2014, PLS 181/2014 e PLS 330/2013, que tramitavam em conjunto e tratavam do mesmo tema.

No mesmo mês, o Projeto de Lei da Câmara 53/2018 seguiu para sanção presidencial. Por ter seguido em caráter de urgência, o mesmo não precisou ser analisado pelas Comissões de Ciência e Tecnologia e Constituição e Justiça. A análise do conteúdo do PLC 53/2018 revela que ele foi inspirado no GDPR e teve como objetivo regulamentar o uso, a proteção e a transferência de dados pessoais no Brasil, visando garantir maior controle dos cidadãos sobre seus dados pessoais (BRASIL, 2018a).

Em agosto de 2018 foi sancionada a Lei nº 13.709, que regulamenta o uso, a proteção e a transferência de dados pessoais que circulam na Internet, no âmbito brasileiro. A lei, que entrará em vigor após 18 meses de sua publicação, possui 65 artigos distribuídos em 10 capítulos. Ela dispõe sobre o tratamento, a proteção e a privacidade de dados pessoais em meios digitais. A lei indica que sua aplicação é destinada ao tratamento de dados pessoais pertencentes ou coletados de indivíduos localizados em território nacional.

Assim como no GDPR europeu, a LGPD brasileira apresenta logo no seu artigo 5º algumas conceituações, tais como: dado pessoal, sensível e anonimizado, banco de dados, titular, tratamento, consentimento e transferência internacional, entre tantas outras definições. A lei brasileira também indica alguns requisitos para que o tratamento de dados pessoais possa ser feito: mediante o fornecimento do consentimento por escrito por parte do

proprietário dos dados, podendo ser revogado a qualquer momento caso este discorde de alguma alteração de finalidade para o tratamento de dados; para o cumprimento de obrigação legal ou regulatória pelo responsável pelo tratamento; pela administração pública para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas; para a realização de estudos por órgão de pesquisa, sem a individualização da pessoa; para a proteção da vida ou da integridade física do titular ou terceiro; para a tutela da saúde, com procedimento realizado por profissionais da área ou por entidades sanitárias; para a execução de contrato ou procedimentos preliminares relacionados a um contrato; para pleitos em processos judicial, administrativo ou arbitral; para a proteção do crédito nos termos do Código de Defesa do Consumidor. Quando o tratamento de dados pessoais for condição para o fornecimento de produto ou serviço, o titular deverá ser claramente informado.

Além de apresentar o conceito de dados sensíveis, que apresentam origem racial ou étnica, convicções religiosas, opiniões políticas etc., a lei proíbe o tratamento dos dados pessoais para a prática de discriminação ilícita ou abusiva. O tratamento de dados pessoais de crianças e adolescentes também são contemplados em ambas as legislações. Em relação aos direitos do titular, a legislação nacional afirma no seu artigo 17º que "Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei" (BRASIL, 2018b). E, assim como na lei europeia, na lei brasileira é assegurado ao titular dos dados pessoais diversos direitos em relação a seus dados, como acessar e corrigir dados incompletos, inexatos ou desatualizados, anonimizar, bloquear, eliminar e/ou fazer a portabilidade dos dados a outro fornecedor de serviço ou produto, entre outros.

A lei brasileira segue as orientações do GDPR em relação às responsabilidades de transferência internacional de dados pessoais, ao definir o papel que cabe aos agentes de tratamento de dados pessoais (controlador, operador e encarregado pelo tratamento de dados pessoais). Também são definidas normas quanto à governança, boas práticas, segurança e sigilo de dados. A lei deve ser aplicável mesmo no caso das empresas com sede no exterior, desde que a operação de tratamento de dados seja realizada no território nacional.

No entanto, ao ser sancionado pela Presidência da República, alguns vetos descaracterizaram a lei originalmente proposta, como ocorrido no inciso II do artigo 23. Foi vetada a proteção e preservação de dados pessoais em relação ao compartilhamento no âmbito do Poder Público e com pessoas jurídicas de direito privado. Também foram vetados

alguns incisos do artigo 52, em relação à fiscalização e às sanções administrativas para as empresas que cometerem infrações previstas na lei, que previam suspensão parcial ou total do funcionamento do banco de dados e da atividade de tratamento dos dados.

Mas os pontos mais criticados foram os vetos aos artigos 55 a 59, que estabeleciam a criação da Autoridade Nacional de Proteção de Dados (ANPD), vinculada ao Ministério da Justiça, e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. Esses órgãos reguladores deveriam propor diretrizes estratégicas e fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade, além de zelar pela proteção dos dados pessoais, nos termos da legislação, fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação. Antes da promulgação da lei, alguns autores já indicavam quais seriam os problemas decorrentes de um eventual veto à criação da ANPD:

> Caso não seja criada uma autoridade verdadeiramente independente para fiscalização, corre-se grande risco de que a lei não seja aplicada de forma adequada. Além disso, diminuem-se as chances de que o Brasil seja classificado pela União Europeia como país que garante nível de proteção equivalente ao europeu, tornando-o um local menos atrativo para investimentos na área de tratamento de dados (ROCILLO et al., 2018).

