A PROTEÇÃO E O TRATAMENTO DOS DADOS PESSOAIS SENSÍVEIS NA ERA DIGITAL E O DIREITO À PRIVACIDADE: OS LIMITES DA INTERVENÇÃO DO ESTADO

PROTECTION AND TREATMENT OF SENSITIVE PERSONAL DATA IN THE DIGITAL AGE AND THE RIGHT TO PRIVACY: THE LIMITS FOR STATE INTERVENTION

Luiz Eduardo Gunther[1]

Rodrigo Thomazinho Comar[2]

Luciano Ehlke Rodrigues[3]

RESUMO

O presente estudo visa analisar como vem ocorrendo o tratamento de dados pessoais sensíveis na era digital e o direito à privacidade, bem como o papel do Estado nesta seara. A metodologia utilizada baseou-se na coleta de dados por meio de artigos científicos e de revisão bibliográfica, com a utilização do método dedutivo-dialético. O objetivo foi investigar como o cidadão brasileiro está se preparando para a aplicação da Lei Geral de Proteção de Dados (LGPD). Para tal desiderato será abordada a Lei 13.709/2018, que entrará em vigor em agosto de 2020, bem como o direito fundamental à privacidade, sendo necessário estabelecer uma ancoragem da temática na Constituição Federal de 1988 e no rol de direitos fundamentais jungidos nesse ordenamento maior. A contribuição deste artigo, portanto, destina-se a analisar os limites da intervenção do estado no tratamento dos dados pessoais sensíveis dos cidadãos brasileiros sem que se desproteja o direito à privacidade.

Palavras-chave: era da informação; tráfego de dados; tecnologia.

---

[1] Pós-Doutor em Direito pela PUC-PR. Doutor em Direito pela Universidade Federal do Paraná. Mestre em Direito pela Universidade Federal do Paraná. Graduado em Direito e em História pela Universidade Federal do Paraná. Desembargador Federal do Trabalho junto ao TRT da 9ª Região. Professor do Centro Universitário Curitiba – UNICURITIBA. Membro do Instituto Histórico e Geográfico do Paraná e da Academia Nacional de Direito do Trabalho.

[2] Mestre em Direito Empresarial e Cidadania pela Faculdade de Direito do Centro Universitário Curitiba-Unicuritiba (2019). Pós-graduação em Direito Processual Civil pela Pontifícia Universidade Católica do Paraná- PUCPR (2002). Graduado pela Universidade Estadual de Londrina- UEL (2000). Membro do Grupo de Pesquisa em Lei Geral de Proteção de Dados e Direitos da Personalidade. E-mail: rodrigoadvoc@hotmail.com

[3] Mestrando pelo Programa de Direito Empresarial e Cidadania; Especialista em Direito e Processo do Trabalho pelo Centro Universitário Curitiba (UNICURITIBA), em 2002. Especialista em Direito e Processo do Trabalho pela Escola da Magistratura Trabalhista (EMATRA-PR- 2004). Graduado pela Pontifícia Universidade Católica do Paraná (PUCPR), em 2000. Membro do Grupo de Pesquisa Reforma trabalhista: os valores sociais do trabalho e da livre iniciativa (2018 – UNICURITIBA). Membro do Grupo de Pesquisa: Lei Geral de Proteção de Dados e os Direitos da Personalidade (UNICURITIBA – 2019). Bolsista CAPES. Advogado Trabalhista Empresarial há 20 anos – email: ehlkerodrigues@hotmail.com

ABSTRACT

This study aims to analyze how the processing of sensitive personal data in the digital age and the right to privacy has been taking place, as well as the role of the State in this area. The methodology used was based on data collection through scientific articles and bibliographic review, using the deductive-dialectic method. The objective was to investigate how the Brazilian citizen is preparing for the application of the General Data Protection Law (LGPD). To this end, Law 13.709 / 2018, which will come into force in August 2020, as well as the fundamental right to privacy, will be addressed, and it will be necessary to establish an anchorage of the theme in the Federal Constitution of 1988 and in the list of fundamental rights joined in this larger order. . The contribution of this article, therefore, is intended to analyze the limits of the state's intervention in the treatment of sensitive personal data of Brazilian citizens without compromising the right to privacy.

Keywords: information age; data traffic; technology.

1 INTRODUÇÃO

Desde os primórdios da Humanidade, o homem sempre esteve intimamente ligado à ideia de evolução e conquistas. Um ponto de destaque na história do homem consiste na incessante busca pelo desconhecido, cabendo destacar, dentre tantos acontecimentos marcantes, a primeira vez em que o homem chegou à lua, quando estavam a bordo da Apollo 11, os astronautas Neil Armstrong, Edwin Aldrin e Michael Collins, em 16 de julho de 1969. A necessidade constante de conquistas marcou a tônica de vários séculos da Humanidade e ainda continua.

Inúmeros fatos permearam a vida humana, mas o século XXI proporcionou avanços em diversos ramos, em especial, o da Tecnologia da Informação, quando a máquina de escrever foi substituída pelos antigos PC´s até chegarmos à era dos celulares e tablets que permeiam o dia-a-dia dos seres humanos nos quatro cantos do Mundo.

Necessário destacarmos que nossa memória nos leva a associar fatos a personagens que os representaram, sendo certo que para este marco histórico e importante para a humanidade acima descrito, a marca do homem foi o registro de sua pegada na Lua, tido como uma comprovação física, palpável e visível de sua conquista. De toda sorte, será mais fácil lembrarmos de Neil Armstrong, enquanto os nomes de Edwin Aldrin e Michael Collins -- embora respeitáveis porquanto estiveram presentes nessa notável expedição -- insistam em cair no esquecimento.

Avançando um pouco no tempo, na segunda década do século XXI, aquilo que até então era conhecido como pegadas físicas, com o advento da Sociedade da Informação preconizada por CASTELLS (1998) e da Internet, são, hoje, transformadas em rastros naquilo que o homem pós-moderno tem denominado de "A era digital".

Necessário se faz, portanto, que seja abordada uma análise do conceito de dados pessoais sensíveis e de como a união europeia (EU) vem normatizando o tratamento desses dados. Mister se faz analisar o direito à privacidade e sua previsão legal no artigo 5º, X, da Constituição da República Federativa do Brasil de 1988 (CRFB).

Por fim, o objetivo do presente estudo reside em investigar quais os limites da Intervenção do Estado no tratamento dos Dados Pessoais Sensíveis dos cidadãos e possíveis conflitos com o Direito à Privacidade.

Partindo-se desse norte, será necessário investigar como a General Data Protection Regulation (GDPR) trata do tema na EU, bem como a Lei 13.709/2018[4], também conhecida como Lei Geral de Proteção de Dados (LGPD) regulará esse relevante tema e impactará a vida de pessoas naturais e pessoas jurídicas de direito privado e público, conforme definido no art. 1º da referida lei. Ao final, procuraremos apresentar os resultados e/ou contribuições do presente estudo ao qual nos propusemos a incursionar.

2 A ERA DIGITAL E OS DADOS PESSOAIS SENSÍVEIS

O mundo tecnológico e a world wide web (web) -- nome pelo qual a rede mundial de computadores internet se tornou conhecida a partir de 1991, quando se popularizou devido à criação de uma *interface gráfica* que facilitou o acesso e estendeu seu alcance ao público em geral -- vem prospectando milhões de pessoas que se vêem encantadas com a informação que lhes é colocada de forma instantânea. Neste contexto, cabe destacar que os acessos na web acabam por deixar rastros e as informações processadas por meios eletrônicos, também conhecidas como dados que são compartilhados pelo globo terrestre em frações de segundos merecem a atenção da comunidade acadêmica.

Se antes da Revolução tecnológica os seres humanos utilizavam-se de cartas, telegramas e ligações telefônicas para interagirem com o Mundo, o que demandava um certo tempo, a forma de comunicação na Era digital avançou rapidamente.

---

[4] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 10. jun. 2019

Hoje em dia, o compartilhamento de informações através das mídias sociais, como é o caso do Facebook, são o novo contexto.

Ocorre que tal compartilhamento de informações pode trazer sérios riscos ao vazamento de dados pessoais em caso de fragilidade do sistema ou ataques de hackers, por exemplo, ou ainda quando os dados pessoais alcançam conotação de mercadoria.

Os rastros são detectados no mundo tecnológico por meio de dados que são trafegados por meio da rede mundial de computadores. Para buscar dinamizar esse instantâneo tráfego de dados, a União Europeia se reuniu e editou o GDPR, ou seja, um Regulamento Geral de Proteção de Dados em 2018, visando dinamizar o tratamento dos dados pessoais sensíveis dos cidadãos no âmbito dos países integrantes da EU e conferir maior proteção aos dados pessoais que circulam no ambiente digital. Neste espectro é que o presente artigo buscará contribuir cientificamente trazendo elementos e conceitos a respeito da era digital, dados pessoais sensíveis e seu tratamento, direito à privacidade e os limites da intervenção do Estado neste tema.

A referida comunidade europeia revelou ao mundo sua preocupação com a forma como os dados pessoais sensíveis são tratados e buscou estabelecer todo um arcabouço normativo que era tratado pela Diretiva 45/96/CE e em 2018 foi alterado pela GDPR para tratar da questão afeita à Proteção de Dados.

A importância e atualidade da discussão reside no fato de que o Brasil publicou em dezembro de 2018, a Lei 13.709/2018[5], que entrará em vigor em agosto de 2020 e causará profundas modificações na forma como as empresas, o Estado e terceiros vem dando ao tratamento dos dados pessoais sensíveis dos brasileiros, inclusive com a previsão de aplicação de multa de até 50 milhões de reais a cargo da Autoridade Nacional de Proteção de Dados (ANPD), em casos em que restar evidenciada a ocorrência de descumprimento da LGPD, o que passará por futuras definições da respectiva ANPD vinculada à Presidência da República do Brasil.

2.1 OS DADOS PESSOAIS SENSÍVEIS – CONCEITO E CONSIDERAÇÕES

[5] Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 10. jun. 2019

Primeiramente, cabe destacar que a própria Diretiva 95/46/CE[6] traz uma definição de dados pessoais sensíveis de acordo com o artigo 2º, como se tratando de qualquer informação relativa a uma determinada pessoa singular identificada ou identificável.

A referida diretiva europeia conceitua como dado pessoal identificável como todo aquele que possa ser identificado de forma direta ou indireta, complementando a aludida normativa europeia que: "[...], nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social (Diretiva 95/46/CE, np)."

Na mesma linha da Diretiva da EU, o poder legislativo elaborou a Lei 13.709/2018 que estabelece um regramento específico no que se refere ao tratamento de dados pessoais sensíveis no Brasil, lei esta que ficou conhecida como Lei Geral de Proteção de Dados, que entrará em vigor somente em agosto de 2020, em face da "*vacatio legis*" de 18 meses estabelecida por nosso legislador.

Segundo Pinheiro (2018, p. 26), os dados pessoais sensíveis podem ser conceituados da seguinte forma:

> São dados que estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

O artigo 5º, incisos I e II da Lei 13.709/2018, define dados pessoais sensíveis da seguinte forma:

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> **II - dado pessoal sensível: 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; (negritos nossos)**

Mais adiante, em se tratando das Diretivas da União Europeia, BRAVO (2007, p. 156) destaca a proibição expressa do processamento de determinados dados pessoais:

---

[6] Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 12.dez.2019

> O art. 8.1 da Diretiva 95/46/CE proíbe o processamento dos dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, o pertencimento a sindicatos, assim como o tratamento de dados relativos à saúde ou à sexualidade. Seu apartado 5 proíbe o processamento de dados relativos à condenações criminais.
> [...] levando em conta os princípios de determinação e limitação da finalidade, legitimidade e proporcionalidade, poder-se-á autorizar um tratamento de tais dados, se de acordo com as seguintes particularidades:

O mesmo autor prossegue seu raciocínio esclarecendo que:

> - Os dados relativos à vida sexual só poderão ser objeto de processamento quando seja necessário para determinação da responsabilidade dos empregadores de uma acusação de assédio sexual.
> - Os dados relativos aos antecedentes penais só poderão ser processados se for necessário com respeito às funções particulares do emprego em questão. Nestes casos, prevê-se o necessário controle prévio por parte da autoridade nacional de controle, para evitar abusos e excessos, assim como verificar a pertinência do processamento.

DONEDA (2010, p. 191) procurou ampliar a questão relativa à proteção de qualquer dado pessoal e não somente do dado sensível concluindo que:

> qualquer dado pessoal e não somente o dado sensível é passível de, em determinadas circunstâncias, dar origem à discriminação ou ao controle, diminuindo as liberdades de escolha de uma pessoa. Os efeitos geralmente atribuídos ao tratamento indiscriminado dos dados sensíveis também podem ocorrer quando da manipulação de dados não sensíveis – tanto é que os dados não sensíveis também merecem proteção, apenas em uma escala inferior.

O mesmo autor continua seus ensinamentos a respeito dos motivos dos dados sensíveis merecerem uma proteção diferenciada, nos seguintes termos:

> O motivo dos dados sensíveis merecerem uma proteção mais intensa é justamente uma consideração probabilística de que tais dados são mais afeitos a apresentarem problemas mais graves quando de sua má utilização – daí exatamente o fato de denominá-los como “sensíveis” em relação aos demais, enfatizando sua peculiaridade neste sentido (DONEDA, 2010, p. 191).

2.2 A ERA DIGITAL E SEU SURGIMENTO

A Era digital antecede o GDPR de maio de 2018 e a Lei 13.709/2018 (LGPD) Brasileira, porquanto os fatos surgem no mundo real e cabe ao legislador elaborar normas que regularão a aplicação de determinados aspectos aptos ao convívio dos homens em sociedade.

Como dissemos anteriormente, o século XXI trouxe inúmeros avanços tecnológicos a saber: celulares (antes analógicos e atualmente os smartphones), computadores de elevado processamento conhecidos como *mainframes*, big data até a criação da inteligência artificial (IA).

Em Castells, a era digital representa a cultura da virtualidade real a partir do pressuposto que tudo é possível de ser gravado em áudio e vídeo, desde eventos, festas e uma série de outras situações, melhor descritas pelo autor:

> As pessoas começaram a filmar seus eventos, de férias a comemorações familiares, assim produzindo as próprias imagens, além do álbum fotográfico. Apesar de todos os limites dessa autoprodução de imagens, tal prática realmente modificou o fluxo de mão única das imagens e reintegrou a experiência de vida e a tela. Em muitos países, da Andaluzia ao sul da Índia, a tecnologia de vídeo da comunidade local permitiu o surgimento da transmissão local rudimentar que misturava difusão de filmes de vídeo com eventos e anúncios locais, muitas vezes à margem dos regulamentos de telecomunicações (1999, p. 363).

O único meio de controlar a rede de tecnologia da informação é simples: não fazendo parte dela, porém o preço a ser pago é extremamente elevado e muitas vezes significa que aqueles que assim optam, ficarão de fora da sociedade virtual (CASTELLS, 1999).

Prossegue o referido autor, nos mostrando um exemplo de como os Estados Unidos da América utilizaram a virtualidade real na campanha presidencial de 1992:

> Na campanha presidencial norte-americana de 1992, o então vice-presidente Dan Quayle queria posicionar-se em defesa dos valores da família tradicional. Armado de suas convicções morais, iniciou um debate incomum com Murphy Brown. Murphy Brown, representada por uma ótima atriz, Candice Bergen, era a personagem principal de uma série popular de TV que (a) (re)presentava os valores e problemas de um novo tipo de mulher: a profissional solteira com os próprios critérios sobre a vida. Nas semanas da campanha presidencial, Murphy Brown (não Candice Bergen) decidiu ter um filho fora do casamento (CASTELLS, 1999, p. 395).

O mesmo autor prossegue sua narrativa se encaminhando para a surpreendente revelação no sentido de que:

> O vice-presidente Quayle apressou-se a condenar seu comportamento como impróprio, provocando revolta nacional principalmente entre as mulheres trabalhadoras. Murphy Brown (não apenas Candice Bergen) retaliou: no episódio seguinte apareceu assistindo à entrevista de televisão em que o vice-presidente Quayle a criticava e reagiu com críticas acirradas à interferência de políticos na vida das mulheres e com a defesa de seu direito a uma nova moralidade. Com isso *Murphy Brown* aumentou sua fatia de audiência, e o

> conservadorismo desatualizado de Dan Quayle contribuiu para a derrota eleitoral do presidente Bush. Os dois acontecimentos foram reais e, em certa medida, socialmente relevantes (CASTELLS, 1999, p. 395).

Partindo-se desse exemplo bem articulado por Castells, podemos destacar a vital importância da velocidade das informações, na medida em que podem influenciar diretamente nas escolhas culturais, entretenimento, alimentação, plano de saúde, músicas, filmes, mas também podem influenciar negativamente ou de forma direcionada no resultado de eleições presidenciais como veremos adiante.

Um exemplo emblemático foi o caso da Cambridge Analítica, amplamente divulgado nas mídias sociais, e que estaria relacionado às eleições norte-americanas de 2016[7], segundo denúncia feita pelos jornais *The New York Times* e *The Guardian*. De acordo com a imprensa, houve uma manipulação das eleições presidenciais norte americanas através da utilização dos perfis dos eleitores no Facebook sem o consentimento destes, com a finalidade de influenciar o resultado das eleições em favor do atual Presidente Donald Thrump.

Sob a perspectiva deste fascinante Universo de Informações e suas implicações para os seres humanos que navegam pela web, os dados classificados como dados pessoais sensíveis representam um novo petróleo (Fernandes, 2017).

Segundo FERNANDES (2017), a Diretiva da União Europeia já vem se dedicando há vários anos sobre o tema afeito à proteção de dados pessoais no que se refere ao fluxo de dados, chegando a conclusão de que:

> A Diretiva 95/46/CE, do Parlamento Europeu e do Conselho da Europa, de 24 de outubro de 1995, veio a responder a esta necessidade, ao obrigar os Estados à adoção de legislação oferecendo garantias semelhantes em todo o espaço europeu, e ao regrar os procedimentos quanto aos fluxos de dados pessoais para países que não os da União Europeia, tendo este passado a ser classificado de modo diferenciado, consoante ofereçam, ou não, um nível de proteção adequado. (FRAZÃO, np)

[7] Por meio de denúncia dos jornais The New York Times e The Guardian, através do aplicativo Facebook, teria ocorrido a utilização de dados de cerca de 50 milhões de pessoas e teriam sido utilizados sem o consentimento delas para utilização na Campanha Eleitoral Pró-Trump através de análise do perfil pessoal de cada usuário. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml.>. Acesso em 18.ago. 2019.

FRAZÃO (2018, np) tem divulgado uma série de artigos[8] acerca da Lei Geral de Proteção de Dados, revelando profunda preocupação acerca da destinação dos dados pessoais: "Passando para o exame do texto da lei, a primeira observação importante é que fica claro que o regime de proteção de dados não tem por finalidade apenas a de tutelar a privacidade dos usuários."

Podemos observar claramente da narrativa da autora que já no artigo 1º da Lei 13.709/2018, o seu objetivo visa proteger "os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (FRAZÃO, 2018, np)."

Com relação ao artigo 2º, o referido e novel diploma legal alusivo à Lei Geral de Proteção de dados elenca uma série de fundamentos aos quais busca proteger, quais sejam:

> além da privacidade, a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa; a livre concorrência e a defesa do consumidor; os direitos humanos; o livre desenvolvimento da personalidade; a dignidade e o exercício da cidadania pelas pessoas naturais.

Merece especial destaque as reflexões e ponderações lançadas por Frazão quanto às cautelas da lei preconizadas pelo legislador ordinário:

> Ao se referir expressamente ao livre desenvolvimento da personalidade, à cidadania e à dignidade, a lei certamente procura evitar muitas das destinações atuais que vêm sendo conferidas aos dados pessoais, os quais, processados por algoritmos, são capazes de fazer diagnósticos e classificações dos usuários que, por sua vez, podem ser utilizados para limitar suas possibilidades de vida. Mais do que isso, a partir de tais dados, as empresas podem discriminar usuários ou mesmo tentar manipular suas opiniões, crenças ou valores em vários âmbitos, inclusive o político (FRAZÃO, 2018, np).

Segundo Pinheiro (2018, p. 25), é possível conceituar o tratamento de dados da seguinte forma:

> Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

[8]Disponível em: <https://www.jota.info/opiniao-e-analise/colunas/constituicao-empresa-e-mercado/nova-lgpd-principais-repercussoes-para-a-atividade-empresarial-29082018>. Acesso em 02.abr.2019

Para Castells (1999, pág. 69), a Era da Informação passou a modificar os seres humanos de uma forma profunda, causando uma integração entre mentes e máquinas, na medida em que:

> Assim, computadores, sistemas de comunicação, decodificação e programação genética são todos amplificadores e extensões da mente humana. O que pensamos e como pensamos é expresso em bens, serviços, produção material e intelectual, sejam alimentos, moradia, sistemas de transporte e comunicação, mísseis, saúde, educação ou imagens. A integração crescente entre mentes e máquinas, inclusive a máquina de DNA, está anulando o que Bruce Mazlish chama de a "a quarta descontinuidade" (aquela entre seres humanos e máquinas), alterando fundamentalmente o modo pelo qual nascemos, vivemos, aprendemos, trabalhamos, produzimos, consumimos, sonhamos, lutamos ou morremos (CASTELLS, 1999, p. 69).

O mesmo autor continua seu raciocínio, afirmando que:

> Com certeza, os contextos culturais/institucionais e a ação social intencional interagem de forma decisiva com o sistema tecnológico, mas esse sistema tem sua própria lógica embutida, caracterizada pela capacidade de transformar todas as informações em um sistema comum de informação, processando-as em velocidade e capacidade cada vez maiores e com custo cada vez mais reduzido em uma rede de recuperação e distribuição potencialmente ubíqua (CASTELLS, 1999, p. 69)."

A Lei 13.709/2018, que entrará em vigor em agosto de 2020, excetua o tratamento de dados pessoais nas seguintes situações, conforme podemos observar no artigo 4º, inciso I, quando for realizado por: a) realizado por pessoa natural para fins exclusivamente particulares e não econômicos; bem como para fins jornalísticos e artísticos, além de acadêmicos, " aplicando-se a esta hipótese os arts. 7º e 11 desta Lei". (BRASIL, 2018).

No mesmo artigo, porém no inciso III, também existe exceção para o tratamento de dados pessoais quando for realizado para fins exclusivos envolvendo segurança pública, defesa nacional, segurança do estado, ou ainda atividades de investigação e repressão de infrações penais.

Em prosseguimento, o inciso V do mesmo artigo também excetua o tratamento de dados pessoais quando estes forem:

> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Por fim, ainda merece destaque o §1º da LGPD, que faz referência ao inciso III acima destacado, no seguinte sentido:

> § 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, que deverá prever medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

Quando o legislador trouxe a inaplicabilidade da Lei Geral de Proteção de Dados para os casos previstos no art. 4º e parágrafos, podemos divisar que prevaleceu a segurança pública, segurança do Estado ou atividades de investigação e repressão de infrações penais.

Todavia, se não houver o treinamento dos operadores responsáveis pelo tratamento dos dados pessoais sensíveis dos cidadãos brasileiros, evidencia-se um grande risco de vazamento desses dados gerando insegurança jurídica e prejuízos de ordem judicial em razão de demandas judiciais vindicando o pagamento de danos morais em decorrência de tais situações.

4 OS LIMITES DA INTERVENÇÃO DO ESTADO NO TRATAMENTO DOS DADOS PESSOAIS SENSÍVEIS

A Lei Geral de Proteção de Dados, como visto acima, estabelece responsabilidade ao Estado em caso de tratamento, divulgação e manipulação de dados sem o consentimento do titular, conforme podemos inferir da leitura do artigo 1º da Lei 13.709/2018:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por **pessoa jurídica de direito público** ou privado, com o **objetivo de proteger os direitos fundamentais de liberdade e de privacidade** e o livre desenvolvimento da personalidade da pessoa natural.
> Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e **devem ser observadas pela União, Estados, Distrito Federal e Municípios**. (Incluído pela Lei nº 13.853, de 2019) (grifo nosso)

Para JUNIOR e FAUSTINO (2019, p. 302) ao tratarem do tema relativo ao uso de aplicativos de serviços para a saúde pública e a proteção de dados pessoais dos usuários a situação é extremamente delicada, porquanto em se tratando de um país como o Brasil

com mais de 210 milhões de habitantes[9], a isso se soma a falta de qualificação dos operadores dos dados, trazendo risco de violação à privacidade de uma gama enorme de usuários, pontificando os autores que:

> A privacidade está ligada a dignidade da pessoa humana, princípio também insculpido na Constituição Federal em seu art. 1o, inciso III e está intimamente ligada com a confidencialidade nos casos envolvendo dados sensíveis relativos à saúde das pessoas, onde no ambiente da internet e das aplicações de internet, a possibilidade da violação da privacidade ganha níveis exponenciais, quer seja pela falta de zelo daqueles que realizam o tratamento dos dados pessoais, quer seja dos próprios usuários, [...]

Mais adiante, os mesmos autores (JUNIOR e FAUSTINO, 2019, p. 306-307), no que se refere especificamente aos dados envolvendo a saúde dos usuários do Sistema Único de Saúde (SUS), que representa dados pessoais sensíveis de uma elevada camada da população brasileira, o risco de vazamento de dados é preocupante, sendo relevante para o presente estudo citar parte das inquietações manifestadas pelos articulistas quanto ao aplicativo E-Saúde lançado em junho de 2016 pelo Ministério da Saúde em âmbito nacional:

> Esse aplicativo ou solução oferece uma série de informações que possuem relação com os dados dos usuários do Sistema Único de Saúde (SUS) como, por exemplo, dados do cartão nacional de saúde, lista de medicamentos retirados em unidades de saúde, informações sobre o cartão de vacinação, lista de exames realizados, dentre outros.
> As informações são centralizadas em um banco de dados e será possível o estreitamento e análise das informações dos usuários em consonância com a utilização de unidades de saúde pública espalhadas pelo Brasil.

Prosseguem na narrativa os mesmos autores salientando quanto as implicações do aplicativo e-Health ou e-Saúde, destacando que:

> Esse aplicativo foi uma das primeiras ações do Estado direcionadas para a população utilizando tecnologia integrada com os serviços de saúde no formato conhecido como e-Health ou e-Saúde, com a possibilidade de operações que envolvem o ciclo completo de tratamento de dados pessoais, onde o aplicativo vai armazenar todo o histórico de saúde de cada usuário com base nos dados no cartão SUS.

Para os autores, no exemplo acima, o risco na proteção e tratamento de dados foi evidente, na medida em que o aplicativo e-Saúde utilizado pela Prefeitura de São Paulo

[9]Disponível em: <https://www.ibge.gov.br/apps/populacao/projecao/index.html?utm_source=portal&utm_medium=popclock>. Acesso em: 10.dez. 2019.

em 2016[10], demonstrou-se vulnerável no que se refere à forma de tratamento desses dados pessoais, quanto mais em se tratando de prontuários médicos de usuários do sistema de saúde que se utilizaram e se ainda continuam a pertencer ao Sistema Único de Saúde (SUS), porquanto não se vislumbra a necessária segurança das informações, ferindo-se, por esse modo, a privacidade de cada um dos usuários que foi exposta na rede de internacional de computadores (internet).

No exemplo acima ocorrido em 2016 (HERNANDES, 2017) resta evidente que não houve consentimento por parte dos titulares dos dados pessoais sensíveis quanto ao vazamento de prontuários médicos de pacientes da rede pública de saúde que estavam sob a guarda e responsabilidade da Prefeitura de São Paulo.

Conquanto o uso da tecnologia no século XXI já seja uma realidade irrenunciável, dado que em pleno final da segunda década do Século XXI é praticamente impossível a não conexão das pessoas por meio de aplicativos e sistemas eletrônicos (whatswap, iFood, facebook, instagram, uber, 99, cabify, glovo, pje, projudi, e-proc, e-doc, além de milhares de app´s) o exemplo acima em relação ao vazamento de dados pessoais de pacientes (prontuário médico) na Internet abre uma verdadeira "caixa de Pandora" quanto aos objetivos desse breve estudo, na medida em que retomamos a seguinte indagação: Quais os limites para a intervenção do estado no tratamento dos dados pessoais sensíveis dos cidadãos brasileiros sem que ocorra violação ao direito à privacidade?

A tecnologia e a era digital vieram para facilitar o acesso às informações, porém, exigem, em contrapartida, um mínimo de investimento e proteção para os usuários titulares desses dados pessoais sensíveis, os quais, sem o consentimento específico, não podem ser divulgados por qualquer meio, quanto mais na rede mundial de computadores,

[10] Segue a parte complementar que retrata o caso ocorrido na Prefeitura de São Paulo em 2016, envolvendo o vazamento de dados pessoais de usuários do SUS por meio do aplicativo e-Saúde: Embora bastante interessante a solução, em uma pesquisa básica no site do Ministério da Saúde ou no próprio aplicativo e-Saúde, não é possível localizar a política de privacidade e os termos de usos, descriminando de forma transparente como serão tratados os dados pessoais do usuário, que tipo de dado pessoal será armazenado efetivamente, quem terá acesso a esses dados, possibilidade de exclusão de dados por parte dos usuários, e, principalmente, a respeito do consentimento dos usuários (pacientes) no que tange à forma de tratamento desses dados pessoais. Embora a solução seja bastante interessante como parte de uma política pública relacionada ao gerenciamento de dados de saúde dos usuários do sistema, esse aplicativo oferece claros riscos aos usuários, devido a não exposição de como esses dados pessoais serão tratados por parte do poder público e qual a extensão desse tratamento, ficando uma lacuna nesse sentido, dessa forma podendo surgir possibilidades de compartilhamento desses dados pessoais dos usuários, bem como episódios de vazamento de dados pessoais sensíveis nos moldes do que ocorreu na Prefeitura de São Paulo no ano de 2016 (HERNANDES, 2016), onde dados pessoais, e até mesmo dados de prontuário médico de pacientes da rede pública municipal de saúde foram expostos na internet sem a autorização, por conta de não estarem protegidos por mecanismos de segurança digital.

porquanto a visualização desses dados fere o direito à privacidade consagrado no artigo 5º, X, da Constituição Cidadã de 1988.

Gomes (2011, p. 615-616) cita o entendimento de Carlos Ari Sundfeld de que: "nos novos tempos, o Poder Legislativo faz o que sempre fez: edita leis, frequentemente com alto grau de abstração e generalidade.

Prossegue o referido autor justificando sua afirmação anterior, da seguinte forma:

> Só que, segundo os novos padrões da sociedade, agora essas normas não bastam, sendo preciso normas mais diretas para tratar das especificidades, realizar o planejamento dos setores, viabilizando a intervenção do Estado em garantia do cumprimento ou a realização daqueles valores: proteção do meio ambiente e do consumidor, busca do desenvolvimento nacional, expansão das telecomunicações nacionais, controle sobre o poder econômico – enfim, todos esses que hoje consideramos fundamentais e cuja persecução exigimos do Estado.

Justamente para que esse tratamento de dados pessoais não seja absoluto por parte da Intervenção do Estado na vida dos cidadãos brasileiros é que foi aposta ressalva no §1º no sentido de que o tratamento de dados pessoais, previsto no inciso III, será objeto de legislação específica dentro de critérios de proporcionalidade e que tais informações (dados pessoais sensíveis) a serem tratadas deverão ser as estritamente necessárias ao atendimento do interesse público, os princípios gerais de proteção e os direitos do titular previstos na Lei 13.709/2018.

5 CONSIDERAÇÕES FINAIS

A conclusão que podemos divisar é a de que existe profunda preocupação do legislador com relação aos abusos no tratamento de dados pessoais sensíveis de todos os cidadãos brasileiros, porquanto o direito à privacidade foi erigido à categoria de direito fundamental na Constituição da República Federativa do Brasil de 1988, de acordo com o artigo 5º, X[11].

[11] Art. 5º. Omissis:

...

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

Procuramos demonstrar que a Era Digital trouxe grandes avanços na forma como as pessoas e os países se comunicam de modo instantâneo e mais prático. Contudo, o tratamento dos dados pessoais sensíveis no Mundo Pós-Moderno deve obedecer a regramentos legais bem específicos, além de exigir o prévio consentimento dos titulares desses dados, sob pena de acarretar o dever de indenizar e incidirem os infratores em elevadas multas que ficarão a cargo da Autoridade Nacional de Proteção de Dados.

A Lei 13.709/2018, que entrará em vigência em agosto de 2020, representa –, ainda que de forma tardia em relação à Europa e diversos países da América Latina, porquanto muitos países já possuem há vários anos regramento específico para o tratamento de proteção dos dados pessoais sensíveis de seus cidadãos[12] – um importante marco legal após a Lei do marco Civil da Internet, para regular tal temática de uma forma um pouco mais criteriosa.

O exemplo trazido em relação ao vazamento de dados pessoais sensíveis corporificados nos prontuários médicos de pacientes usuários do SUS pela Prefeitura do Estado de São Paulo é fato inconteste de que o assunto é extremamente sério na medida em que pode trazer um desprestígio do Brasil frente ao cenário mundial.

Além disso, representa um alerta de risco na segurança da informação digital, bem como para a própria economia do país, porquanto não se vislumbra como o nosso país possa oferecer segurança jurídica de investimento para empresas estrangeiras sem que comprove que está alinhado – de forma efetiva – com o GDPR e as normativas da EU em relação ao respeito ao tratamento dos dados pessoais sensíveis.

Por outro prisma, na perspectiva da cidadania de cada um dos brasileiros é vital que o Estado, as empresas e toda a sociedade estejam cientes de seus direitos, mas, sobretudo, de seus deveres no que tange aos ditames da Lei Geral de Proteção de Dados que, como dito anteriormente, entrará em vigência a partir de agosto de 2020 e afetará a todos.

Nestes aspectos, uma das contribuições desse estudo foi que o Estado enquanto detentor da titularidade da Autoridade Nacional de Proteção de Dados (ANPD), deve envidar esforços para utilizar o critério pedagógico e informativo a todos os destinatários das regras estabelecidas pela Lei 13.709/2018, e, acima de tudo, cumpra seu papel de ente público que segue os princípios da Administração Pública afeitos à Legalidade, Impessoalidade, Moralidade e Publicidade, atingindo-se a almejada eficiência dentro de

[12] Argentina, Chile, Uruguai, por exemplo.

valores que se coadunam com a moral e a ética tão caros em nosso país, afunilando-se no princípio vetor da Dignidade da Pessoa Humana (art. 1º, III, CRFB/88).

É nesta conjugação entre o direito e a tecnologia que àquele se confere o importante atributo de velar pelo cumprimento da legalidade também no mundo cibernético.

REFERÊNCIAS

BRASIL. Lei n.º 13.709/2018. Lei Geral de Proteção de Dados. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Acesso em 10 jun. 2019

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em 10 dez. 2019.

BUENO, Chris. Chegada do homem à Lua comemora 40 anos com nova missão. **Cienc. Cult.**, São Paulo, v. 61, n. 3, p. 19-20, 2009. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci_arttext&pid=S0009-67252009000300008&lng=en&nrm=iso>. Acesso em: 18.aug.2019.

BRAVO, Álvaro A. Sanchez. **A proteção dos dados pessoais dos trabalhadores: Perspectiva Comunitária Europeia.** Revista do Tribunal Regional do trabalho da 15ª Região. n°. 30, Campinas, 2007. p. 153-160. Disponível em: <https://portal.trt15.jus.br/documents/124965/2647700/R+30-2007.pdf/27615c99-c09f-40ed-a17a-3c2c95edd63d>. Acesso em 02 dez. 2019.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, Joaçaba, v. 12, n. 02, p. 91-108, 2011. Disponível em: <https://editora.unoesc.edu.br/index.php/espacojuridico/article/viewFile/1315/658>. Acesso em: 28 dez. 2019.

CASTELLS, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 1999.

União Europeia. **DIRETIVA 45/96/CE**. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/ALL/?uri=CELEX%3A31995L0046>. Acesso em: 12.dez.2019.

GOMES, Joaquim B. Barbosa. Agências Reguladoras: A Metamorfose do Estado e da Democracia Uma Reflexão de Direito Constitucional e Comparado). In: CLEVE, Clemerson Merlin; BARROSO, Luís Roberto (org.). **Doutrinas Essenciais. Direito Constitucional. Volume VI. Constituição Financeira, Econômica e Social**. São Paulo: Revista dos Tribunais, 2011.

FERNANDES, David Augusto. Dados pessoais: Uma Nova Commodity, ligados ao Direito à intimidade e a Dignidade da Pessoa humana. **Revista Jurídica – Unicuritiba**. vol. 04, n°. 49, Curitiba, 2017. pp. 360-392. Disponível em:

<http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/2298/1428>. Acesso em 05. jun. 2019

FRAZÃO, Ana. **Nova lgpd: as demais hipóteses de tratamento de dados pessoais**. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/ -19092018 Publicado em 19/09/2018>. Acesso em 02.abr. 2019

GONÇALVES, Tânia Carolina Nunes Machado; VARELLA, Marcelo D. Os desafios da Administração Pública na disponibilização de dados sensíveis. **Rev. direito GV**. São Paulo, v. 14, n. 2, p. 513-536, aug. 2018. Disponível em: om <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S1808-24322018000200513&lng=en&nrm=iso>. Acesso em: 05. nov. 2019. http://dx.doi.org/10.1590/2317-6172201821.

HARARI, Yuval Noah. **21 lições para o século 21**. Tradução: São Paulo: Companhia das Letras, 2018.

HERNANDES, Raphael. Gestão Haddad expõe na internet dados de pacientes da rede pública. In: **Folha de São Paulo.** 2016. Disponível em <http://www1.folha.uol.com.br/cotidiano/2016/07/1788979-gestao-haddad-expoe-na-internet-dados-de-pacientes-da-rede-publica.shtml>. Acesso em 30. jul. 2019.

BARRETO JUNIOR, Irineu Francisco; FAUSTINO, André. Aplicativos de serviços de saúde e proteção dos dados pessoais dos usuários**. Revista Jurídica** vol. 01, n°. 54, Curitiba, 2019. p. 292 – 316. DOI: 10.6084/m9.figshare.7841105. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3311/371371803>. Acesso em 06 jun. 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: comentários à Lei n. 13.709/2018**. São Paulo: Saraiva Educação, 2018.

REINALDO FILHO, Demócrito. A Diretiva Europeia sobre proteção de dados pessoais. Uma análise de seus aspectos gerais. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 18, n. 3507, 6 fev. 2013. Disponível em: <https://jus.com.br/artigos/23669>. Acesso em: 9 jan. 2020.

SILVA, Letícia Brum da; SILVA, Rosane Leal da. **A proteção jurídica de dados pessoais na internet: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil**. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>. Acesso em 17. ago. 2019.

SILVA, Lucas Gonçalves; MELO, