UNIVERSIDADE FEDERAL DO CEARÁ
FACULDADE DE DIREITO
CURSO DE BACHARELADO EM DIREITO

ANNA CECÍLIA MOREIRA CABRAL

PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL: AVANÇOS LEGISLATIVOS

FORTALEZA
2019

ANNA CECÍLIA MOREIRA CABRAL

PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL: AVANÇOS LEGISLATIVOS

Monografia apresentada ao Curso de Bacharelado em Direito da Universidade Federal do Ceará, como registro parcial para obtenção do título de Bacharel em Direito.

Orientador(a): Prof. Msc. Maria José Fontenelle Barreira Araújo

FORTALEZA

2019

Dados Internacionais de Catalogação na Publicação
Universidade Federal do Ceará
Biblioteca Universitária
Gerada automaticamente pelo módulo Catalog, mediante os dados fornecidos pelo(a) autor(a)

C117p Cabral, Anna Cecília Moreira.
Privacidade e proteção de dados no Brasil: avanços legislativos / Anna Cecília Moreira Cabral. – 2019.
45 f. : il.

Trabalho de Conclusão de Curso (graduação) – Universidade Federal do Ceará, Faculdade de Direito, Curso de Direito, Fortaleza, 2019.
Orientação: Profa. Ma. Maria José Fontenelle Barreira Araújo.
Coorientação: Prof. Dr. Sidney Guerra Reginaldo.

1. Privacidade e proteção de dados. I. Título.

CDD 340

ANNA CECÍLIA MOREIRA CABRAL

PRIVACIDADE E PROTEÇÃO DE DADOS NO BRASIL: AVANÇOS E DESAFIOS

Monografia apresentada ao Curso de Bacharelado em Direito da Universidade Federal do Ceará, como requisito parcial para obtenção do título de Bacharel em Direito.

Aprovada em: ___/___/_____.

BANCA EXAMINADORA

_____
Prof. Msc. Maria José Fontenelle Barreira Araújo (Orientador)
Universidade Federal do Ceará (UFC)

_____
Prof. Dr. Sidney Guerra Reginaldo
Universidade Federal do Ceará (UFC)

_____
Doutoranda Tatiana Maria Ribeiro Silva
Universidade Estadual do Ceará (UECE)

À Deus.

Aos meus pais, Francisca de Assis e César Cabral.

Aos amigos construídos na jornada.

AGRADECIMENTOS

À Deus, sustento nos dias de luta.

À Nossa Senhora, pela proteção e cuidado ao conduzir meus caminhos.

Aos meus pais, pela criação e suporte incomensurável ao longo do curso.

Ao professor Sidney Guerra, pela atenção e alegria das orientações.

Aos professores e mestrando participantes da banca examinadora pela disponibilidade, pelas valiosas colaborações e sugestões.

Aos amigos construídos ao longo da jornada universitária, os quais considero como indispensáveis para o meu amadurecimento pessoal e profissional.

Ao Escritório Ferrer Advogados e Ao Centro de Apoio e Defesa do Advogado da OAB/CE, onde estagiei e adquiri aprendizados essenciais para o exercício de minha profissão.

“As máquinas do final do século XX tornaram completamente ambígua a diferença entre o natural e o artificial, entre a mente e o corpo, entre aquilo que se autocria e aquilo que é externamente criado, podendo-se dizer o mesmo de muitas outras distinções que se costumavam aplicar aos organismos e às máquinas. Nossas máquinas são perturbadoramente vivas e nós mesmos assustadoramente inertes.” (HARAWAY, 2009, p. 42)

RESUMO

O presente trabalho aborda a relação entre o direito à privacidade e à proteção dos dados pessoais, apresentando essa correspondência como uma resposta da nova legislação às demandas surgidas em decorrência da popularização da internet e do avanço tecnológico. Para tanto, faz-se a análise sobre as previsões da Lei Geral de Proteção de Dados LGPD (Lei nº 13.709/18) e demais legislações concernentes ao tema. Além disso, também foi feito um estudo comparativo com as normas que constituem o recente Regulamento 679/2016 da União Europeia, sendo esta legislação precursora no mundo sobre a temática de proteção de dados. Assim, busca-se verificar a aplicabilidade da lei que entrará em vigor em agosto de 2020 e que deve resguardar princípios fundamentais para que a norma seja plenamente efetiva e eficaz, além de se ajustar às expectativas internacionais. Falar em direito à privacidade e à proteção dos dados pessoais é falar sobre um direito fundamental humano que se relaciona diretamente com a manutenção de uma sociedade em que são garantidas as liberdades fundamentais, ou seja, uma sociedade democrática. A privacidade se apresenta como um instrumento jurídico consolidado e reconhecido no ordenamento jurídico brasileiro e, assim, deve ser considerada e apropriada para o desenvolvimento da tutela desses dados.

Palavras-chave: privacidade; proteção de dados pessoais; internet; Marco Civil da Internet; Lei Geral de Proteção de Dados; regulação

ABSTRACT

This work approaches the relationship between the right to privacy and the protection of personal data, presenting this correspondence as a response of the new legislation to the demands arising from the popularization of the internet and technological advances. To do so, the analysis of the provisions of the General Law on Data Protection LGPD (Nº. 13,709/ 18) and other legislation concerning the subject is made. In addition, a comparative study was also made with the standards that constitute the recent Regulation 679/2016 of the European Union, this legislation being the precursor in the world on the subject of data protection. Thus, it seeks to verify the applicability of the law that will come into force in February 2020 and which must safeguard fundamental principles for the norm to be fully effective and effective, in addition to adjusting to international expectations. To speak of the right to privacy and protection of personal data is to speak about a fundamental human right and is directly related to the maintenance of a society in which fundamental freedoms are guaranteed, that is, a democratic society. Privacy is presented as a legal instrument consolidated and recognized in the Brazilian legal system and, therefore, should be considered and appropriate for the development of the protection of such data.

Keywords: Privacy; Protection of personal data; Internet; Brazilian Civil Rights Framework for the Internet; General Law of Data Protection; regulation

LISTA DE ABREVIATURAS E SIGLAS

CF	Constituição Federal
MS	Mandado de Segurança
GDPR	General Data Protection Regulation
LGPD	Lei Geral de Proteção de Dados
GPO	General Protection Officer
ANPD	Autoridade Nacional de Proteção de Dados
OCDE	Organização de Cooperação e Desenvolvimento Econômico

SUMÁRIO

1 INTRODUÇÃO

Hoje, vivendo em uma sociedade em que a tecnologia da informação permite um constante fluxo de informações, a sociedade começou a refletir sobre o surgimento de novos desafios e ameaças à proteção dos dados pessoais dos cidadãos. Desse modo, é de extrema importância discutir sobre privacidade neste ambiente de intenso compartilhamento de informações via internet. Podemos dizer, ainda, que a proteção de dados é um direito fundamental humano e, por isso, é essencial que a legislação e a tutela sejam regularmente atualizadas e aperfeiçoadas. No presente trabalho, analisaremos a temática do acordo com o método de pesquisa indutivo.

Este assunto tem assumido crescente relevância e despertado a atenção dos indivíduos para a necessidade de salvaguardar a sua intimidade e de dados que podem indicar informações referentes ao seu endereço residencial, orientação sexual, posicionamentos políticos e etc. Com isso, faz-se necessário que todos se questionem a respeito de quem tem acesso a tais dados, quem os compartilha e com que finalidade. Ademais, o uso inadequado de dados pessoais pode causar danos físicos, materiais ou imateriais às pessoas singulares, como a perda de controle sobre tais informações, a limitação dos seus direitos, entre outras duras consequências. Ainda assim, há, todavia, um longo caminho a percorrer no que concerne à formação e consciencialização dos indivíduos para esta problemática.

Tem-se que o problema é ainda mais complexo, uma vez que o cidadão, via de regra, não tem conhecimento a respeito da quantidade de informações que despejam na internet, e muito menos o que acontece posteriormente, o que justifica ainda mais a noção de urgência e seriedade voltadas para o assunto. No Brasil, há alguns anos, apesar do tema envolver toda a sociedade e referir-se a direitos fundamentais a falta de conhecimento e, assim, a não prioridade na implementação de medidas, culminava na possibilidade dos que tem acesso a esses dados agirem da maneira que lhes é conveniente, sendo possível desconsiderar quaisquer direitos do titular dos dados pessoais.

Desse modo, todas as esferas da sociedade, dentre elas as empresas privadas e o Judiciário, terão que se adequar as mudanças e inovações tecnológicas. Isso se dá, pelo fato de que o Direito pode ser entendido como o reflexo de sua sociedade, e por isso, novos conflitos e demandas têm surgido em detrimento das relações digitais. Assim, diante desse cenário, em

2018, foi sancionada a lei nº 13.709/18, intitulada Lei Geral de Proteção de Dados (LGPD), que fará com que a partir de 2020 cidadãos, Poder Público e empresas se adaptem a uma nova política de tratamento e compartilhamento de dados no Brasil.

2 DIREITO À PRIVACIDADE

Antes de iniciarmos o debate acerca da proteção dos dados pessoais propriamente dita, faz-se necessário apresentar as linhas introdutórias referentes ao direito à privacidade no ordenamento jurídico brasileiro. Pode-se dizer que a noção de "privacidade" existente na legislação brasileira, conforme Marcel LEONARDI, (2012, p. 47), é extremamente ampla, e, por isso, o autor utiliza a expressão "palavra-camaleão" para explicá-la, visto que ela é capaz de sustentar diversos significados, o que acarreta uma ampla margem para diferentes interpretações para esse instituto. Porém, toda essa subjetividade pode ser prejudicial para encontrar a solução de casos práticos e para a concretização de políticas públicas. Além disso, também gera dificuldade em eventual situação de confronto com outra norma jurídica ou princípio.

