PRIVACIDADE e LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

PRIVACY AND GENERAL PERSONAL DATA PROTECTION LAW

Maria Eugenia Finkelstein

Mestre em Direito Comercial pela Pontifícia Universidade Católica de São Paulo.
Doutora em Direito Comercial pela Faculdade de Direito da Universidade de São Paulo.
Professora da Faculdade de Direito da Pontifícia Universidade Católica de São Paulo.
Professora convidada do Instituto de Empresa de Madrid, Espanha e da Universidad de Castilla La Mancha (Albacete, Espanha).
E-mail: eugenia@finkelstein.com.br

Claudio Finkelstein

Doutor em Direito pela Pontifícia Universidade Católica de São Paulo e Livre-Docência pela Pontifícia Universidade Católica.Mestre em Direito Internacional - University of Miami. Professor da Pontifícia Universidade Católica de SP. Diretor do Instituto Nacional do Contencioso Econômico e do Instituto Brasileiro de Direito Constitucional e vice Presidente da Sociedade Brasileira de Direito Internacional.
E-mail: claudio@finkelstein.com.br

Recebido em: 07/01/2019
Aprovado em: 29/08/2019

RESUMO: É notório que desde o advento da internet, a coleta de dados invadiu sobremaneira a privacidade das pessoas. Novas normas se faziam necessárias à proteção da privacidade na sociedade da informação. A Lei Geral de Proteção de Dados vem solucionar esse problema. A análise de dados viabiliza diversas práticas comerciais e melhora o desempenho do sistema, diminuindo os riscos e ampliando a circulação de produtos e serviços, possibilitando, inclusive, o desenvolvimento tecnológico. Além disso, também há o interesse público na coleta e utilização de dados, tanto para a segurança pública, quanto para fins de investigação criminal e combate a ilícitos, por exemplo. Portanto, com uma análise do conceito de privacidade e da importância da Lei Geral de Proteção de Dados Pessoais, pretende-se nesse escrito responder por que a preocupação com a proteção de dados aprofunda-se na medida em que a economia migra para o meio digital.

Palavras-chave: Privacidade. GDPR. LGPD. Dados Pessoais, dados Pessoais Sensíveis, Tratamento de dados.

ABSTRACT: It is well known that since the advent of the internet, data collection has greatly invaded people's privacy. New rules were necessary to protect privacy in the information society. The General Data Protection Law solves this problem. Data analysis enables various commercial practices and improves the system's performance, reducing risks and expanding the circulation of products and services, including enabling technological development. In addition, there is also a public interest in the collection and use of data, both for public security and for the purposes of criminal investigation and combating illicit acts, for example. Therefore, with an analysis of the concept of privacy and the importance of the General Law for the Protection of Personal Data, it

is intended in this writing to answer why the concern with data protection deepens as the economy migrates to the digital environment.

Key-words: Privacy. GDPR. LGPD. Personal Data. Sensible Personal Data Data Treatment

SUMÁRIO: Introdução; 1 Conceito de Privacidade; 2 Necessidade de Proteção; 3 Evolução Legislativa; 4 A Lei no. 13.709/18 (LGPD); 4.1 Da Definição de Dados Pessoais; 4.2 Do tratamento dos Dados Pessoais; 4.3 Dos dados Pessoais Sensíveis; 4.4 O tratamento de dados pessoais pelo Poder Público; 4.5 Descumprimento à LGPD; Considerações Finais; Referências.

INTRODUÇÃO

O presente artigo visa analisar o conceito de privacidade, bem como correlacioná-lo com a nova Lei Geral de Proteção de Dados Pessoais (Lei no. 13.709/18).

Antes de mais nada, é preciso entender que a legislação aplica-se à captação, armazenamento e disseminação de dados no meio físico ou eletrônico, mas que o assunto tornou-se premente em face da maior facilidade de captação de dados no meio eletrônico.

Dados sempre foram importantes para que os fornecedores pudessem orientar e programar suas práticas comerciais. Assim, a importância da utilização desses dados dá-se para fins econômicos. A análise de dados viabiliza diversas práticas comerciais e melhora o desempenho do sistema, diminuindo os riscos e ampliando a circulação de produtos e serviços, possibilitando, inclusive, o desenvolvimento tecnológico. Além disso, também há o interesse público na coleta e utilização de dados, tanto para a segurança pública, quanto para fins de investigação criminal e combate a ilícitos, por exemplo.

Mas, por que a preocupação com a proteção de dados aprofunda-se na medida em que a economia migra para o meio digital?

Com o desenvolvimento da tecnologia e intensificação dos fluxos de informação, surgem novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, refletindo em mudanças no conceito de direito à privacidade, de modo que a informação que antes era dispersa, torna-se organizada. Riscos que envolvem a violação à privacidade e à personalidade dos cidadãos na sociedade da informação crescem exponencialmente, como a possibilidade de uso indevido dos dados pessoais, cadastro e classificação dos indivíduos, propagandas de *marketing* invasivas, publicidade comportamental, vigilância estatal, utilização indevida da *Big Data*, coleta de dados através da *Internet* das coisas, entre outros.

Para tanto, vamos estudar, ainda que de maneira breve, o conceito de privacidade, para podermos entender melhor a análise da importância da Lei Geral de Proteção de Dados Pessoais.

Apesar de sua substantivação no direito brasileiro, a disciplina da proteção de dados ainda não é praticada amplamente no Brasil. Afinal, a Lei Geral de Proteção de Dados Pessoais somente entrará em vigor em agosto de 2020, para fins de cumprimento pelos agentes econômicos, com exceção de seu artigo 65, I. Ainda, existem diversas omissões que apenas poderão ser sanadas pela Agência Nacional de Proteção de Dados (ANPD), em futura regulamentação.

1 CONCEITO DE PRIVACIDADE

O conceito de privacidade é difícil de ser definido. Apesar disso, a privacidade é defendida na Declaração Universal dos Direitos Humanos Constituição Federal do Brasil,

assegurado pelo Código Civil, Penal, de Defesa do Consumidor, e protegido por leis esparsas. No direito norte-americano é comum a definição de privacidade como "*the right to be left alone.*[1]"

No texto constitucional, o tema ganhou status de direito fundamental, principalmente ao resguardar a inviolabilidade da correspondência, bem como o direito à intimidade e à vida privada.[2] Tal abordagem, entretanto, utilizou o termo privacidade como sinônimo de intimidade, e acabou por gerar uma dualidade na conceituação da privacidade por parte da doutrina. *"O direito à intimidade é quase sempre considerado como sinônimo do direito à privacidade. Esta é uma terminologia do direito americano (Right of Privacy), para designar aquele, mais empregada no direito dos povos latinos"*.[3]

A Constituição Federal prevê também o direito do cidadão de não ter revelado os fatos que não deseja, tutelando, portanto, o âmbito cível e até mesmo penal, para responsabilizar o infrator do ilícito gerado, mas principalmente com sanção patrimonial.