Assim, a não criação de um órgão independente e especializado para fiscalizar o tratamento e utilização de dados pessoais faz com que o Brasil não esteja totalmente de acordo com os parâmetros estabelecidos pelo GDPR em um de seus pontos mais emblemáticos.

4 CONSIDERAÇÕES FINAIS

Este artigo abordou a privacidade e proteção de dados pessoais, por meio de uma revisão do contexto histórico desses temas e da apresentação de legislações relacionadas aos mesmos. Para isso, aludiu mais especificamente ao Regulamento 2016/679 da União Europeia, ao Marco Civil da Internet e à Lei de Proteção de Dados brasileira (Lei nº 13.709/2018), que foram tomados como objetos de investigação documental. Foram apresentadas considerações gerais sobre as questões mais latentes em relação à legislação europeia e à nova regulamentação sobre a proteção de dados pessoais aprovada no Brasil recentemente. Percebe-se que o momento tem se mostrado bastante efervescente e favorável à discussão do tema, principalmente por causa dos escândalos envolvendo a monitoração, a venda e o vazamento de dados pessoais por parte de grandes empresas mundialmente conhecidas.

Apesar do Brasil ter sido pioneiro ao criar o Marco Civil da Internet, ou seja, uma lei para regulamentar o uso da rede mundial de computadores e definir direitos e deveres de usuários e provedores da web no país, até o primeiro semestre de 2018 o Brasil ainda não tinha uma lei aprovada em relação à privacidade e proteção de dados pessoais.

Observa-se que direito à privacidade e à proteção de dados pessoais tem evoluído diante das mudanças socioeconômicas e tecnológicas em curso. No Brasil, se fazia premente a aprovação de uma Lei específica sobre a matéria. No entanto, a legislação nacional foi sancionada com vetos que descaracterizaram o projeto de lei aprovado no Senado, o que pode comprometer a adequação de sua aplicabilidade.

O ponto mais crítico foi o veto à criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, que seriam responsáveis por interpretar a lei, zelar pela proteção dos dados pessoais, fiscalizar, aplicar sanções em caso de descumprimento à legislação e definir seus parâmetros de aplicação. Os artigos vetados incluíam não só a definição da natureza desses órgãos, mas também outros aspectos fundamentais, como a estrutura organizacional dos mesmos. Essa lacuna pode comprometer a integração do Brasil às normas da União Europeia em relação ao fluxo de dados internacionais.

Pelo fato do tratamento de dados pessoais fazer parte do cotidiano de todos, pessoas físicas, jurídicas, poder público e empresas privadas, esse tema ganha cada vez mais centralidade nas dinâmicas socioeconômicas atuais. Estamos diante de um subdomínio das políticas de informação nacionais de grande relevância na atualidade.

Espera-se que o debate que o artigo apresenta possa auxiliar pesquisas futuras, que intencionem abordar aspectos da privacidade e proteção de dados pessoais, tais como segurança e criptografia de dados, vigilância e vigilância pública, mercado de dados, novos modelos de negócios digitais, Internet das Coisas e *big data*. Além disso, também se faz premente a sensibilização das pessoas em relação ao tema, pois a necessidade de que se aumente cada vez mais a consciência sobre a questão dos dados pessoais é urgente para uma melhor adequação e utilização dos mesmos.

REFERÊNCIAS

BEZERRA, Arthur Coelho. Privacidade como ameaça à segurança pública: uma história de empreendedorismo moral. **Liinc em Revista**, Rio de Janeiro, v.12, n.2, p. 231-242, nov. 2016, Disponível em: <http://revista.ibict.br/liinc/article/view/3720>. Acesso em: 28 jul. 2018.

BEZERRA, Arthur Coelho; WALTZ, Igor. Privacidade, neutralidade e inimputabilidade da internet no Brasil: avanços e deficiências no projeto do marco civil. **Revista Eletrônica Internacional de Economia Política da Informação da Comunicação e da Cultura**, v. 16, n. 2, p.161-175, maio/ago. 2014. Disponível em: <http://ridi.ibict.br/handle/123456789/858>. Acesso em: 10 jul. 2018.

BRAMAN, Sandra. **Change of State:** information, policy and power. London: MIT Press, 2006.