De acordo com RODOTÀ (2008, p. 25), o direito à privacidade, em sua acepção clássica é insuficiente. Isso se dá pelo fato de que ele o considera como uma tutela que se restringe a questões estritamente privadas e que busca combater invasores externos. Por isso, o autor defende que o conceito de privacidade deve ser reposicionado de acordo com as formas de organização de poder, e assim, promover uma modificação qualitativa na sua concepção, levando em conta que "a infraestrutura da informação representa hoje um dos seus componentes fundamentais".

Diante disso, LEONARDI (2012, p. 52-76) elenca algumas das possíveis definições da privacidade, sendo elas: o direito a ser deixado só; o resguardo contra interferências alheias; o segredo ou sigilo; e o controle sobre informações e dados pessoais.

Para fins deste trabalho, o estudo ficará restrito ao quarto conceito indicado pelo autor, considerado por ele como "um dos aspectos mais relevantes para o direito à privacidade" atualmente. (LEONARDI, 2012, p. 68)

Todavia, também faz-se necessário discorrer sobre a relação entre moral e tecnologia. Por essa razão pode-se observar as considerações apresentados por Latour,

segundo o qual, os dados e a inteligência artificial também são atores sociais. Segundo o próprio Latour:

> Conceber humanidade e tecnologia como polos opostos é, com efeito, descartar a humanidade: somos animais sociotécnicos e toda interação humana é sociotécnica. Jamais estamos limitados a vínculos sociais. Jamais nos defrontamos unicamente com objetos. [...] A ilusão da modernidade foi acreditar que, quanto mais crescemos, mais se extremam a objetividade e a subjetividade, criando assim um futuro radicalmente diferente de nosso passado. Após a mudança de paradigma em nossa concepção de ciência e tecnologia, sabemos agora que isso nunca acontecerá e, na verdade, nunca aconteceu. [...] [Os artefatos] merecem ser alojados em nossa cultura intelectual como atores sociais de pleno direito. Os artefatos somos nós. O alvo de nossa filosofia, teoria social e moralidade cifra-se em inventar instituições políticas capazes de absorver essa grande história, esse vasto movimento em espiral, esse labirinto, esse fado.

Em consenso com a citação acima, a obra Moralizing technology: understanding and designing the morality of things, de Peter-Paul Verbeek visa alargar o alcance da ética para ajustar melhor as modificações sociais na era tecnológica e, ao fazê-lo, conclui que a natureza é inseparável da humanidade e da tecnologia. Para Verbeek, as tecnologias são "mediadores morais" que modelam a maneira como percebemos e interagimos com o mundo e, desta forma, criam e norteiam possíveis comportamentos do ser humano**.**

2.1 A Evolução do Conceito de Privacidade

Novas técnicas e ferramentas tecnológicas deram início aos debates doutrinários acerca do direito à privacidade. Essas reflexões permitiram o acesso e a maior divulgação de fatos relativos à esfera privada do indivíduo de um modo anteriormente não existente. Tal fato pode ser observado no famoso artigo sobre privacidade de Warren e Brandeis, intitulado "The right to privacy", no qual os autores denunciavam como a fotografia, os jornais e aparatos tecnológicos tinham invadido os sagrados domínios da vida privada e doméstica (1890, p. 2). A principal finalidade dos referidos escritos é buscar reconhecer um direito à privacidade na "common law", levando em consideração precedentes jurisprudenciais dos tribunais ingleses.

Ao discorrerem sobre o direito à privacidade, Warren e Brandeis condicionam a sua proteção à inviolabilidade da personalidade, em contrapartida ao que se acreditava anteriormente, em que se associava a proteção da vida privada à propriedade.

Assim, os autores afirmam o entendimento de que o princípio que resguarda escritos pessoais e outras produções, não contra o furto ou a apropriação física, mas contra toda forma

de publicação, é na realidade não o princípio da propriedade privada, mas o da inviolabilidade da personalidade (1890, p. 7, trad. livre).

Além disso, Warren e Brandeis, ao indicar o direito à privacidade, almejam também definir os limites desse direito, nos termos a seguir: (a) o direito à privacidade não veda a comunicação de tudo que é privado, pois se isso acontecer nos parâmetros legais, como por exemplo, em uma Assembleia Legislativa ou em um Tribunal, não há violação desse direito; (b) o direito à privacidade não impede a publicação do que é de interesse geral; (c) em caso de consentimento do indivíduo afetado, exclui-se a violação do direito; (d) se a intromissão for gerada por uma revelação verbal que não cause danos, a reparação não será exigível; (e) a alegação de veracidade da informação pelo agressor não exclui a violação do direito; e (f) a ausência de dolo também não exclui a violação desse direito (1890, p. 12-14).

A partir da análise desse artigo, percebe-se que a proteção à privacidade teve um caráter, sem sua grande parte, individualista em seus primórdios, muito em decorrência do direito a ser deixado só (right to be let alone). Também é válido ressaltar a exigência absoluta de abstenção do Estado no âmbito privado individual para a garantia do instituto.

A transformação da função do Estado, durante o século XX, conjuntamente à revolução tecnológica, induziu a modificação do sentido e o alcance do direito à privacidade. Passou a ser visto como uma garantia de controle do indivíduo sobre as próprias informações e um requisito para qualquer regime democrático (Doneda, 2006). Com isso, pode-se afirmar que, no século passado, ocorreu um "processo de inexorável reinvenção da privacidade" (Rodotà, 2008, p. 15).

Além disso, a partir de então, também foi reconhecido na esfera internacional e transformou-se, com o intuito de fazer emergir a dimensão de proteção de dados pessoais, à medida que surgiram novos desafios ao ordenamento jurídico a partir do tratamento informatizado dos dados (Doneda, 2006, p. 27).

A modificação desse conceito pode ser observada, de forma mais clara, a partir da década de 70, quando surgiram legislações específicas e de decisões judiciais de vários países e foram aprovados acordos internacionais e transnacionais em diferentes níveis. Tais instrumentos compartilham o conceito segundo o qual os dados pessoais merecem uma tutela forte, visto que constituem uma projeção da personalidade do indivíduo.

2.2 A primeira geração das normas de proteção de dados pessoais

A primeira geração das normas de proteção de dados pessoais surgiu como resposta ao processamento eletrônico de dados nos âmbitos da administração pública e das empresas privadas. Assim como também surgiram às ideias de centralização dos bancos de dados em grandes bancos de dados nacionais (Mayer-Schönberger, 2001). Podemos citar alguns exemplos de normas da primeira geração no âmbito europeu, são elas: as leis do Estado alemão de Hesse (1970); a Lei de Dados da Suécia (1973); o Estatuto de Proteção de Dados do Estado alemão de Rheinland-Pfalz (1974); e a Lei federal de Proteção de Dados da Alemanha (1977). Além disso, nos Estados Unidos foram aprovados nesse mesmo período o Fair Credit Reporting Act (1970), objetivando regular os relatórios de crédito dos consumidores, e o Privacy Act (1974), aplicável à administração pública.

Outras legislações importantes também contribuíram para a consolidação de um conceito de privacidade relacionado à proteção de dados pessoais. Entre elas, podemos destacar a Convenção 108 do Conselho da Europa (1981), as Diretrizes da OCDE para a proteção da privacidade e dos fluxos de dados pessoais para além das fronteiras dos países (1980) e a Diretiva Europeia 95/46/CE referente à proteção de dados pessoais (1995).

Ainda discorrendo sobre a evolução do conceito de privacidade em âmbito mundial, houve a decisão do Tribunal Constitucional alemão no julgamento acerca da "Lei do Recenseamento de População, Profissão, Moradia e Trabalho", sendo esta considerada uma referência histórica. O tribunal tornou o conceito do livre controle do indivíduo sobre o fluxo de suas informações na sociedade mais radical e decidiu pela inconstitucionalidade parcial da referida lei, sob a ótica da existência de um direito à "autodeterminação informativa" com base nos artigos da Lei Fundamental que versam sobre a dignidade humana e o livre desenvolvimento da personalidade, respectivamente.

A sentença da Corte Constitucional criou o ponto de partida para a teoria da proteção de dados pessoais e para as normas nacionais e europeias advindas posteriormente, reconhecendo um direito subjetivo fundamental e definindo o indivíduo como principal foco no processo de tratamento de seus dados. O referido julgamento consolidou a ideia de que tal direito subjetivo fundamental não pode ter o seu escopo fundamental violado. Ademais, ao ser consolidado pelo legislador, percebe-se uma limitação ao poder legislativo, que passa a estar vinculado à um direito à autodeterminação da informação.

A Corte argumentou, ainda, que o moderno processamento de dados pessoais configura uma grave ameaça aos direitos de personalidade do indivíduo, visto que possibilitava o armazenamento ilimitado de dados e a sua combinação podendo resultar em um conjunto de informações minucioso a respeito da pessoa, ocorrendo, ainda, sem a sua participação ou conhecimento de fato.

Por isso, decidiu que a Constituição alemã protege o indivíduo contra o tratamento indevido desses dados, justificando que o indivíduo tem o poder para determinar o fluxo de suas informações na sociedade, com base na consolidação do direito fundamental ao livre desenvolvimento da personalidade. Desse modo, entende-se a participação do cidadão essencial no processamento da coleta, do armazenamento e da transmissão de seus dados (Mayer-Schönberger, 2001).

A partir do momento em que a evolução tecnológica resulta no armazenamento e processamento rápido e eficiente de dados, faz-se a associação entre proteção à privacidade e informações pessoais, realizando uma alteração no conteúdo do direito à privacidade.

Visto que as mudanças sociais e tecnológicas demandam uma proteção específica da privacidade e, mais especificamente, dos dados pessoais. Nas palavras de Carlos Affonso Pereira:

> O alcance das mudanças que nascem no meio social a partir da difusão de tais tecnologias impõe, por seu turno, o aperfeiçoamento da regulamentação jurídica então existente visando estabelecer soluções para os conflitos que venham a surgir. Vale destacar que nem sempre a edição de novas regras se faz necessária frente ao avanço tecnológico, todavia ordinariamente a sofisticação no manuseio de técnicas em constante evolução requer a tutela legal de suas peculiaridades.
>
> A proteção do direito à privacidade perante o progresso tecnológico e a faculdade de acesso e distribuição indevida de dados de terceiros tornou-se um desses conflitos, demandando o trabalho não apenas dos juristas, mas igualmente dos legisladores e magistrados no sentido de se definir o locus da privacidade no cenário contemporâneo.
>
> A concepção do direito à privacidade como proteção do isolamento individual encontra-se aquém da tutela requerida pela intensa movimentação de dados pessoais na internet. Assim, o controle da coleta, armazenamento e utilização de dados torna-se imperativo, sendo essa a função primordial que tem a desempenhar o direito à privacidade frente às novas tecnologias.

Por fim, conclui-se, a princípio, que ele passa a ser compreendido como um fenômeno coletivo exigindo igualmente uma tutela jurídica coletiva. Posteriormente, a privacidade passa a significar também o controle dos dados pessoais pelo próprio indivíduo,

que decide quando, como e onde os seus dados pessoais devem ser armazenados, o que faz com que, a privacidade, antes ligada somente a uma ideia de liberdade, passa a igualdade e a outros direitos fundamentais, em detrimento da crescente possibilidade de prejuízos causados ao indivíduo pelo Estado e pelo mercado.

2.3 A Economia da Informação

O conceito de economia na sociedade pós-industrial quando pesquisadores notaram um aumento gradual dos setores não-agrícolas e não-industriais dos países de economias avançadas. Os primeiros estudos a respeito do tema resultaram na conclusão equivocada que a classificou como uma economia de serviços. Machlup (1962) foi um dos primeiros autores que utilizou o termo "*indústria baseada no conhecimento*" para caracterizá-la. Ele concluiu, em 1959, que as funções relacionadas à produção do conhecimento tinham ultrapassado outras em termos numéricos. Em 1977, Marc Uri Porat (1977) avaliou a importância dessa economia e criou o termo "*economia da informação"*.

Com o desenvolvimento da Internet e mais tarde da World Wide Web, a economia da informação gradativamente amadureceu para a economia desenvolvida como é hoje, resultando no crescimento do PIB da economia mundial.

Por sua vez, a definição mais citada da "*economia da informação*" é a de Porat, que distingue dois domínios da economia: o domínio da matéria e da energia e o domínio da informação. Porat classifica o setor de informações em primário e secundário. Os trabalhadores do "*setor de informações primário*" são aqueles que se concentram na criação e manuseio das informações. Já os trabalhadores do "*setor de informações secundário*" são aqueles que lidam principalmente como itens não-informativos, mas cujo trabalho envolve informações como um elemento secundário. São os trabalhadores de empresas e de indústrias sem relação com a informação e que produzem informações para uso interno, na produção de bens agrícolas ou industriais.

O autor Porat inclui no setor de informações primário os segmentos de invenção e produção de conhecimento em empresas privadas e serviços de informação, a distribuição da informação e comunicação, o gerenciamento de risco, pesquisa e administração, o processamento de informações e serviços de transmissão, bens ligados à

informação, determinadas atividades governamentais e suas instalações de apoio, e, por fim, o comércio de bens e serviços relacionados à informação.

Outras definições existentes nas bibliografias e pesquisas são variações das definições dos autores Porat ou Machlup. Dentre elas, podemos citar o autor Sérgio Amadeu da Silveira (2017, p. 13 e 14), o qual afirma que:

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

Entretanto, a OCDE (Organização de Cooperação e Desenvolvimento Econômico) adotou a definição de Porat em seus estudos sobre a natureza, a dimensão e o desenvolvimento das economias da informação.

3 PROTEÇÃO DE DADOS PESSOAIS COMO DIREITO FUNDAMENTAL

No contexto atual, podemos considerar a serem analisados interesses contrapostos, em relação à proteção de dados pessoais. Por um lado, há a proteção da vida privada dos indivíduos e por outro, questões relativas à segurança interna e internacional, reorganização da administração pública e interesses de mercado (RODOTÀ, 2008, p. 13).

Com base nisso, o autor afirma (RODOTÀ, 2008, p. 37):

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

No que diz respeito às relações de mercados, não se pode dizer que o aumento dos custos para as empresas e para a administração pública é o argumento primordial para ocasionar as normas sobre a proteção de dados (RODOTÀ, 2008, p. 53).

Ainda, o autor discorre sobre a importância da proteção coletiva dos dados, visto que afirma (RODOTÀ, 2008, p. 50):

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

Diante desse contexto, entende-se que "a preocupação com as possibilidades infinitas de combinações de dados pessoais, associadas a poderosas habilidades de pesquisa e a impressionantes capacidades de armazenamento, todas potenciadas pelo uso da informática, levaram a construção deste direito, que foi sendo acolhido como um novo direito fundamental" (CASTRO, 2005, p. 29). Ademais, "que não seria compatível com o direito à autodeterminação informativa a uma ordem social e jurídica na qual o cidadão não pudesse saber quem, o quê, quando e com que motivo sabe alguma coisa sobre ele." (CASTRO, 2005, p. 29).

Segundo Maria Celina Bodin, o princípio constitucional da dignidade é o único princípio capaz, na atualidade, de atribuir a unidade axiológica e a lógica sistemática necessárias ao entendimento dos institutos jurídicos e das categorias do direito civil referentes ao tema. Assim, afirma:

> A "dignidade da pessoa humana" decorre do reconhecimento da pessoa como um ser integrado à natureza, dotado de uma racionalidade evoluída, com a capacidade de reconhecer-se no próximo, relacionar-se com ele, exercendo sua aptidão para dialogar e amar. [...] Para Kant a "dignidade da humanidade consiste precisamente nesta capacidade de ser legislador universal, se bem que com a condição de estar ao mesmo tempo submetido a essa mesma legislação" e, por isso, "a autonomia é, pois, o fundamento da dignidade da natureza humana e de toda a natureza racional".
>
> Portanto, o simples fato de integrar o gênero humano já qualifica a pessoa como destinatária do valor da dignidade. Esse atributo é inerente a todos os homens, decorrente da própria condição humana, que o torna credor de igual consideração e respeito por parte de seus semelhantes. A dignidade é composta por um conjunto de direitos existenciais compartilhados por todos os homens, em igual proporção, não obstante as diversidades socioculturais dos povos. A Declaração Universal dos Direitos Humanos, já em seu art. 1º, põe em destaque os dois pilares da dignidade humana: "Todas as pessoas nascem livres e iguais em dignidade e direitos. São dotadas de razão e consciência e devem agir em relação umas às outras com espírito de fraternidade".

Portanto, conforme exposto anteriormente, a evolução histórica dos direitos à privacidade e intimidade, resultaram no avanço para um entendimento que esteja adaptado a realidade fática atual, resultando, assim, no direito de proteção de dados pessoais como

fundamental ao indivíduo. Esse entendimento demonstra a necessidade de que os ordenamentos jurídicos tenham leis fortes e eficazes que regulem o fluxo de dados.

3.1 A Importância do Consentimento no Tratamento de Dados

A entrada em vigor da lei geral europeia de proteção de dados (GDPR) foi um marco mundial no que diz respeito as atualizações de Termos de Uso e Políticas de Privacidade por empresas, principalmente de tecnologia, do mundo todo. Isso se dá pelo fato de que a legislação é aplicável a todas as sociedades que tratem dados em território europeu, mesmo que não estejam sediadas na Europa e estabelece altas multas àquelas que não se adequarem às suas normas.

No Brasil, foi publicada, em 2018, a Lei 13.709/18, conhecida como lei geral de proteção de dados (LGPD) que, foi bastante inspirada na lei europeia, também com o objetivo de regulamentar o tratamento de dados, por sua vez, em território brasileiro.

Dessa forma, empresas que operam em ambiente digital devem se adaptar às normas da GDPR e da nova lei brasileira de proteção de dados, principalmente porque, agora precisam se proteger das multas lá cominadas, que podem causas prejuízos ao capital da empresa.

Nesse contexto, analisaremos um dos pontos de fundamental importância para a eficácia dos termos de determinada aplicação de internet: o consentimento do usuário.

Primeiramente, faz-se necessário saber que os Termos de Uso como as Políticas de Privacidade são negócios jurídicos existentes entre a sociedade que opera em ambiente digital e seus usuários. Para que sejam válidos e eficazes, devem ser expostos com a finalidade de levar ao conhecimento dos usuários, que, por sua vez, devem manifestar sua aceitação. Sabe-se que no direito contratual, aceitação é o ato pelo qual uma pessoa manifesta, de modo inequívoco, seu consentimento às cláusulas de um contrato. Por meio da aceitação, estabelece-se o vínculo contratual. Enquanto no mundo não virtual, a aceitação ocorre, via de regra, pela assinatura do instrumento contratual, no âmbito digital esta pode ser manifestada pelo preenchimento de um formulário eletrônico, envio de e-mail, ou até mesmo por um simples clique do usuário determinada *checkbox* ou *link*.

Disto isto, de acordo com a aplicação das multas cominadas pelo GDPR e, em breve, com pela LGPD, a coleta de dados do usuário somente poderá ser feita após obtenção de seu consentimento válido. Mas como definir legalmente o que é consentimento válido? Para responder a essa questão, devemos analisar o conceito de consentimento nas recentes leis de proteção de dados.

O GDPR define consentimento como *"manifestação de vontade, livre, específica, informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento".*

No mesmo sentido, a LGPD apresenta definição semelhante em seu artigo 5º, XII:

> *Art. 5º Para os fins dessa lei considera-se:*
>
> *XII: consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;*

Das legislações apresentadas, conclui-se que os seguintes elementos constitutivos do consentimento válido são: o consentimento livre, informado, inequívoco e para finalidade específica e determinada. Portanto, faremos a análise de cada um deles.

O consentimento livre é aquele em que deve ser disponibilizado ao usuário pleno controle sobre o tratamento de seus dados pessoais, podendo ele escolher quais dados deseja fornecer ou não. Além disso, ele deve poder retirar seu consentimento a qualquer tempo caso desejar, não podendo o usuário ser submetido a consentir com o tratamento de seus dados pessoais para ter acesso a determinada aplicação de internet. Caso isso ocorra, o consentimento do usuário não é considerado livremente fornecido, podendo o contrato ser invalidado por ineficácia da aceitação.

Não obstante, as legislações de diversos países tendem ao entendimento de que o consentimento para tratamento de dados essenciais deve ser diferenciado dos demais, observando a liberdade de escolha do usuário quanto ao fornecimento de dados não obrigatórios. Assim, o consentimento só pode ser exigido, como condição inequívoca ao acesso a determinado meio digital, em relação ao tratamento de dados absolutamente

necessários à prestação dos serviços em questão. Caso as exigências extrapolem o objetivo dos serviços a serem prestados, o consentimento não será considerado livre.

O consentimento inequívoco depende de manifestação por meio de um ato positivo do usuário, ou seja, deve haver uma ação indicando sua aceitação. Desse modo, a aceitação não pode ser passiva, de maneira que o silêncio do usuário não pode ser considerado consentimento.

Por fim, a coleta de dados não pode ser utilizada para fins não previstos, ou seja, sem prévio consentimento do usuário, devendo ser sempre vinculada a uma ou mais finalidades específicas e informadas na respectiva Política de Privacidade.

3.2 Riscos do Vazamento de Dados para o Indivíduo

Em todo o histórico de casos de vazamento de dados, possivelmente, o mais famoso foi o escândalo envolvendo a empresa *Cambridge Analytica* que demonstrou as graves consequências advindas do uso indevido e não autorizado de dados pessoais, que vão além da individualidade de cada cidadão, ao ponto de repercutir nos rumos democráticos de uma nação. A partir do ocorrido, ficou explícito o impacto da ausência de regras claras sobre o uso de dados e de uma autoridade que as tornem eficazes.

No Brasil, a empresa já pretendia atuar no futuro pleito eleitoral para a presidência da república, através do oferecimento de conteúdos e propagandas direcionadas a eleitores com base em seus interesses descobertos por meio dos seus dados pessoais coletados e utilizados indevidamente, com o objetivo de influenciar os seus votos. Diante da repercussão, o Ministério Público iniciou investigação para averiguar se realmente houve coleta e uso não autorizado de dados pessoais para essas finalidades.

Dentre os acontecimentos mais recorrentes e evidentes nesse sentido, também é possível ressaltar a atuação de robôs que disseminam notícias falsas e que podem ter efeitos extremamente maléficos para a sociedade. Tais ações também buscam ativamente impedir que os usuários se informem de maneira adequada. Outra estratégia comum dos perfis automatizados é o compartilhamento de links contaminados, que tem como objetivo o roubo de dados e informações pessoais. Essas informações, que podem ser fotos de perfil em rede social, por exemplo, podem ser utilizadas para a criação de outros perfis-robô que tenham

características que sejam capazes de iniciar conexões nas redes com usuários reais sem a permissão de seu titulares.

O fator mais prejudicial da ausência de uma lei geral é o de que não há parâmetro interpretativo prevaleça quanto à legalidade no uso dos dados, uma vez que inexistiria, em alguns contextos, limitações claras ao tratamento destes. Dessa forma, ficou à época ainda mais evidente a necessidade de uma LGPD brasileira.

3.3 O regulamento da União Europeia

Neste tópico será discutido o Regulamento da União Europeia, também conhecido como General Data Protection Regulation – GDPR, sendo ela a lei com maior relevância no cenário internacional acerca do assunto. Ele dispõe em sua ementa que é relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Desse modo, iremos analisar, de forma geral, como o Regulamento lidou com a problemática dos dados pessoais. Para tanto, destacam-se as considerações abarcadas pelo advogado Guilherme B. de Campos Guidi, membro da International Assiociation of Privacy Professionals, (2018, 92 e 93):

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

> utilizar como padra de operação a escolha pela preservação da privacidade em detrimento da publicidade na ausência de um posicionamento expresso do titular de dados.
>
> A segunda mudança, de igual importância, vem na reafirmação dos programas de incentivo ao cumprimento do Regulamento, pela criação de selos e sistemas de certificação relacionados ao grau de zelo da empresa com a privacidade de seus usuários.

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

Assim, o autor afirma (VALENTE, 2018, p. 111):

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

Ainda, é importante ressaltar que o Regulamento é válido para qualquer pessoa localizada na União Europeia, e não apenas a cidadãos europeus.

Nesse sentido (SOPRANA, 2018):

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

Em relação às entidades privadas tem-se que (SOPRANA, 2018):

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

A lei estimula e vira promover maior transparência das empresas e organizações que lidam e comercializam os dados pessoais. Em seu texto dispõe de diversas regras que impõe que as mesmas precisam estar "aptas a comunicar sua responsabilidade sobre o ciclo de vida dos dados: coleta, tratamento, compartilhamento, armazenamento e descarte" (SOPRANA, 2018).

3.4 Proteção de dados na América Latina: legislação da Argentina

No cenário da América Latina, a maior parte dos países ainda não regulamentou a matéria pertinente à proteção de dados pessoais, visto que existem apenas leis setoriais sobre o tema, como, por exemplo, a lei acerca da vida privada, no Chile e a lei sobre informações de caráter privado, no Paraguai. Países como Peru e México promulgaram leis específicas de proteção aos dados há alguns anos.

Entretanto, Argentina e Uruguai são dois países que destacam-se no meio por já possuírem legislação acerca do tema. Este último, em 2004, iniciou a discussão do tema com a Lei nº 17.838, que tratava da restrição de dados para informações comerciais. Em 2012, a Comissão Europeia, nos termos da Diretiva 95/46/CE, decidiu que a República Oriental do Uruguai possuía adequação do nível de proteção de dados pessoais no relativo ao seu tratamento automatizado.

A Argentina, por sua vez, primeiro país latino-americano que editou uma lei de proteção de dados, recebeu certificação da União Europeia quanto ao nível de segurança no tratamento das informações, em razão da maior abrangência ao tratar do assunto em sua primeira lei sobre o tema, bem como o decreto que regulamenta e confere eficácia a Lei. Em uma análise geral, pode-se dizer que ela cria os órgãos de supervisão de proteção de dados e estabelece sanções em caso de descumprimento. Em virtude dessa organização e do reconhecimento dado pela União Europeia acerca de sua segurança, tem-se que a Lei Argentina de Proteção de Dados é uma excelente referência existente na América Latina e pode ser vista como um bom modelo para a regulamentação em outros países, motivo pelo qual será analisada com mais profundidade a seguir.

Neste sentido, em muitas ocasiões o direito à privacidade entra em conflito com o direito à informação, porque alguns dados, em respeito ao primeiro, devem ser protegidos e mantidos em segredo, podendo violar o direito à informação de outras pessoas. Em que pese serem ambos direitos reconhecidos como direitos fundamentais na maioria dos Estados, deve-se sempre objetivar um equilíbrio entre eles, evitando que a proteção de um interfira no outro (DELPECH, 2004, p. 279). É por este motivo que se encontra na Lei Argentina, por exemplo, a possibilidade de retificação, atualização ou supressão de dados, soluções que respeitariam tanto o direito à privacidade como o direito à informação. Entretanto, é importante ressaltar

que de acordo com o caso concreto deve-se analisar a melhor solução, “acomodando e situando” direitos dentro de uma perspectiva aceitável (BAUZÁ, 2013, p. 55).

Os dados pessoais estão caracterizados na legislação argentina como “informação de qualquer tipo referida a pessoas físicas ou de existência ideal determinadas ou determináveis” (ARGENTINA, 2000). Além da mera classificação como “informações”, deve-se lembrar de que a combinação de dados pessoais permite a obtenção de um perfil muito preciso dos interesses e atividades de um indivíduo, sendo que estes dados podem ser utilizados para fins diversos, principalmente comerciais e publicitários. Ademais, surgem outros riscos, mais preocupantes, como é o caso de roubo de identidade, para fins criminosos, ou até mesmo perda de um possível emprego, devido a buscas prévias acerca do candidato pela empresa que deseja contratar (DOMÍNGUEZ, 2013).

É diante deste contexto de utilização comercial (e também outros fins, em que se pode afetar a privacidade e a segurança) não autorizada pelos usuários que a existência de leis regulamentadoras ganha importância e se justifica. Como afirmou Sánchez Bravo (1998, p.53), ainda nos primórdios da Internet, a proteção de dados pessoais:

> “[...] frente a possíveis abusos informáticos, dentro do âmbito da liberdade dos cidadãos, vem determinada pelas exigências próprias de um Estado de Direito como proteção, não só da intimidade, senão também dos direitos e liberdades públicas em sentido amplo [...]”.

A construção da República Argentina acerca do direito à privacidade e à proteção de dados pessoais iniciou-se com a inclusão do artigo 1071 “bis” do Código Civil, que previa sanções àqueles que praticassem atos lesivos à intimidade alheia. A doutrina, na época, mostrou-se dividida acerca da eficácia da modificação, porque foi considerada por muitos como “[...] uma norma de regulamentação estéril” (DELPECH, 2004, p. 283). Também foi promulgada a Lei 24.766, que define sanções penais para os delitos de violação de segredos e para a ilegítima divulgação de informações de pessoas físicas ou jurídicas armazenadas em meios informáticos. Porém, estes crimes aplicam-se a bases de dados não estatais e definem somente pena de multa quando o autor não for funcionário público – única pena possível tendo em vista que a Lei aplica-se apenas a funcionários não estatais (ARGENTINA, 1996).

Por fim, em outubro de 2000, foi sancionada a Lei 25.326, conhecida por Lei de Proteção de Dados Pessoais, sendo seu decreto promulgado em novembro de 2001. Possui

como objetivo fundamental a proteção total de dados pessoais de bancos públicos ou privados destinados a fornecer informação16, com o fim de garantir o direito à honra e à intimidade das pessoas, consoante o art. 43 da Constituição Nacional da República Argentina (DELPECH, 2004, p. 285). Por ser uma lei nacional, tem alcance em todo território do país, além de proteger cidadãos argentinos e estrangeiros, dentro ou fora do país, e sempre que os dados estejam armazenados dentro do território argentino (ARGENTINA, 2000).