Já no Código Civil, a questão da privacidade também foi levada em consideração, embora que de forma genérica. A abordagem ocorre no Livro I "Das Pessoas", destacando a proteção de divulgação de escritos, da transmissão da palavra, e da exposição ou utilização da imagem das pessoas físicas ou jurídicas que poderão ser proibidas de imediato, inclusive se o intuito for apenas comercial, sem falar em prejuízo no tocante à fama, honra e respeitabilidade, questões também protegidas pelas normas citadas.

Desse modo, é compreensível que a vida privada consiste naquilo que é particular ao indivíduo. Nesse sentido a privacidade figura como gênero na qual a intimidade atua como espécie.

A importância ao direito de privacidade é tão vasta que serve de pilar à proteção do direito de personalidade. Maria Helena Diniz comenta os ensinamentos de Gofredo Telles Júnior:

> *"a personalidade consiste no conjunto de caracteres próprios da pessoa. A personalidade não é um direito, de modo que seria errôneo afirmar que o ser humano tem direito à personalidade. A personalidade é que apóia os direitos e deveres que dela se irradiam, é objeto de direito, é o primeiro bem da pessoa que lhe pertence como primeira utilidade..." 4*

Sob esse prisma é possível identificar que o direito de personalidade, visa preservar e garantir o desenvolvimento do indivíduo, defendendo-o de agressões praticadas contra a sua identidade intelectual, física e moral.

É preciso deixar claro que, assim como na constituição, na língua portuguesa "intimidade" também é utilizada como sinônimo de "privacidade". No campo do Direito, Paulo José da Costa discorreu acerca da intimidade, definindo-a como:

> *"a necessidade de encontrar na solidão aquela paz e aquele equilíbrio, continuamente prometidos pela vida moderna; de manter-se a pessoa, querendo, isolada, subtraída ao alarde e à publicidade, fechada na sua intimidade, resguardada dos olhares ávidos. A intimidade corresponderia à vontade do indivíduo de ser deixado só".*

---

[1] *The right to be left alone – the most comprehensive of rights and the right most valued by a free people*. Olmstead v. U.S. (1928) – Juiz Louis Brandeis.

[2] A privacidade e os arquivos de consumo na internet - uma primeira reflexãoRevista de Direito do Consumidor | vol. 41/2002 | p. 151 - 165 | Jan - Mar / 2002
Doutrinas Essenciais de Responsabilidade Civil | vol. 8 | p. 1151 - 1168 | Out / 2011 | DTR\2002\720

[3] SILVA, José Afonso da. Curso de Direito Constitucional Positivo, 10. ed., São Paulo, Malheiros Editores, 1992, p.202.

[4] Nota apud DINIZ, Maria Helena. Curso de Direito Civil Brasileiro, Teoria Geral do Direito Civil, 1. vol., São Paulo, Ed. Saraiva, 1982, p.81.

Além disso, na concepção de Ada Pellegrini Grinover,[5] o direito à intimidade integra múltiplas manifestações dos direitos da personalidade como o direito à imagem, à defesa do nome, à tutela da obra intelectual, à inviolabilidade do domicílio, ao direito ao segredo, representando assim, um atributo da personalidade.

Outros autores apresentam uma perspectiva diferente, segundo a qual o direito à intimidade já significaria uma premissa geral da personalidade e da capacidade jurídica. O objeto do direito à vida privada pode ser definido como a intimidade por ele preservada refletindo, assim, valores materiais, morais e espirituais, como um bem jurídico.

Tomemos como exemplo o monitoramento como elemento de invasão da privacidade. Via de regra, referido fator é caracterizado pela sua transitoriedade – se somos observados ao andar pela rua, se não estivermos fazendo nada fora do comum, seremos esquecidos em seguida. Assim, em relação à investigação – que é de caráter permanente – o monitoramento é considerado elemento menos relevante de invasão da privacidade. Porém, caso surja uma tecnologia que elimine o caráter de transitoriedade do monitoramento, seu efeito sobre a privacidade será mais relevante. [6]

Um marco na história da privacidade veio do advento da evolução tecnológica, bem como dos meios de comunicação, o desenvolvimento da internet e o surgimento das redes sociais, verdadeiros palcos da exposição do cotidiano. O monitoramento da vida íntima foi extremamente facilitado pelas novas tecnologias, restando cada vez mais frágil a tutela a estes direitos protegidos.

George Orwell previa em sua obra 1984, publicada ainda em 1949, uma verdadeira transgressão de privacidade que ocorreria futuramente em consonância com os avanços tecnológicos. Os indivíduos eram relatados como verdadeiras marionetes da tecnologia, que servia como ferramenta para o controle total dos indivíduos, destruição ou manipulação da memória histórica dos povos e guerras para assegurar a paz. O Estado se classifica como um verdadeiro *"big brother*", o "grande irmão" do cidadão ao vigiar a todos, sacrificando sua intimidade e privacidade em troca da "paz", criando padrões e zelando por todos na tendência de evitar a desordem mundial

A Internet constitui o maior exemplo de como as tecnologias de monitoramento e investigação têm evoluído. É praticamente impossível ter qualquer movimentação na rede que não seja incorporada por alguma empresa, vide o atual exemplo do Google ou do Facebook, ou aplicativos como Waze e Uber, que cada vez mais ampliam o gênero de dados que adquirem de seus usuários[7]. Além disso, é importante ressaltar que local costumeiro da vida privada – a residência - é reservado, e firma-se longe das vistas da comunidade, ocultando-se do público.

Há também entidades denominadas provedores de vias que identificam precisamente onde, quando e quão rápido o indivíduo acessou cada *site*, documentando que lojas visitou, por quais *links*[8] se interessou, em qual ordem e por quanto tempo. Ademais, os dados coletados neste monitoramento cibernético são permanentes e, portanto, investigáveis por qualquer pessoa que tenha interesse em ter acesso a essas informações. Assim, podemos ver que neste caso específico, o aumento do que é monitorado implica o aumento do que é investigável.

---

[5] GRINOVER, Ada Pellegrini. Liberdades Públicas e Processo Penal. As Intervenções Telefônicas. São Paulo, Saraiva, 1978.

[6] É de se notar que desde os ataques terroristas de 11 de setembro de 2001, várias agências governamentais estão reforçando o caráter de permanência do monitoramento, com quase que integral aceitação da opinião pública. Neste sentido, é de se mencionar o projeto americano Registro de Informação total, coordenado pelo Departamento de Defesa, ainda em fase de pesquisa, batizado pela imprensa de "Grande Irmão", em alusão ao livro de George Orwell, 1984. Revista Veja, 27 de novembro de 2002, p. 87.

[7] https://brasil.elpais.com/brasil/2019/06/12/tecnologia/1560347825_866607.html - acesso em 17/06/2019

[8] Conexão, ou seja, elementos físicos e lógicos que interligam os computadores da Rede. Na *Web* são palavras-chaves destacadas em um texto, que, quando clicadas, nos levam para o assunto desejado, em outro arquivo ou servidor.

2 NECESSIDADE DE PROTEÇÃO

Nesse contexto, a questão da privacidade na Internet vem cada vez mais recebendo atenção das cortes internacionais,[9] uma vez que o seu tênue limite é cada vez mais invadido pela tecnologia.

Ademais, sempre que um usuário adentra um *site*, preenche formulários virtuais. E o que é pior, não se sabe se os dados fornecidos são verdadeiros nem se pode ter certeza acerca da forma de utilização desta informação.

Sabe-se que na atual fase tecnológica em que a sociedade se encontra,[10] a informação é um dos bens de maior valor. Por esta razão, a sua proteção deve ser questão de importância máxima, merecendo a atenção do legislador.

Claro está que o desenvolvimento tecnológico não apresenta somente aspectos negativos. A evolução da tecnologia dos mecanismos de monitoramento proporciona uma queda no tempo e nas despesas envolvidas em buscas. Já para aquele que está sendo investigado, existe a consciência de saber que sua privacidade pode estar sendo invadida. Assim, com a evolução das tecnologias de monitoramento, de um lado, a pessoa que busca as informações o faz muito mais rapidamente e a baixo custo econômico e, de outro lado, a pessoa investigada tem menor possibilidade de aperceber-se disso, e assim não sofre o inconveniente referido acima, presenciamos nesse particular o surgimento de uma nova ética, mitigando conceitos pré-estabelecidos em troca de um bem maior, que é a manutenção da paz.

Lessig[11] esclarece esse ponto por meio de um exemplo. Suponhamos que o FBI[12] desenvolva um programa para investigar computadores à procura de um arquivo ilegal específico, sem que o usuário do computador investigado sequer perceba. Suponhamos, ademais, que esse programa não possa detectar nada além desse arquivo ilegal e que, não encontrando o arquivo ilegal, o programa se autodestrua. Estaria este programa do FBI violando o princípio da privacidade? Lessig entende que certamente há um senso de invasão de propriedade, mas que a 4ª Emenda à Constituição norte-americana não está mais atrelada à invasão da privacidade e, sim, à razoabilidade da invasão da privacidade. Como a busca neste caso só será inconveniente para os culpados, o autor considera, que em hipóteses como esta, a invasão é razoável.

O aumento da eficiência nos métodos de monitoramento e investigação proporciona maior facilidade para manter, utilizar e coletar informações. É justamente o que ocorre na Internet. Nesse âmbito, a informação é coletada invisivelmente, eficientemente e sem inconvenientes para o usuário. A informação é mais facilmente obtida e as proteções legais contra essa busca desaparecem.

Lessig[13] apontou, ainda, como eventual meio alternativo à ausência de leis que protejam a privacidade, a inserção de ineficiências nas tecnologias sendo desenvolvidas, que dificultem o uso indevido das mesmas. Isso porque um sistema totalmente eficiente pode ser mais danoso do que um menos eficiente, quando controlado por pessoa mal intencionada. Como, de acordo com o autor, estas tecnologias de monitoramento são utilizadas principalmente pelos governantes de

[9] Nos Estados Unidos: United States v. Hambrick, W.D. Va., filed 7/7/99; Mclaren v. Microsoft Corp., Texas Ct. App., Dallas, filed 5/28/99; Vega-Rodriguez v. Puerto Rico Telephone Co., CA 1, filed 4/8/97; Condon v. Reno, DC SC, filed 9/11/97; Oklahoma v. United States, DC Okla, filed 9/17/97, in www.fd.unl.pt, disponível em 2 de agosto de 2002.

[10] Quer-se dizer, Sociedade da Informação.

[11] L. Lessig. *Architecture of Privacy*, disponível no *site* http://lawschool.stanford.edu/faculty/lessig/, em 8 de maio de 2002.

[12] Sigla que significa *Federal Bureau of Investigation* (departamento norte americano federal de investigação).

[13] L. Lessig. *Architecture of Privacy*, disponível no *site* http://lawschool.stanford.edu/faculty/lessig/,em 8 de maio de 2002.

diferentes países, os artifícios que fazem com que referidos sistemas sejam menos eficientes servem para prevenir o abuso de poder governamental, e são, portanto, um instrumento de salvaguarda da privacidade. Como exemplo de sistemas de limitação da eficiência governamental, Lessig menciona a tripartição do poder no sistema democrático. A atuação do Poder Executivo é limitada pela atuação dos demais poderes e vice-versa. Da mesma forma, um sistema tecnológico totalmente eficiente deveria ser limitado por certos artifícios. Ainda, aponta o fato do controle exercido sobre os mecanismos de controle na Internet ser realizado pelo governo. O autor entende que isto é danoso para a comunidade de usuários. Para Lessig, todo controle exercido por um ente externo – ou seja, que não faça parte de determinada comunidade (como é o caso do governo em relação à comunidade de usuários da Internet) – faz com que esta comunidade perca a prática do exercício de tal controle, e assim perca sua identidade como comunidade. Portanto, Lessig acredita que os controles sobre referidos mecanismos devem ser feitos pela própria comunidade de usuários.

Para muitos, a invasão de privacidade é absolutamente inadmissível. Porém, é de se lembrar que não são todas as informações que merecem proteção jurídica. Neste sentido, Cláudio de Lucena Neto,[14] citando Dmitri Abreu e Sean Boran classificou as informações da seguinte forma:

> - "pública – informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, e cuja integridade não é vital;
> - interna – o acesso a esse tipo de informação deve ser evitado, embora as consequências do uso desautorizado não sejam por demais sérias. Sua integridade é importante, porquanto não seja vital;
> - confidencial – informação restrita aos limites da empresa, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
> - secreta – informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia."

No Brasil a proteção da privacidade é princípio constitucional previsto pelos incisos X, XI e XII, do artigo 5º, da Constituição Federal de 1988.[15]

É de se salientar que o estudo da privacidade do usuário da Rede é uma das matérias que se inserem entre as mais importantes da Sociedade da Informação e que acaba estando relacionada ao Comércio Eletrônico, uma vez que são os *sites* de comércio eletrônico os principais coletores de informações na Rede.

Dentro do tema privacidade na Internet, são três os pontos que merecem destaque:

> (i) a privacidade do usuário invadida pela montanha de *junk mail*[16] ou *spams*[17] que um usuário recebe sem pedir nem desejar;

[14] D. Abreu e S. Boran. *Melhores práticas para classificar as informações e The IT security cookbook information classification, apud* C. L. Neto. *Função social da privacidade,* in www.jus.com.br em 2 de agosto de 2002.

[15] "X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação"; "XI – a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial"; e XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

[16] *Junk mail* significa mensagem de correio eletrônico não solicitada, enviada a muitos destinatários, com conteúdo genérico.

(ii) a privacidade do usuário garantida pela Constituição Federal,[18] que determina invioláveis a intimidade, a casa e o sigilo da correspondência,[19] das comunicações telegráficas, de dados e das comunicações telefônicas, salvo por ordem judicial; e

(iii) a privacidade do usuário em si, pois por vezes seus dados pessoais e hábitos de consumo são comercializados.

A questão da privacidade do consumidor eletrônico vem atormentando legisladores ao redor do mundo[20]. Stéfano Rodotá[21] informa que a definição da privacidade como o direito de ser deixado só perdeu o sentido na sociedade da informação. Agora, a privacidade abrange novas dimensões relativas à coleta e tratamento de dados pessoais. Há, assim, uma necessidade de reformulação conceitual que deve ser acompanhada pelas modernas legislações.

É nosso entendimento que a comercialização dos dados coletados pelos *sites* para outros fins, para empresas comerciais ou de prestação de serviços não coligadas à empresa que os coletou, merece maior atuação do Direito em defesa dos usuários e de sua privacidade. Este tipo de comércio é um claro caso de violação de privacidade, que caracteriza uma não observância aos direitos e garantias fundamentais da pessoa. Neste sentido e em resposta a esta necessidade, veio a Lei Geral de Proteção de Dados (LGPD).

Conforme já mencionado, a cada vez que o usuário trafega na Rede, para que possa usufruir de seus benefícios, deverá preencher formulários virtuais, nos quais informa seus dados pessoais, seus hábitos de consumo e, às vezes, seus dados patrimoniais e preferências. Dessa forma, os *sites* que se dedicam ao comércio eletrônico organizam verdadeiros bancos de dados acerca de seus usuários, cuja utilização encontra-se numa zona cinzenta, uma vez que nem o usuário nem o Poder Público sabem exatamente a forma da utilização destas informações.

Sabe-se que esses bancos de dados, mormente, serão utilizados para alavancar a venda de produtos associados aos *sites* direcionados ao comércio eletrônico, mas não se sabe de forma

---

[17] *Spam* significa mensagem de correio eletrônico não solicitada, enviada a muitos destinatários ao mesmo tempo, geralmente com finalidades comerciais.

[18] Veja-se o artigo 5º, incisos X, XI e XII.

[19] Aqui se encontra a importante questão sobre se pode a empresa ter acesso a *e.mails* de seus empregados, prática já coibida pela Justiça do Trabalho. Neste sentido: "O Governo da terra dos bretões, no ano 2000, autorizou as empresas a interceptarem os *e. mails* de seus contratados, considerando que elas têm o direito de zelar pelo correto uso de seus recursos. Curiosamente, neste peculiar recanto planetário (onde o direito à privacidade depende dos humores dos aplicadores da *common law*), o Lloyd Bank avisou seus funcionários que seus *e mails* seriam monitorados. E eles aceitaram!

Já os franceses se indignaram com a medida de seus sócios na comunidade européia, tal qual os espanhóis. Todavia, esses últimos não se jungiram à mera indignação: agiram! Através de seus sindicatos pressionaram o Senado que, no final daquele ano, aprovou uma moção para que o governo regulamentasse o uso do correio eletrônico e da Internet como instrumento entre os trabalhadores e os sindicatos, garantindo-se-lhes a inviolabilidade das comunicações, vez que a 'jurisprudência espanhola tem entendido que o local de trabalho não constitui, por definição, um espaço onde se possa exercer o direito à intimidade'. Esse direito está limitado ao seu exercício, dentro do local de trabalho, nos lugares de descanso, mas não naqueles em que efetivamente se desenvolve a atividade do empregado". A. M. Silva Neto. *Privacidade na Internet – Um Enfoque Jurídico*. São Paulo: Edipro, 2001, p. 50.

[20] J. Winer. *Globalization and the Harmonization of Law*. London: BookEns Ltd, 1999, p. 103.

"Almost each of these issues has concerned whether there ought to be government intervention in the application of existing laws or the elaboration of new ones to the digital environment. And each debate, with few exceptions, has encountered the dilemma of jurisdiction and the efficacy of national action without parallel international action.

Some issues can be resolved by one state acting singly. For instance, a state that is sensitive to the problem of 'hacking' and that wishes to enforce its laws relating to the protection of personal information could mandate that computers containing personal information meet certain security and encryption criteria. In this case, the legislation would relate to technical standards of security and these standards would be enforceable due to the fact that the law governs persons who maintain the computer systems, and these persons are located on the territory of the state over which the state has jurisdiction."

[21] RODOTÁ, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Tradução: Danilo e Luciana Doneda. Rio de janeiro: Renovar, 2008, p. 92.

clara e exata a forma de sua utilização e se essas informações são ou não fornecidas a outros *sites* ou mesmo ao Poder Público, sem ordem judicial.

Tal 'perigo' se materializou em março de 2018[22] quando veio a público o escândalo da *Cambridge Analityca* (CA), empresa britânica que se mostrou apta a analisar imensa quantidade de material e dados combinando-os com ciência comportamental, visando identificar pessoas e empresas que poderiam ser contatadas via envio de material de marketing ou mesmo influenciando campanhas políticas e eleições presidenciais. A CA, sem autorização expressa e sem publicar tais resultados coletava dados de diversas fontes, mas principalmente de plataformas de mídia social, como o Facebook.

É fato que o Direito, assim como as outras ciências humanas, está sempre um passo atrás da sociedade e sua dinâmica de desenvolvimento. Dessa forma, o campo jurídico tem procurado suprir as necessidades de adaptação aos ambientas virtuais. Não é à toa que a temática virtual já recebeu alguma tutela do legislador, como na Lei de Acesso à Informação, no Marco Civil da Internet e no Código de Defesa do Consumidor. E, agora, na Lei Geral de Dados Pessoais.

Para entender a necessidade de uma legislação protetiva de dados pessoais, faz-se necessário entender o ingresso da sociedade em um novo patamar de produção de bens e serviços. Nesta sociedade da informação, a geração, o armazenamento e a transferência das informações são realizados instantaneamente, sendo que as novas tecnologias agregam valor à informação. Vale dizer: a informação passou a ser considerada um produto, podendo, inclusive, vir a ser objeto de transações comerciais.

Na sociedade da informação há, assim, excesso de informações e riscos relacionados ao uso indevido dos instrumentos computadorizados para desvios ou abusos relacionados aos dados coletados ou armazenados. Nesta realidade, os empresários podem obter informações fundamentais para suas operações cotidianas através da inteligência e do armazenamento de dados.

Entretanto, no âmbito do armazenamento de dados e sua utilização, viu-se a necessidade de um novo complemento à legislação nacional visando uma maior proteção. Um dos inúmeros casos que ilustra a importância dessa demanda foi a aquisição do aplicativo de mensagem WhatsApp pelo Facebook[23] por um valor aproximado de U$ 19 bilhões de dólares, uma das maiores transações do ramo. A rede de troca de mensagens sempre teve como um dos principais pilares a proteção dos dados de seus usuários[24], comportamento não tão praticado por Mark Zuckerberg[25].

Para averiguar se não passaria a haver a utilização de dados dos usuários do Whatsapp, visto o potencial de mercantilização dessas informações, a Eletronic Privacy Information Center/EPIC e o Center Digital for Democracy entraram com um procedimento no órgão regulador americano (Federal Trade Commission/ FTC)[26], no qual se objetivou investigar os propósitos da aquisição.

Entretanto, em 2015 a política de dados do WhatsApp foi alterada, e foi incluído o compartilhamento de informações com o Facebook e suas plataformas adjacentes. A justificativa

---

[22] https://www.theguardian.com/news/2018/mar/18/what-is-cambridge-analytica-firm-at-centre-of-facebook-data-breach, acesso em 20.06.2019.

[23] BIONI e Ricardo, B 2019, Proteção de Dados Pessoais - A Função e os Limites do Consentimento, Rio de Janeiro.

[24] https://blog.whatsapp.com/91/Just-wanted-to-say-a-few-things...? – Post de Jan Koum, um dos fundadores do WhatsApp sobre coleta de dato dos usuários Acesso em 07/06/2019

[25] https://g1.globo.com/economia/tecnologia/noticia/2018/12/06/e-mails-revelam-que-mark-zuckerberg-apoiou-compartilhamento-de-dados-de-usuarios-do-facebook.ghtml - acesso em 07/06/2019

[26] https://epic.org/privacy/internet/ftc/whatsapp/ - acesso em 07/06/2019

no aplicativo dada aos usuários seria a de "melhorar suas experiências com anúncios e produtos do Facebook''.[27]

3 EVOLUÇÃO LEGISLATIVA

No Brasil em todos os textos constitucionais houve menção ao direito à inviolabilidade do domicílio e ao sigilo de correspondência, e apenas na Constituição de 1988 foi contemplado o direito à intimidade e à proteção privada.

No campo internacional, assim como ocorreu no Brasil, é possível perceber que a preocupação com o direito à privacidade vem aumentando conforme a modernidade do século XX. Por exemplo, na constituição Norte Americana de 1788 não havia menção expressa ao direito de inviolabilidade do domicílio, nem à intimidade. Porém, com a Quarta e Quinta emendas, e ainda, com a Declaração Universal dos Direitos do Homem este direito passou a ser contemplado. Nesse sentido é interessante citar o artigo 12 da Declaração de 1948[28].

A Organização das Nações Unidas atua fortemente na proteção da intimidade, merecendo destaque seu trabalho de denunciar a influência negativa de descobertas científicas e da tecnologia moderna[29]. A Convenção Interamericana dos Direitos Humanos de 22 de Novembro de 1969, no artigo 11, também aborda a questão[30].

Também o Marco Civil da Internet, Lei no. 12.965/14, possui artigos visando a proteção à confidencialidade e inviolabilidade da vida privada digital e os fluxos de tráfego da Internet, além de garantir que a guarda e disponibilização de registros de conexão e de acesso a aplicações a internet resguardem a intimidade, honra e imagem de seus usuários. Nesse sentido, é o seu art. 7º[31], inclusive exigindo o consentimento expresso do usuário para coleta, uso, armazenamento e tratamento de dados pessoais.

---

27 https://www.academia.edu/28751735/Nova_Politica_de_Privacidade_do_Whatsapp_questoes_a_serem_debatidas_sobre_consentimento - acesso em 07/06/2019

28 *"Ninguém será objeto de invasões arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de atentados a sua honra e a sua reputação. Toda pessoa tem direito à proteção da lei contra tais invasões ou atentados."*

29 Deve ser também ressaltado o artigo 17 do Pacto sobre Direitos Políticos e Civis da ONU de 23 de Março de 1976:
"1º Ninguém será objeto de invasões arbitrárias ou ilegais em sua vida privada, seu domicílio e sua correspondência, nem de atentados ilegais a sua honra e a sua reputação.
2º Toda pessoa tem direito à proteção da lei contra tais perturbações e tais atentados."

30 "Proteção da honra e da intimidade.
1 – Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
2- Ninguém pode ser objeto de influências arbitrárias ou abusivas em sua vida privada, na de sua família, em sua casa ou em sua correspondência, ou de ataques ilegais à sua honra ou reputação.
3- Toda pessoa tem direito à proteção da lei contra tais influencias e ataques."

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

Deste modo, a tutela do direito à intimidade é extremamente garantida em legislações internacionais e, ainda que de forma esparsa, prevista no ordenamento nacional. Contudo, a questão da evolução tecnológica é que vem conturbando tais instrumentos legais. É notável a importância que o tratamento de dados ganhou nos últimos anos do legislador, principalmente na Lei Europeia GDPR (*General Data Protection Regulation*) .

O Regulamento Geral de Proteção de Dados Pessoais Europeu n° 679 ou *General Data Protection Regulation* (GDPR) foi promulgado em 27 de abril de 2016 e entrou em vigor em 25 de maio de 2018, trazendo consigo novo entendimento sobre a proteção de dados pessoais, expandindo sua abrangência para além do próprio território europeu. Trata de forma sistemática da proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação deles. Foi editado em razão da necessidade de modernização da legislação considerando a introdução de novas tecnologias às realidades empresariais. Seu objetivo foi reforçar e unificar a proteção de dados pessoais na União Europeia por meio de uma adaptação dos princípios à sociedade da informação, que cada vez mais realiza coleta e tratamento de dados pessoais físicos ou digitais, por meio da internet, ou não. O GDPR é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Saliente-se, porém, que os regulamentos e leis atinentes à proteção de dados pessoais baseiam-se na premissa de que um indivíduo possui uma expectativa de privacidade, a menos que tal expectativa tenha sido restringida ou mesmo renunciada em face de acordo, contrato, lei ou consentimento unilateral. Em outras palavras, nota-se que a proteção aos dados pessoais é, por assim dizer, uma continuidade de todas as legislações existentes que protegiam a privacidade[32].

4 O SURGIMENTO DA LEI N° 13.709/2018

Em 2010 houve uma consulta pública executada pelo Ministério da Justiça sobre os limites de privacidade e uso de dados no Brasil, que contou com 2.500 contribuições[33]. Posteriormente a discussão se alastrou, principalmente com a disseminação de casos como o

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

[32] "O ponto fixo de referência nesse processo é que, entre os novos prismas para a abordagem da questão, mantém-se uma constante referência objetiva a uma disciplina jurídica específica para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo-lhe características próprias." DONEDA, Danilo, O Direito Fundamental à proteção de dados. In: MARTINS Guilherme Magalhães. Direito Privado e Internet. São Paulo: Atlas, 2014, p. 65.

[33] https://www2.camara.leg.br/camaranoticias/noticias/ADMINISTRACAO-PUBLICA/480920-CONSULTA-PUBLICA-SERA-BASE-PARA-PROJETO-DE-LEI-SOBRE-PROTECAO-DE-DADOS-PESSOAIS.html Acesso em 03 de junho de 2019

Wikileaks, as revelações de espionagem por Edward Snowden e o escândalo da *Cambridge Analytica* com suas possíveis implicações no controle dos processos eleitorais democráticos.

A consulta pública foi fonte para um texto maduro que gerou em 2016 o PL 5276/2016, aprovado sob unanimidade na Câmara dos Deputados. Ainda neste ano, as movimentações políticas de impeachment tiraram o foco da PL. Em 2017 o tema foi retomado pela Comissão de Assuntos Econômicos do Senado, e pressionado com ênfase no caráter de urgência, dada a vantagem econômica que o texto poderia proporcionar ao Brasil.

No ano seguinte, o estabelecimento de uma legislação sobre a privacidade de dados virtuais se tornou condição para o Brasil ingressar como país-membro da Organização para Cooperação e Desenvolvimento Socioeconômico (OCDE), fato que enfatizou a importância econômica da criação normativa[34].

Em 14 de agosto de 2018 foi sancionada pelo então presidente Michel Temer [35]a Lei n° 13.709/2018, também denominada Lei Geral de Proteção de Dados Pessoais, que entrará em vigor em agosto de 2020. Seu principal objetivo é a blindagem do cidadão quanto ao armazenamento, por parte de empresas públicas e privadas, de seu próprio fluxo informacional no meio digital, assegurando privacidade e liberdade. A penalidade máxima para as empresas que descumpram a lei é de até 2% (dois por cento) do faturamento no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração.

A LGPD foi aprovada em Agosto de 2018, com vetos do Presidente da República. Nestes vetos, foi suprimida a criação da Autoridade Nacional de Proteção de Dados, por entender o Governo que tal deveria se dar por um ato do Executivo. Somente em 28 de dezembro de 2018 foi editada a MP 869/2018, que estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD) como órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD. No entanto, ela passou à alçada da Presidência da República e não mais ao Ministério da Justiça[36]. Quando estava quase para expirar, no dia 03 de junho de 2019, a referida Medida Provisória virou lei, após um processo legislativo de urgência, com prorrogações. A ANPD é fundamental à temática da proteção de dados no Brasil, uma vez que caberá a este órgão a edição de normas sobre o tema, bem como a interpretação da LGPD, entre outras funções[37].

De acordo com o texto original sancionado, a LGPD entraria em vigor após dezoito meses de sua promulgação. Contudo, diante da Medida Provisória 869/2018, editada em 27 de

---

[34] https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018 - Acesso Em 03 de Junho de 2019

[35] https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/ - Acesso em 03 de Junho de 2019

[36] "55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados - ANPD, órgão da administração pública federal, integrante da Presidência da República"

[37]

- *Zelar pela proteção de dados*
- *Editar normas sobre o tema*
- *Deliberar sobre a interpretação da lei*
- *Requisitar informações à controladores e operadores*
- *Fiscalizar e aplicar sanções por descumprimento à LGPD*
- *Comunicar às autoridades competentes sobre infrações penais*
- *Comunicar descumprimentos à LGPD à órgãos de controle interno*
- *Estimular adoção de padrões que facilitem o controle e proteção dos titulares de seus dados pessoais*
- *Difundir conhecimentos sobre à LGPD*
- *Promover ações de cooperação com autoridades de proteção de dados internacionais e transnacionais*
- *Realizar consultas públicas*
- *Elaborar estudos e relatórios sobre a proteção de dados*
- *Desafio inicial é a conscientização sobre tratamento de dados no país através de muitas publicações de programas, progressos, dificuldades, prestação de informação e esclarecimento de dúvidas*

dezembro de 2018, a LGPD entrará em vigor 24 (vinte e quatro) meses após sua promulgação, isto é, somente em agosto de 2020.

O artigo 6º da LGPD, abaixo transcrito, apresenta os princípios da legislação:

Art. 6º ***As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios****:*

I. ***finalidade****: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;*

II. ***adequação****: tratamento de dados pessoais deve ser compatível com as finalidades informadas ao titular, de acordo com o contexto do tratamento;*

III. ***necessidade****: O tratamento de dados pessoais deve ser limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;*

IV. ***livre acesso****: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;*

V. ***qualidade dos dados****: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;*

VI. ***transparência****: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;*

VII. ***segurança****: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;*

VIII. ***prevenção****: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;*

IX. ***não discriminação****: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;*

X. ***responsabilização e prestação de contas****: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*

A LGPD traz em seu bojo, ainda, uma nova mitigação, a da territorialidade[38]. Tradicionalmente o Estado exerce seu poder soberano exclusivamente na delimitação de seu território, respeitando os atos praticados no estrangeiro a lei que lá estiver vigente. Todavia tal lógica não pode prosperar no meio digital pois estes fenômenos desafiam a *mens* legislativa, por surgirem da mesma forma e com o mesmo conteúdo em diversos locais (jurisdições), ao mesmo tempo. Assim é necessário que o mesmo ato ou fato esteja em consonância com diversos sistemas jurídicos ao adentrar, ainda que secundariamente, tais fronteiras geográficas.

[38] Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I - a operação de tratamento seja realizada no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou (Redação dada pela Medida Provisória nº 869, de 2018)
III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Assim, o critério da extraterritorialidade da LGPD determina que, independentemente de sua origem geográfica, ao ser acessado ou acessar sistemas localizados no território nacional, deve adimplir com suas regras.

4.1 Da Definição de Dados Pessoais

Os dados pessoais seriam "informação relacionada a pessoa natural identificada ou identificável"[39], ou seja, podem englobar materiais como nome, endereço, endereço eletrônico, idade, estado civil de indivíduos e diversas outras possibilidades de informações.

É de se ressaltar que os dados "anonimizados"[40] não serão considerados dados pessoais para os fins da Lei, salvo se for possível descobrir a sua autoria. Nesse quesito o legislador se refere aos dados relativos a titulares que não possam ser identificados, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento. Portanto, dados cuja autoria seja não só indeterminada, mas também, indeterminável, não serão protegidos pelo presente dispositivo legal.

Além do mais, quanto ao objeto da legislação, o artigo 1° é claro que o dispositivo normativo "dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais". Nesses termos, embora a discussão acerca da LGPD tenha nascido da fértil realidade virtual, seus efeitos não se limitam à condição de proveniência da realidade digital.

Outro aspecto oriundo da origem dos dados pessoais é a sua perspectiva transnacional, que, mesmo não sendo os dados ou seu tratamento evidentemente a brasileiros, a operação poderá sofrer consequências da norma. À luz do artigo 3º fica evidente a extraterritorialidade da lei, segundo o qual poderá ser aplicada nos casos de operações de tratamento serem realizadas em território nacional, no caso das operações objetivarem uma troca comercial a ser realizada em território nacional, ou se os indivíduos que forneceram ou receptaram os dados estiverem no Brasil.

4.2 Do Tratamento dos Dados Pessoais

O termo "*tratamento*", utilizado pela legislação é referente a toda operação realizada com dados pessoais, como as que se referem a coleta, transmissão, arquivamento de informações e entre outras. Basicamente denota toda operação que pode ser feita ao adquirir, manter ou transmitir dados pessoais.

Os agentes do tratamento designam aqueles que realizam operações de tratamento com os dados pessoais em qualquer meio, podendo ser organizações públicas, organizações privadas, pessoas físicas ou jurídicas[41]. Tais agentes são distinguidos legislativamente como *controlador* – aquele que determina o tratamento de dados – e *operador – aquele* que na prática efetivamente os coleta. Eles são responsáveis também por assegurar a segurança das informações que realizam tratamentos, devendo se precaver para que pessoas não autorizadas tenham acesso a elas. Em caso de infrações à Lei, os agentes de tratamento poderão responder por sanções administrativas, que podem variar de advertências a multas.

Nesse contexto, são definidos princípios gerais de proteção que devem nortear referidos procedimentos com Dados Pessoais[42], e posteriormente estabelecidos as formas como deverão ser tratados.

[39] Art. 5° inciso III da Lei n° 13.709/2018
[40] Art. 12° da Lei n° 13.709/2018
[41] PINHEIRO e Peck, P. 2018., Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD, São Paulo P.29
[42] Art. 6° da Lei n° 13.709/2018

Em um primeiro momento deve haver explícito consentimento, representado por escrito ou por outros meios de demonstração de vontade, por parte do titular dos dados quanto a retenção destes por parte de terceiros[43]. É interessante destacar que há a possibilidade de sua revogação.

Já durante o período de tratamentos de dados pessoais, o indivíduo titular poderá, por direito, saber a finalidade da coleta de dados, por quanto tempo eles ficarão armazenados, ter informações sobre o controlador e como contatá-lo. A finalidade de armazenamento deverá ser de apoiar ou promover atividades do controlador ou para garantir uma prestação de serviços ou assegurar direitos do titular dos dados pessoais.

Alcançada a determinada finalidade, ou se os dados se tornarem desnecessários para este fim poderá ocorrer o encerramento do tratamento. Há outras hipóteses que também podem incorrer no término do tratamento, como a determinação por autoridade nacional, se violado algum disposto da lei, e a solicitação feita pelo titular dos dados pessoais.

O artigo 7º da LGPD, abaixo transcrito, apresenta as hipóteses de tratamento de dados pessoais:

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I. mediante o fornecimento de consentimento pelo titular;

II. para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados;

III. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;

IV. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V. quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VII. para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII. para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX. quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X. para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

4.3 Dos Dados Pessoais Sensíveis

Os dados pessoais sensíveis aos termos do inciso II art. 5° da LGBD são aqueles "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". Sucintamente são dados de particularidade maior, que denotam a forma de pensar e ser do indivíduo bem como sua origem sociocultural e biológica.

Além da classificação diferenciada, esse gênero de dado pessoal também possui forma de tratamento diversa. O seu tratamento se restringe aos casos nos quais o autor dos dados consente de forma específica e destacada, para finalidades específicas, exceto em algumas hipóteses de exigências legais, judiciais e em usos por órgão de pesquisas, que deverão se comprometer com o anonimato dos titulares dos dados.

O artigo 11 da LGPD, abaixo transcrito, apresenta as hipóteses de tratamento de dados pessoais:

[43] Art. 7º inciso I da Lei n° 13.709/2018

Art. 11 O tratamento de dados pessoais sensíveis:

I. mediante o fornecimento de consentimento pelo titular;

II. para o cumprimento de obrigação legal ou regulatória pelo controlador dos dados;

III. pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos;

IV. para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V. para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;

VI. para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VII. para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

4.4 O tratamento de dados pessoais pelo Poder Público

Dentre os efeitos da LGPD há sua regulação quanto ao Poder Público, que deve realizar o tratamento de dados estritamente da forma descrita em Lei. De acordo com a definição do art. 5º, X, o tratamento de dados consiste em:

"(...) toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; (...)".

Sendo assim, no art. 7º da Lei, onde há referência expressa a requisitos obrigatórios ao processamento de dados, é imposto ao Poder Público que o faça apenas para: *"(...) o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres (...)".*

Mesmo assim, para que possa haver esse tratamento de dados, é preciso que haja consentimento do titular, classificado pela Lei como a manifestação livre, informada e inequívoca do sujeito que autoriza o uso dos dados à finalidade específica.

O ônus de comprovação de que se trata de consentimento livre deve ser daquele que pretende controlar os dados em questão.

Tratando-se de uma relação empregatícia, por exemplo, a maioria das autoridades de proteção de dados na Europa entende que não pode ser considerada a existência de consentimento livre para que os dados de um funcionário sejam processados por uma empresa, dada a relação de subordinação existente entre os polos.

Enquanto no Brasil e nos países da União Europeia a comprovação do consentimento expresso é exigida, nos Estados Unidos é comum que o sujeito apenas receba uma notificação em que é informado a respeito da renovação da política de tratamento de dados. Desta forma, é considerada a existência de consentimento tácito – também chamada como *opt-out provision* – ou seja, para não haja mais o tratamento de dados, é necessário que o titular sinalize seu desejo de forma clara.

É previsto pela LGPD que o tratamento de dados poderá ser realizado para cumprimento de obrigação legal ou regulatória pelo controlador.

Analisando o setor financeiro como exemplo, é comum que diretrizes impostas pelo Banco Central sejam exigidas do controlador de dados e, posteriormente, transmitidas ao detentor dos dados como uma obrigação legal.

Poderá também haver o processamento de dados quando assim necessário para execução de contratos, a pedido do titular dos dados, ou quando se tratar de requisito necessário para satisfazer os interesses legítimos do responsável pelo tratamento dos dados ou de terceiros.

Entretanto, a classificação de "interesse legítimo" é controversa. A comprovação deverá ser feita através de toda documentação possível, mitigando os riscos do tratamento. Se a autoridade fiscalizatória não concordar com os mecanismos usados para a classificação de determinada situação como de interesse legítimo, o processador dos dados estará sujeito a multa e sanções impostas pela LGPD, tal como a interrupção do processamento de dados.

Dentre as questões mais complexas envolvendo o processamento de dados e o Poder Público está o caso das empresas que prestam serviços de transporte particular por aplicativo. Nas cidades de São Paulo, Campinas, Porto Velho, Campo Grande e Fortaleza, por exemplo, dados básicos à cada viagem - tais como a duração, trajeto, locais de origem e partida – são obtidos cotidianamente.

No entanto, no caso de alguns municípios do Distrito Federal tem sido exigido que relatórios mensais sejam enviados à agências reguladoras, a fim de regulamentar a atividade realizada por essas empresas. Já em Tocantins, a prefeitura de Palmas tem exigido que os dados das corridas sejam compartilhados em tempo real com suas autoridades.

Apesar das diferenças em relação ao tratamento dos dados, a maioria dos municípios tem preocupação legítima com a confidencialidade dessas informações. Em São Paulo, por exemplo, há regulação que determina a possibilidade aos aplicativos de transporte de solicitarem restrição quanto às informações que compartilham com a prefeitura do município.

No estado de São Paulo e do Distrito Federal, empresas de transporte por aplicativo ajuizaram ação para discutir a constitucionalidade das regulações, bem como a possibilidade de proibição dos serviços no caso de não apresentação dos dados solicitados e a questão envolvendo aplicação de sanções.

De acordo com as empresas haveria uma ofensa a confidencialidade dos dados dos usuários, visto que seria exigida a apresentação de dados cadastrais como nome, qualificação pessoal, parentesco e endereço.

Em São Paulo, foi determinado que seria nomeado um "gerenciador de informações", responsável pela manutenção da confidencialidade dos dados - entretanto, não houve tal nomeação. No Distrito Federal, por outro lado, a agência responsável pelo processamento de dados declarou que o risco do vazamento dessas informações não teria suporte factual.

Tendo em vista as questões emergentes quanto aos conceitos e aplicação da LGPD, se espera que com o início das atividades da Agência Nacional de Proteção de Dados a interpretação da Lei possa ser realizada de forma a completar as lacunas e as dúvidas quanto aos conceitos e a abrangência da proteção de dados no Brasil, inclusive em relação às questões envolvendo o Poder Público.

4.5 Descumprimento da LGPD

O artigo 52 da LGPD dispõe sobre as medidas aplicáveis àqueles que desobedecerem a nova legislação, sendo certo que a interpretação sobre a própria lei cabe à ANPD.

São as penalidades:

a) Advertência e adoção de medidas corretivas
b) Multa de até 2% do faturamento da pessoa jurídica (limite de R$50 milhões por infração)
c) Publicação da infração
d) Bloqueio e eliminação dos dados em questão
e) Multa diária
f) Indenização ao titular dos dados

É necessário esclarecer que a sanções podem ser aplicadas cumulativamente, por dia e infração.

Ademais, caberá, ainda, indenização ao titular dos dados, uma vez que qualquer pessoa que intervenha no tratamento de dados tem a obrigação de manter a segurança desses. Desta feita, respondem solidariamente, junto ao operador de dados, por qualquer dano a terceiros em decorrência do descumprimento da LGPD, os agentes de tratamento que derem causa ao dano decorrentes da inobservância das medidas de segurança.

CONSIDERAÇÕES FINAIS

Em um comparativo com a LGPD, a GDPR tem objetivos que condizem com os da Lei nacional, visando também assegurar direitos fundamentais de pessoas naturais mediante proteção de dados. A norma estrangeira, cujo texto serviu de base à LGPD, é menos dúbia, e trabalha de forma mais minuciosa ao tratar dos seus conceitos. Por exemplo, no momento de classificar os tipos de dados em pessoais e pessoais sensíveis, junto dos quais também são propostos os dados genéticos, biométricos e os relativos à saúde[44]. A pena para o não cumprimento da lei pode chegar a 20 milhões de euros ou a 4% do faturamento anual da empresa responsável.

A legislação brasileira, aos moldes da legislação europeia introduz a regulação estatal sobre uma realidade que irrompeu com a contemporaneidade. A ética autoregulada dos operadores das redes digitais e das empresas de marketing da era digital agora tem um novo patamar e devem se adequar a tal realidade.

No atual contexto de evolução digital, vive-se em um mundo onde a publicidade direcionada irrompe diariamente na tela do celular e dos computadores dos cidadãos, e, consequentemente, a informação pessoal se torna cada dia mais valiosa enquanto produto e moeda de troca. Medidas como a Criação da Lei n° 13.709/2018 são necessárias ao desenvolvimento social saudável tanto dentro do mundo virtual como fora dele. Por ora resta aguardar a vigência da lei, para ser possível averiguar se seus moldes bastarão ou não à segurança do cidadão.

REFERÊNCIAS

BIONI e Ricardo, B, Proteção de Dados Pessoais - A Função e os Limites do Consentimento, Rio de Janeiro, 2019.

DINIZ, Maria Helena. Curso de Direito Civil Brasileiro, Teoria Geral do Direito Civil, 1. vol., São Paulo, Ed. Saraiva, 1982.

GRINOVER, Ada Pellegrini. Liberdades Públicas e Processo Penal. As Intervenções Telefônicas. São Paulo, Saraiva, 1978.

MARTINS Guilherme Magalhães. Direito Privado e Internet. São Paulo: Atlas, 2014.

PINHEIRO e Peck, P. *Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD*, São Paulo, 2018.

[44] PINHEIRO e Peck, P. 2018., *Proteção de dados pessoais - comentários à Lei n. 13.709/2018 LGPD*, São Paulo p.38

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

SILVA NETO, A. M.. *Privacidade na Internet – Um Enfoque Jurídico*. São Paulo: Edipro, 2001.

SILVA, José Afonso da. Curso de Direito Constitucional Positivo, 10. ed., São Paulo, Malheiros Editores, 1992.

WINER, J. *Globalization and the Harmonization of Law*. London: BookEns Ltd, 1999.

Sites

http://lawschool.stanford.edu/faculty/lessig/

https://blog.whatsapp.com/91/Just-wanted-to-say-a-few-things...?

https://brasil.elpais.com/brasil/2019/06/12/tecnologia/1560347825_866607.html -

https://epic.org/privacy/internet/ftc/whatsapp/

https://g1.globo.com/economia/tecnologia/noticia/2018/12/06/e-mails-revelam-que-mark-zuckerberg-apoiou-compartilhamento-de-dados-de-usuarios-do-facebook.ghtml -

https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/

https://www.academia.edu/28751735/Nova_Politica_de_Privacidade_do_Whatsapp_questoes_a_serem_debatidas_sobre_consentimento

https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/de-2010-a-2018-a-discussao-brasileira-sobre-uma-lei-geral-de-protecao-de-dados-02072018

https://www2.camara.leg.br/camaranoticias/noticias/ADMINISTRACAO-PUBLICA/480920-CONSULTA-PUBLICA-SERA-BASE-PARA-PROJETO-DE-LEI-SOBRE-PROTECAO-DE-DADOS-PESSOAIS.html

www.fd.unl.pt

www.jus.com.br