BRASIL. **Constituição da República Federativa do Brasil de 1988**, 05 out. 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituição.htm>. Acesso em: 28 jul. 2018.

BRASIL. Lei 10.406, de 10 de janeiro de 2002. **Código Civil**. Disponível em: <http://www.planalto.gov.br/CCivil_03/Leis/2002/L10406.htm>. Acesso em: 10 jul. 2018.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial [da] República Federativa do Brasil**, Brasília, DF, 24 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 1 jul. 2018.

BRASIL. Câmara dos Deputados. **Comissão Parlamentar de Inquérito de Crimes Cibernéticos. Relatório final**. Brasília, 2016. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D%3E+RCP+10/2015>. Acesso em: 4 ago. 2018.

BRASIL. **Projeto de Lei da Câmara n° 53, de 2018a**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <https://legis.senado.leg.br/sdleg-getter/documento?dm=7738646&disposition=inline>. Acesso em: 4 ago. 2018.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018b**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Disponível em: <http://legis.senado.leg.br/legislacao/DetalhaSigen.action?id=27457334>. Acesso em: 7 set. 2018.

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

HUGUES, Eric. **A cypherpunk's manifesto**. 9 mar. 1993. Disponível em: <http://www.activism.net/cypherpunk/manifesto.html>. Acesso em: 28 jun. 2018.

MARQUES, Rodrigo Moreno; KERR PINHEIRO, Marta Macedo. Marco Civil da Internet: uma análise sob a ótica da razão jurídica. In: MOURA, Maria Aparecida. (Org.). **A construção social do acesso público à informação no Brasil:** contexto, historicidade e repercussões. Belo Horizonte: Editora UFMG, 2014.

POLIDO, Fabrício Bertini Pasquot; ANJOS, Lucas Costa dos; BRANDÃO, Luíza Couto Chaves; MACHADO, Diego Carvalho; OLIVEIRA, Davi Teofilo Nunes. **GDPR e suas repercussões no direito brasileiro - Primeiras impressões de análise comparativa.** Belo Horizonte: IRIS - Instituto de Referência em Internet e Sociedade, 2018. Disponível em: <http://irisbh.com.br/gdpr-e-suas-repercussoes-no-direito-brasileiro/>. Acesso em: 10 jul. 2018.

QUEIROZ, Iranilda Ulisses Parente. **Proteção à intimidade e à vida privada a luz da Constituição Federal de 1988**. 5 jun. 2006. Disponível em: <https://www.direitonet.com.br/artigos/exibir/2662/Protecao-a-intimidade-e-a-vida-privada-a-luz-da-Constituicao-Federal-de-1988>. Acesso em: 10 jul. 2018.

ROCILLO, Paloma; VIEIRA, Victor Barbieri Rodrigues; PORTO JÚNIOR, Odélio; POLIDO, Fabrício Bertini Pasquot. O que significa uma lei de proteção de dados para o Brasil? **IRIS - Instituto de Referência em Internet e Sociedade**, 2018. Disponível em: <http://irisbh.com.br/o-que-significa-para-o-brasil-uma-lei-de-protecao-de-dados/>. Acesso em: 1 ago. 2018.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. A privacidade e o mercado de dados pessoais. **LIINC em Revista**. v.12, n.2, p. 203-216, novembro 2016. Disponível em: <http://revista.ibict.br/liinc/article/view/3719>. Acesso em: 15 set. 2018.

VIEIRA, Manuela do Corral. Vigilância e anonimato em aplicativos mobile: um estudo sobre a privacidade em relações homoafetivas no digital. **Liinc em Revista**, Rio de Janeiro, v.12, n.2, p. 308-321, nov. 2016. Disponível em: <http://www.ibict.br/liinc http://dx.doi.org/10.18617/liinc.v12i2.900>. Acesso em: 28 jul. 2018.

UNESCO. Organização das Nações Unidas para a Educação. **Declaração Universal dos Direitos Humanos.** 1948. Disponível em: <http://unesdoc.unesco.org/images/0013/001394/139423por.pdf>. Acesso em: 28 jun. 2018.

UNIÃO EUROPEIA. Regulamento nº 2016/679 do Parlamento Europeu e do Conselho, de 23 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 4 maio 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 1 ago. 2018.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Proteção de Dados). **Jornal Oficial da União Europeia**, Estrasburgo, 24 out. 1995. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:31995L0046&from=PT>. Acesso em: 1 ago. 2018.

WARREN, Samuel D.; BRANDEIS, Louis. The right to privacy. **Harvard Law Review**, v. 4, n. 5, 15 dez. 1890, p. 193-220. Disponível em: <http://www.jstor.org/stable/1321160>. Acesso em: 28 jun. 2018.