No pertinente à forma de coletar os dados, a Lei Argentina determina, em regras gerais, que estes devem ser determinados, certos, adequados e pertinentes de acordo com o âmbito e a finalidade para a qual foram colhidos. Somente podem ser captados de forma leal17 e legal18, não sendo possível utilizá-los para objetivos diversos dos informados aos titulares da informação, além de ser obrigatória a exatidão e atualização se necessário. Ainda, ao titular deve ser possível acessá-los, sendo imperativa a destruição dos dados quando não forem mais necessários ou pertinentes para os fins pelos quais foram recolhidos (ARGENTINA, 2000). A Lei 25.326 prevê expressamente, em rol taxativo, quais são os dados considerados sensíveis e quais as exceções em que poderão ser recolhidos. Isto porque a regra é a da proibição do tratamento destes dados, que poderão ser objeto de recolhimento em apenas cinco casos19: quando forem de relevante interesse geral, autorizado por lei; quando usadas para fins científicos ou de estatística e os titulares não possam ser identificados; em relação às associações religiosas ou organizações políticas, que poderão ter um registro de seus membros; com relação a dados relativos a antecedentes penais e contravenções, que poderão ser utilizados por autoridades públicas competentes; e, por fim, estão permitidos o recolhimento e tratamento de dados em estabelecimentos de saúde públicos ou privados e dos profissionais que tratam ou trataram o indivíduo, ressaltando-se os princípios do segredo profissional (ARGENTINA, 2000).

Ainda, no mesmo artigo sétimo, há a previsão da proibição (no parágrafo terceiro) de registros ou bancos de dados sensíveis mesmo com a autorização dos titulares da informação, ressalvando-se, por certo, as exceções acima previstas. Uma questão interessante prevista na lei e no decreto é a obrigatoriedade de registro de todos os arquivos, registros bases ou banco de dados públicos ou privados destinados a fornecer informações. Tal registro deve ser realizado junto à Direção Nacional de Proteção de Dados Pessoais, órgão de controle vinculado ao Ministério da Justiça e dos Direitos Humanos, destinado a realizar a fiscalização do cumprimento da lei e a auxiliar os indivíduos para o pleno exercício de seus direitos e tem

como principal objetivo justamente o controle junto os bancos de dados existentes (ARGENTINA, 2000).

Sendo referência na América Latina, os países vizinhos poderão utilizar-se desta Lei como uma diretriz para regulamentarem seus próprios Estados, que muitas vezes possuem maior número de internautas e, portanto, de cidadãos a ser protegidos.

4 ASPECTOS GERAIS DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Em 2018, foi aprovada no Congresso Nacional a Lei Geral de Proteção de Dados brasileira (LGPD). O processo público e legislativo começou em 2010, com a abertura de uma consulta pública sobre o tema, promovida pelo Ministério da Justiça, que resultou, posteriormente, na propositura do PL 5276/2016, anexado ao PL 4060/2012, perante a Câmara dos Deputados. Após anos de trâmite legislativo, consultas públicas, mais de 2500 contribuições de atores nacionais e internacionais, de todos os setores e inúmeros eventos, a lei foi sancionada pelo Ex-Presidente Michel Temer.

A LGPD criou novas regras para o uso de dados pessoais no Brasil, tanto no âmbito online quanto offline, nos setores privados e públicos. É importante ressaltar também que o país já dispunha de mais de quarenta normas que direta e indiretamente tratavam da proteção à privacidade e aos dados pessoais. Todavia, a LGPD vem com o objetivo de organizar as diversas e ineficazes leis de regulação, que por vezes eram conflituosas e causavam insegurança jurídica, tornando o país menos adequado no contexto de uma população mundial cada vez mais movida a dados. O texto legislativo, resultado de uma extensa discussão, visa não somente garantir direitos individuais, mas também fomentar o desenvolvimento econômico, tecnológico e a inovação por meio de regras claras e transparentes para o uso adequado de dados pessoais. Assim, ao ter uma Lei Geral, o Brasil passa a compor o rol de mais de 100 países que hoje podem ser considerados adequados para proteger a privacidade e o uso de dados.

Dentre os objetivos gerais da lei, podemos afirmar que esta visa garantir o direito à privacidade e à proteção de dados pessoais dos cidadãos ao permitir um maior controle sobre seus dados, por meio de práticas transparentes e seguras, visando garantir direitos e liberdades fundamentais. Além disso, as regras serão mais claras para empresas no que se refere a coleta, armazenamento, tratamento e compartilhamento de dados pessoais para entidades privadas

para fomentar o desenvolvimento econômico e tecnológico numa sociedade movida a dados. Essas ações irão fortalecer e aumentar a confiança da sociedade na coleta e uso dos seus dados pessoais, além de também proporcionar maior segurança jurídica como um todo no uso e tratamento de dados pessoais.

Também é importante ressaltar as vantagens da formulação de uma Lei Geral, dentre elas, a de que as regras serão únicas e harmônicas, independentes do setor da economia. Haverá uma importante e considerável redução de custos, visto que será possível diminuir custos operacionais causados por incompatibilidades sistêmicas de tratamentos feitos por agentes diversos, além de fomentar uma maior qualidade dos dados em circulação. Tornará o Brasil apto a maior interação internacional, na medida em que passará a processar dados oriundos de países que exigem um nível de proteção de dados adequados, o que pode fomentar, principalmente, os setores de tecnologia da informação. Por fim, a lei também promoverá mais liberdade de mercado, visto que indivíduos poderão transferir seus dados de um serviço para outro, aumentando a competitividade entre empresas.

Como dito acima, a LGPD não foi aprovada em pouco – pelo contrário, foram anos de intensa discussão, que levaram a um texto extremamente maduro quando comparado com a primeira versão de 2010.

Em suma, a LGPD terá um impacto na sociedade como poucas leis antes tiveram, uma vez que, hoje, praticamente toda e qualquer prática se vale do uso de dados pessoais. Empresas de todos os setores terão que se adaptar e uma nova cultura sobre o uso adequado de dados algo que dependerá de muito esforço de todos os setores levando em consideração que o Brasil, diferente de outras regiões do mundo, principalmente da Europa, ainda está iniciando o debate com relação a esse tema. Portanto, empresas precisam se adequar às regras de hoje e compreender que se antever à futura regulamentação é, também um investimento e uma vantagem competitiva. Em relação a isso os professores Renato Leite e Bruno Bioni afirmam que:

> É necessário ver o livre fluxo internacional de dados como um diferencial competitivo entre diferentes mercados. Um dos princípios basilares no tratamento de dados pessoais na sociedade em que o fluxo destes não respeita fronteira geográficas é a necessidade dos diferentes países onde os dados serão tratados oferecerem níveis adequados de proteção dos dados pessoais, para que os direitos garantidos aos cidadãos em uma jurisdição não sejam mitigados em outra com um sistema protetivo inferior.

Também é importante destacar os princípios da legislação. Um princípio fundamental que todas as atividades de processamento de dados devem seguir é o princípio da finalidade, que indica a correlação necessária que deve existir entre o uso dos dados pessoais e a finalidade comunicada aos interessados quando da coleta dos dados. Esse princípio é essencial para se limitar o acesso de terceiros ao banco de dados. De forma semelhante, ele também serve como parâmetro para julgar se determinado uso dos dados pessoais é adequado e razoável, de acordo com a finalidade informada no primeiro momento ao interessado (Doneda, 2006, p. 216). Por fim, esse princípio exige que o responsável pelo tratamento de dados estabeleça de forma expressa e limitada a finalidade do tratamento de dados, sob pena de se considerar ilegítimo o tratamento realizado com base em finalidades amplas ou genéricas (Rossnagel, 2003, p. 140).

O princípio da transparência, também chamado de princípio da publicidade, exige que a existência de um banco de dados pessoais seja de conhecimento público. Ele reafirma o preceito democrático, segundo o qual não podem existir bancos de dados sigilosos e baseia-se na ideia de que a transparência é uma das principais formas de se combaterem os abusos (Bennett, 1992, p. 156). Em contrapartida a esse direito de informação, surge para o banco de dados o dever de publicar seu nome, sede e conteúdo, em registros públicos, diários oficiais ou meios de grande circulação, sob pena de ineficácia desse direito. Em alguns países, exige-se autorização estatal prévia ou notificação ao órgão supervisor como pressuposto para o funcionamento dos bancos de dados.

Para possibilitar o controle do titular acerca dos seus dados, outro princípio relevante é o princípio do consentimento. Afinal, o exercício da liberdade de controle de dados pessoais baseia-se no consentimento do titular, que pode determinar um maior nível de proteção ou um maior fluxo dos seus dados. Segundo esse princípio, o consentimento deve ser consciente e informado, e apenas situações excepcionais (previstas legalmente) justificam o processamento de dados sem o prévio consentimento do titular.

Outro princípio relevante é o da qualidade dos dados. Ele se refere à exigência de que os dados constantes de um banco sejam objeto de um tratamento leal e lícito, sejam adequados pertinentes e não excessivos em relação à finalidade declarada, além de serem objetivos, exatos e atualizados. Tal princípio enseja cautela na formação do banco de dados, assim como demanda a sua constante atualização, de forma a impedir que os dados contidos restem ultrapassados com o passar do tempo.

No princípio da qualidade dos dados, incluem-se os direitos de acesso, retificação e cancelamento dos dados. O acesso refere-se ao direito do indivíduo de receber a informação acerca dos dados registrados sobre ele, quando assim o requisitar (Cueva, 1990, p. 187). Essa faculdade compreende o conhecimento sobre os dados armazenados, incluindo informações acerca da sua origem; sobre os organismos receptores das informações transmitidas ou a sua categoria; e sobre o objetivo do armazenamento. O direito de retificação e cancelamento dos dados visa assegurar a qualidade dos dados pessoais, de modo a corrigi-los em caso de equívoco ou cancelá-los, caso estejam obsoletos ou tenham sido indevidamente armazenados. Em caso de correção ou cancelamento dos dados, é direito do indivíduo que todos os organismos que receberam por transferência os seus dados sejam notificados para tomarem as devidas providências.

O princípio da segurança física e lógica refere-se à exigência básica de que qualquer banco de dados pessoais esteja protegido contra extravios, destruições, modificações e desvios não autorizados pelos interessados (Doneda, 2006, p. 217). Por fim, um importante princípio da matéria de proteção de dados pessoais é o princípio da responsabilidade, que visa assegurar a reparação adequada e integral dos danos materiais e morais causados ao indivíduo em razão da violação ao seu direito à privacidade.

Finalmente, faz-se necessário diferenciar as definições de dados pessoais, contidas no artigo 5º, sendo classificados de forma separada os dados pessoais, consistentes em "*informação relacionada a pessoa natural identificada ou identificável*" e dados sensíveis, consistentes em "*dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*". O tratamento de dados pessoais somente poderá ocorrer mediante a autorização prévia, gratuita, informada e inequívoca do titular (KUJAWSKI; THOMAZ, 2018, p. 3) e, em caso de dados sensíveis, o referido consentimento deverá ainda estar disposto em cláusula própria, separada das demais.

4.1 A Medida provisória 869/18 e a Autoridade Nacional de Proteção de Dados

No dia 28 de dezembro de 2018, foi publicado no Diário Oficial da União o texto da Medida Provisória n° 869 que, além de promover alterações na Lei Geral de Proteção de Dados, também cria a Autoridade Nacional de Proteção de Dados (ANPD). É importante

destacar que a MP n° 869/18 também altera a *vacatio legis* da LGPD para 24 meses, o que significa que a norma passa a entrar em vigor em agosto de 2020, e não mais em fevereiro de 2020. Ademais, durante este período de adaptação, a ANPD deverá exercer uma função colaborativa e consultiva, visando ajudar nos processos de adequação e conformidade com a nova lei. Tal período de adequação é extremamente importante para que tanto os cidadãos, quanto as empresa brasileiras, se conscientizem de que é extremamente importante a criação de uma cultura de proteção de dados no país.

No momento de sua promulgação, em agosto de 2018, a LGPD sofreu vetos presidenciais do Ex-Presidente da República Michel Temer, principalmente no que se refere aos artigos que constituíam e organizavam a ANPD e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. O veto foi justificado com o argumento de que houve "vício de iniciativa", ou seja, quando um poder propõe algo que não é de sua competência, neste caso, o Congresso Nacional. Assim, segundo ele, a iniciativa para a criação destes órgãos deveria vir do Poder Executivo, como foi feito por meio da Medida Provisória. Tal fato atrasou a criação de um órgão muito importante que é essencial, prejudicando a eficácia dos objetivos da LGPD. Até o presente momento, a Medida Provisória aguarda apreciação pelo Senado Federal.

Além disso, uma importante figura a ser mencionada é o encarregado, também conhecido como *Data Protection Officer* (DPO). De acordo com a MP, ele não precisa mais ser uma pessoa natural, abrindo espaço, desta forma, para a possibilidade de indicação de pessoas jurídicas, comitês, ou grupos de trabalho, que podem exercer tais funções. Ainda, deixa clara a possibilidade de terceirização de tal serviço.

Também foi revogada a previsão que impedia que a totalidade dos dados pessoais de banco de dados de segurança nacional e pública fosse tratada por pessoa de direito privado, permitindo agora que as controladas pelo Poder Público possam tratá-los; a possibilidade de requisição de relatórios de impacto à proteção de dados foi retirada, no caso de tratamentos para finalidades de segurança nacional e pública, o que pode influenciar nas obrigações de transparência pelo Poder Público.

Outras modificações também podem ser descritas como as obrigações de transparência e informações para o titular dos dados foram diminuídas quando o tratamento for fundamentado nas bases legais de cumprimento de obrigação legal e política pública; Foi

incluído inciso que deixa claro ser possível compartilhar dados de saúde quando a finalidade for a prestação de serviços de saúde suplementar, mesmo se houver obtenção de vantagem econômica. O que continua vetado é a comercialização simples e pura de dados de saúde (*raw data*); Não será mais necessária a revisão por pessoa natural de decisões totalmente automatizadas que afetem interesses dos titulares dos dados.

Com o novo texto, os titulares continuam a ter direito à revisão, mas não necessariamente por uma pessoa natural. A previsão de que a ANPD poderia realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais foi revogada, mas atribui-se à ANPD a competência para requisitar informações, a qualquer momento, aos controladores e operadores de dados pessoais que realizem operações de tratamento de dados pessoais; O Art. 26 trata do uso compartilhado de dados pessoais pelo Poder Público. O § 1º trata de exceções ao compartilhamento de tais dados com entes privados, aumentando o seu rol. Com a nova redação, fica possível a transferência de dados pessoais de responsabilidade do Poder Público para entidades privadas quando: (i) o ente privado tiver indicado um encarregado; quando houver previsão legal ou em instrumentos jurídicos administrativos; quando a transferência for para fins de prevenção à fraude, segurança e integridade do titular dos dados; e dados forem publicamente acessíveis;

As competências da ANPD foram alteradas quando comparadas com o texto enviado ao Congresso Nacional. Dentre as alterações significativas, destacam-se: Retirada de previsão expressa do poder de auditoria em entes privados e públicos para averiguar o cumprimento destes com as normas de proteção de dados, mantendo-se, todavia, o poder de requisição de informações e de fiscalização na hipótese de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo.

A ANPD deverá articular-se com as autoridades reguladoras públicas (como, por exemplo, BACEN e agências reguladoras) para exercer suas competências em setores específicos de atividades econômicas e governamentais sujeitas à regulação; Não estará mais dentre as suas obrigações elaborar a Política Nacional de Proteção de Dados Pessoais e da Privacidade, apesar de a Política ser mencionada na parte da MP que cria o Conselho Nacional de Proteção de Dados Pessoais e Privacidade; Haverá um fórum permanente de comunicação, inclusive por meio de cooperação técnica, com órgãos e entidades da administração pública que sejam responsáveis pela regulação de setores específicos da

atividade econômica e governamental, a fim de facilitar as competências regulatória, fiscalizatória e punitiva da ANPD.

Sendo assim, é possível que compreender a Autoridade Nacional de Proteção de Dados é de grande importância, pois diversos mecanismos de proteção de dados instituídos pela legislação dependem da atuação assertiva desse órgão. Conforme explicam os pesquisadores do Instituto de Tecnologia e Sociedade do Rio de Janeiro, Teffé e Mangeth:

> Sua autonomia e independência são, sem dúvidas, essenciais para a efetividade das proteções dispostas para a privacidade e os dados pessoais. Como a Autoridade deve ter entre suas funções a possibilidade de monitorar o próprio Estado, ela deve se encontrar em posição que lhe permita atuar sem intervenções indevidas.
>
> [...]
>
> Dispõe o referido PL que a Autoridade terá como atribuições, por exemplo, zelar pela proteção dos dados pessoais; estimular a adoção de padrões técnicos bem como de serviços e produtos que facilitem o exercício de controle pelos titulares sobre seus dados pessoais; fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação; promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança; promover ações de cooperação com autoridades de proteção de dados pessoais de outros países; dispor sobre as formas de publicidade das operações de tratamento de dados pessoais; solicitar às entidades do poder público, que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, a natureza dos dados e os demais detalhes do tratamento realizado; e realizar ou determinar a realização de auditorias, no âmbito da atividade de fiscalização, sobre o tratamento de dados pessoais efetuado pelos agentes de tratamento, incluindo o poder público.

Até então, diversos congressos e seminários foram realizados com o fim de amadurecer as discussões sobre a temática para, desse modo, fomentar a elaboração de propostas eficazes para a proteção dos dados e a salvaguarda dos direitos fundamentais envolvidos.

4.3 O impacto econômico de uma Lei Geral de Proteção de Dados

Nesse sentido, também pode-se dizer que uma Lei Geral de Proteção de Dados Pessoais visa fomentar o desenvolvimento econômico e tecnológico por meio de regras com o objetivo de assegurar os interesses de todos os setores de uma economia e sociedade cada vez mais movida por dados.

Assim, a iniciativa privada poderá se valer do fato de proteger seus dados pessoais corretamente como diferencial competitivo e uma vantagem econômica, o que faz com que a privacidade possa se tornar um importante elemento de competitividade, visto que os usuários poderiam, por exemplo, além de migrar para serviços que lhes sejam mais atraentes ou

inovadores, mas também optar pelos lhes forneçam maiores garantias no que concerne à proteção de seus dados pessoais.

Na obra literária “entre dados e robôs”, o professor doutor Eduardo Magrani discorre a respeito do tema e afirma que:

> Com a crescente difusão do Big Data e de técnicas de computação, a evolução tecnológica e a pressão econômica se espalharam rapidamente e os algoritmos se tornaram um ótimo recurso para inovação e para modelos de negócios. Esta rápida difusão dos algoritmos e sua crescente influência, porém, trazem consequências para o mercado e para a sociedade, o que inclui questões de ética e de governança. Tendo em vista que os algoritmos têm a capacidade de penetrar em inúmeros ramos de nossas vidas (inclusive colonizando o mundo da vida, conforme sustentado nesse trabalho) conforme se tornam mais sofisticados, úteis e autônomos, há o risco de que eles tomem decisões importantes no lugar de seres humanos.

Além disso, dentre os objetivos da nova legislação brasileira estão regras claras para empresas, devendo estar, estabelecer premissas básicas sobre coleta, armazenamento, tratamento e compartilhamento de dados pessoais para terceiros, no caso de comercialização desses ativos. Ademais, a lei também tem a função de promover desenvolvimento, fomentando o desenvolvimento econômico e tecnológico. E, por fim, garantir o direito do consumidor, garantindo também à livre-iniciativa e a livre concorrência.

5 CONCLUSÃO

O presente trabalho objetivou discutir a problemática de proteção dos dados pessoais, através da leitura aprofundada de artigos, doutrinas, relatórios e notícias, analisando o desenvolvimento dos direitos à privacidade e intimidade até o entendimento de proteção de dados pessoais como um direito fundamental do indivíduo. Transcorreu-se também sobre as aplicações de legislação relativas e pertinentes ao tema, bem como, a respeito da legislação da Argentina e do Regulamento 2016/679 da União Europeia. No primeiro capítulo, discorreu-se acerca do contexto histórico da problemática, o qual apontou uma dinâmica ímpar das relações sociais e da economia atual. Tratou-se também do desenvolvimento e evolução do direito à privacidade e intimidade, de onde, com o decorrer da história, e de novas necessidades, derivou o conceito de proteção de dados pessoais como um direito fundamental.

Em seguida, estudamos acerca das aplicações dos dados pessoais, e se conclui que seus usos são variados, sendo eles: para utilidade comercial, campanhas políticas, além de serem utilizados para fins de vigilância de governos e também para a governança eletrônica. Entendemos, ainda, que o manuseio dos dados pessoais, no contexto brasileiro, foram

acobertados tardiamente por um regulamento que defina limitações, de que modo e por quem pode se dar o tratamento dos dados pessoais nos âmbitos descritos.

Posteriormente, analisamos o Regulamento 2016/679 da União Europeia, com apontamentos acerca da efetiva proteção dos dados pessoais, com o objetivo de realizar um estudo comparativo com tal legislação modelo e estabelecer os devidos direitos dos titulares dos dados, analisando de forma podem corrigir as lacunas referentes aos agentes e as autoridades envolvidas, instituir uma autoridade fiscalizadora e possibilitar meios eficazes para a proteção dos dados pessoais.

A partir das considerações descritas, pode-se compreender que as legislações ao redor do mundo tentam responder aos seguintes questionamentos: como é possível controlar a maneira com que as empresas coletam os dados dos indivíduos? Se sim, quem está controlando essas informações? Quais são os limites do seu uso? E, a partir dessa discussão, entender como é possível proteger a privacidade. Assim, buscou-se demonstrar que esses questionamentos são de grande importância para os governos, para as empresas e também para a população exigir que mudanças sejam feitas.

Uma das principais ferramentas para conseguirmos proteger a nossa privacidade online é o país onde moramos ter uma excelente legislação de dados pessoais. Até a metade de 2018, o Brasil não tinha nenhuma lei específica de proteção de dados pessoais. Países como a Argentina tem, o Chile tem, o Uruguai tem e vários outros países latino-americanos.

Em relação a Europa, o Brasil já está atrasado há mais de trinta anos, visto que eles tem uma lei de proteção de dados desde a década de 70. Uma grande corrente de pesquisadores afirma que privacidade não existe, visto que depois da internet, ela pode ser vista como ilusória. Talvez você não se importe de compartilhar alguns dados, mas é preciso saber como eles são utilizados e a maioria dos usuários não sabe como isso é feito. Por isso, privacidade é um dos assuntos mais importantes do mundo que a gente vive hoje e vai continuar sendo pelas próximas décadas.

O fluxo de informação e dados em uma sociedade é algo positivo em muitos aspectos. Não se pode falar de privacidade e troca de dados, um em oposição ao outro. O importante é ter um fluxo apropriado de informações, levando sempre em consideração a quem pertencem esses dados e quem está enviando e recebendo essas informações. Assim, é

preciso que, de fato, a sociedade civil e instituições entendam os termos e as condições pelas quais essas informações estão sendo compartilhadas.

Conforme também foi exposto, a utilização comercial dos dados pessoais é um dos pontos que mais se deve proteger, porquanto de um lado há o interesse de diversas empresas e do setor público, que possuem vantagens técnicas e econômicas, e de outro, a sociedade civil como os titulares de dados pessoais. Ainda, outros apontamentos observados seria a possibilidade de introduzir na lei meios tecnológicos de fazer o resguardo dos dados e de importar da regulação europeia incentivos para que se alcancem os objetivos da lei, como são os casos dos selos medidores de privacidade.

Diante do que foi exposto, podemos concluir também que a validade do consentimento dos usuários aos Termos de Uso e Políticas de Privacidade de aplicações de internet independe da simples redação de referidos documentos. Trata-se de aspecto prático que, se não implementado corretamente, pode tornar ineficazes termos cuidadosamente redigidos, deixando as sociedades que operam em ambiente digital desprotegidas em caso de uma eventual disputa.

A Lei Geral de Proteção de dados demonstra que o ideal seria a consolidação de políticas de privacidade sensatas, feitas através de negociações que levem em conta as preocupações de indivíduos e demais setores da sociedade, visto que, como foi discutido anteriormente, se o indivíduo não tem privacidade perante o governo, pode estar sob orisco de governos totalitários e autoritários. Por isso, privacidade não é apenas um benefício a indivíduos, mas também a sociedade como um todo. O que culminou na demonstração exaustiva da legislação em resguardar a capacidade de comprovação de consentimento válido do usuário é uma dentre muitas questões fundamentais para a proteção de empresas digitais às altas multas cominadas pelo GDPR e pela lei recém aprovada no Brasil.

Em detrimento do que foi apresentado, entende-se que a melhor forma de proteger a privacidade dos cidadãos é a informação, entendendo, assim, como seus dados são coletados e monitorados para tomar as providências inclusive tecnológicas para fazer um mínimo de proteção de vida privada. Por isso, o Direito deve estimular o desenvolvimento de meios de regulação técnicos e sensíveis a valores éticos. Os dados e a inteligência artificial são dotados de imprevisibilidade, assim, devem ser orientados por valores constitucionalmente garantidos para que estejam alinhados com o Estado Democrático de Direito. Por fim, a sociedade civil,

governo e empresas devem atuar em conjunto para, entendendo o modelo de negócio proposto, sugerir soluções práticas capazes de garantir a validade e eficácia de Termos de Uso e Políticas de Privacidade.

REFERÊNCIAS

LEONARDI, Marcel. *Tutela e privacidade na internet*. São Paulo: Saraiva, 2012.

RODOTÀ, Stefano. *A vida na sociedade da vigilância*: a privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

BENNETT, Colin. *Regulating privacy. Data protection and public policy in Europe and UnitedStates.* Itahaca: Cornell University Press, 1992.

BRASIL. *Constituição: República Federativa do Brasil de 1988.* Brasília, DF: Senado Federal, 1988.

CASTELLS, Manuel. *A sociedade em rede (A era da informação, economia, sociedade e cultura).* São Paulo: Paz e Terra, 1999. v. 1.

GARFINKEL, Simson. *Database nation.* Sebastopol: O'Reillly, 2000.

LIMBERGER, Têmis. *O direito à intimidade na era da informática.* Porto Alegre: Livraria do Advogado, 2007.

LYON, David. The roots of the information society Idea. In: O'SULLIVAN, Tim; JEWKES, Yvonne (Ed.). *The media studies reader.* London: Arnold, 1998.

SAMPAIO, José Adércio Leite Sampaio. *Direito à intimidade e à vida privada.* Belo Horizonte: Del Rey, 1997.

WUERMELING, Ulrich. Harmonization of European Union Privacy Law. In: *14 John Marshall Journal of Computer & Information Law 411,* 1996.

FORTES, Vinicius Borges. *Os direitos de privacidade e a proteção de dados pessoais na internet.* Rio de Janeiro: Lumen Juris, 2016.

MARTINS, Guilherme Magalhães (Coord.). *Direito Privado e Internet.* São Paulo: Atlas, 2014.

MOSCHOVITOS, CJP. *History of the Internet: A Chronology, 1843 to the Present.* ABC-CLIO, 1999.

NIVER, H. *Tim Berners-Lee: Inventor of the World Wide.* Web. New York: Rosen Publishing, 2016.

PECK. P. *Direito Digital.* Ed.6. São Paulo: Saraiva, 2016

Cutait, R. (2018), *Privacidade na saúde*, publicado em 23.02.2018, disponível em: https://veja.abril.com.br/blog/letra-de-medico/privacidade-na-saude/, Acesso em 20.05.2019.

Falha de Segurança expõe dados de Milhares de pacientes do SUS, disponível em: https://canaltech.com.br/seguranca/falha-de-seguranca-expoe-dados-de-milhares-depacientes-do-sus-em-sao-paulo-72271. Acesso em 20/05/2019.

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

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

ARTIGO19. *Proteção de dados pessoais no Brasil: ANÁLISE DOS PROJETOS DE LEI EM TRAMITAÇÃO NO CONGRESSO NACIONAL.* 2017. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 20/05/2019.

BANISAR, Dave; GUILLEMIN, Gabrielle; BLANCO, Marcelo. *Proteção de dados pessoais no Brasil - Análise dos projetos de lei em tramitação no Congresso Nacional*. 2017. Disponível em: <http://artigo19.org/wp-content/blogs.dir/24/files/2017/01/Proteção-de-Dados-Pessoais-no-Brasil-ARTIGO-19.pdf>. Acesso em: 20/05/2019.

BBC BRASIL. *5 coisas que você talvez não saiba sobre o Facebook reveladas por Zuckerberg em depoimento*. 2018. Disponível em: <https://www.bbc.com/portuguese/geral-43727418>. Acesso em: 20/05/2019.

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

BRAGA, Lamartine Vieira; ALVES, Welington Souza; FIGUEIREDO, Rejane Maria da Costa; SANTOS, Rildo Ribeiro. *O papel do Governo Eletrônico no fortalecimento da governança do setor público.* Disponível em: <https://search.proquest.com/openview/e683eeaa069b662aed4a721ef686e187/1?pq-origsite=gscholar&cbl=2045880>. Acesso em: 20/05/2019.

BRASIL. *LEI Nº 12.965, DE 23 DE ABRIL DE 2014. Marco Civil Da Internet*. Brasília, 10 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 20/05/2019.

BURCH, Sean. *Facebook Is "Rotten", Privacy Is Its "Kryptonite", Says Ex-FTC Advisor: Social network's business model is at odds with protecting its users, according to one expert*. 2018. Disponível em: <https://www.thewrap.com/facebook-privacy-kryptonite-ftc/>. Acesso em: 20/05/2019.

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

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

CELLA, José Renato Gaziero; COPETTI, Rafael. *COMPARTILHAMENTO DE DADOS PESSOAIS E A ADMINISTRAÇÃO PÚBLICA BRASILEIRA*. Disponível em: <http://indexlaw.org/index.php/revistadgnt/article/view/2471/pdf>. Acesso em: 20/05/2019.

CHARLEAUX, João Paulo. *O que é o Vault 7, o "maior vazamento da história da CIA", segundo o Wikileaks*. Disponível em: <https://www.nexojornal.com.br/expresso/2017/03/07/O-que-é-o-Vault-7-o-maior-vazamento-da-história-da-CIA'-segundo-o-Wikileaks>. Acesso em: 21/05/2019.

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

CÓRDOVA, Yasodara; DONEDA, Danilo. *Um lugar para os robôs (nas eleições): A utilização de APIs para o controle das informações que circulam em redes de bots*. 2017. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/um-lugar-para-os-robos-nas-eleicoes-20112017>. Acesso em: 21/05/2019.

DANCE, Gabriel J.x. CONFESSORE, Nicholas; LAFORGIA, Michael. Facebook Gave Device Makers Deep Access to Data on Users and Friends: The Company formed data-sharing partnerships with Apple, Samsung and dozens of other device makers, raising new concerns about its privacy protections. 2018. Disponível em: <https://www.nytimes.com/interactive/2018/06/03/technology/facebook-device-partners-users-friends-data.html>. Acesso em: 21/05/2019.

DATA PRIVACY BRASIL. A GDPR não aplica somente a dados de cidadãos europeus! Vamos acabar com esse mito! Disponível em: <http://dataprivacy.com.br/a-gdpr-nao-aplica-somente-a-dados-de-cidadaos-europeus-vamos-acabar-com-esse-mito/>. Acesso em: 21/05/2019.

DATA PRIVACY BRASIL. Esqueça as multas da GDPR! A sua real preocupação deve ser outra: contratos! Disponível em: <http://dataprivacy.com.br/esqueca-as-multas-da-gdpr-a-sua-real-preocupacao-deve-ser-outra-contratos/>. Acesso em: 21/05/2019.

DOTTI, Renè Ariel. Proteção Da Vida Privada e Liberdade de Informação. São Paulo: RT, 1980.ELIAS, Paulo Sá. Algoritmos, Inteligência Artificial e o Direito. Disponível em:

<https://www.conjur.com.br/dl/algoritmos-inteligencia-artificial.pdf>. Acesso em: 21/05/2019.

ELOLA, Joseba. O reconhecimento facial abre caminho para o pesadelo de George Orwell: Tecnologia ameaça a privacidade das pessoas e abre as portas à distopia descrita no livro '1984'. Por outro lado, permite identificar em tempo recorde terroristas logo após cometerem atentados. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/01/05/tecnologia/1515156123_044505.html>. Acesso em: 21/05/2019.

ÉPOCA NEGÓCIOS. Facebook admite que coleta dados de quem não tem conta na plataforma: A revelação foi feita hoje pelo presidente da companhia, Mark Zuckerberg, durante audiência. 2018. Disponível em: <https://epocanegocios.globo.com/Tecnologia/noticia/2018/04/facebook-admite-que-coleta-dados-de-quem-nao-tem-conta-na-plataforma.html?utm_source=facebook&utm_medium=social&utm_campaign=post>. Acesso em: 21/05/2019.

FARIAS, Edilsom Pereira de. Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação. Porto Alegre: Sérgio Antônio FOXX, Chris. Google e Facebook são acusados de violar nova lei de proteção de dados da Europa. 2018. Disponível em: <https://www.bbc.com/portuguese/internacional-44259419https://www.bbc.com/portuguese/internacional-44259419>. Acesso em: 21/05/2019.

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

G1. Dados de 2,7 milhões de europeus no Facebook foram usados de forma 'inadequada' pela Cambridge Analytica: Rede social admitiu que 87 milhões de usuários tiveram dados explorados por consultoria políticas, mas não listava cidadãos da União Europeia. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/dados-de-27-milhoes-de-europeus-no-facebook-foram-usados-de-forma-inadequada-pela-cambridge-analytica.ghtml>. Acesso em: 21/05/2019.

G1. EUA confirmam que Facebook é investigado por acesso não consentido a dados de mais de 50 milhões de usuários: Rede social pode ser multada por não proteger informações pessoais e prejudicar consumidores. 2018. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/eua-confirmam-que-facebook-e-investigado-por-acesso-nao-consentido-a-dados-de-mais-de-50-milhoes-de-usuarios.ghtml>. Acesso em: 21/05/2019.

GADELHA, Julia. A evolução dos computadores. Disponível em: <http://www2.ic.uff.br/~aconci/evolucao.html>. Acesso em: 21/05/2019.

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

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

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

GUGIK, Gabriel. A história dos computadores e da computação. Disponível em: <https://www.tecmundo.com.br/tecnologia-da-informacao/1697-a-historia-dos-computadores-e-da-computacao.htm>. Acesso em: 21/05/2019.

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

GUILHERME, Paulo. Por que o Facebook comprou o WhatsApp e o Instagram? Este gráfico explica. 2014. Disponível em: <https://www.tecmundo.com.br/facebook/60080-facebook-comprou-o-whatsapp-o-instagram-grafico-explica.htm>. Acesso em: 21/05/2019.

IGLESIAS, Daphne. Privacidade em perspectivas: Nudging Privacy: Benefits and Limits of Persuading Human Behaviour Online. Organizadores: Sérgio Branco e Chiara de Teffé. Rio de Janeiro: Lumen Juris, 2018.ITAGIBA, Gabriel. Fake news e Internet: esquemas, bots e a disputa pela atenção.2017. Disponível em: <https://itsrio.org/wp-content/uploads/2017/04/v2_fake-news-e-internet-bots.pdf>. Acesso em: 21/05/2019.

ITSRIO. Anteprojeto de lei de proteção de dados pessoais: Contribuição do ITS para o debate público. 2015. Disponível em: <https://itsrio.org/wp-content/uploads/2015/07/Consulta-APL-de-Dados.pdf>. Acesso em: 21/05/2019.

ITSRIO. PegaBot: Descubra se aquele perfil de rede social é bot. Plataforma em fase de testes. Disponível em: <https://itsrio.org/pt/projetos/pegabot/>. Acesso em: 21/05/2019.

LAZARI, Rafael de. Noções de Direito Constitucional. Disponível em: <https://www.novaconcursos.com.br/media/wysiwyg/Retificacoes/2-Nocoes-de-direito-constitucional.pdf>. Acesso em: 21/05/2019.

LEMOS, Ronaldo. Governo é acusado de vender dados: Proteção de dados pessoais precisa valer também para o setor público. Disponível em: <https://www1.folha.uol.com.br/colunas/ronaldolemos/2018/06/governo-e-acusado-de-vender-dados.shtml?loggedpaywall#_=_>. Acesso em: 21/05/2019.

FREDOOM HOUSE. Manipulating Social Media to Undermine Democracy. Disponível em: <https://freedomhouse.org/report/freedom-net/freedom-net-2017>. Acesso em: 21/05/2019.

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

MENDONÇA, Renata. Como os testes de Facebook usam seus dados pessoais e como empresas ganham dinheiro com isso. 2018. Disponível em: <http://www.bbc.com/portuguese/salasocial-43106323>. Acesso em: 21/05/2019.

MONTEIRO, Renato Leite. A nova Regulação de Proteção de Dados Pessoais aprovada na União Europeia e sua influência no Brasil. Disponível em: <https://renatoleitemonteiro.jusbrasil.com.br/artigos/273633610/a-nova-regulacao-de-protecao-de-dados-pessoais-aprovada-na-uniao-europeia-e-sua-influencia-no-brasil>. Acesso em: 21/05/2019.

MORSE, Jack. Facebook bug affected 14 million people's privacy settings. 2018. Disponível em: <https://mashable.com/2018/06/07/facebook-public-settings-14-million-bug/#Wnk.aQAXliqn>. Acesso em: 21/05/2019.

NETTO, Andrei. NSA e CIA espionaram eleições francesas de 2012, diz WikiLeaks: Agências de inteligência americanas queriam detalhes sobre as relações do ex-presidente Nicolas Sarkozy com assessores, seus meios de financiamento e detalhes de outros 'candidatos emergentes' ao Palácio do Eliseu. Disponível em: <https://internacional.estadao.com.br/noticias/geral,nsa-e-cia-espionaram-eleicoes-francesas-de-2012-diz-wikileaks,70001668941>. Acesso em: 21/05/2019.

PAYÃO, Felipe. WikiLeaksvaza documentos: CIA vigia o seu Android, iPhone e smart TV. Disponível em: <https://www.tecmundo.com.br/wikileaks/114808-wikileaks-vaza-documentos-cia-vigia-android-iphone-smart-tv.htm>. Acesso em: 21/05/2019.

PEREIRA, Ana Paula. O que é algoritmo? Disponível em: <https://www.tecmundo.com.br/programacao/2082-o-que-e-algoritmo-.htm>. Acesso em: 21/05/2019.

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

SANTOS, Coriolano Aurélio de Almeida Camargo; CRESPO, Marcelo. Inteligência artificial, tecnologia e o Direito: o debate não pode esperar! Disponível em: <http://www.migalhas.com.br/DireitoDigital/105,MI249734,41046-Inteligencia+artificial+tecnologia+e+o+Direito+o+debate+nao+pode>. Acesso em: 21/05/2019.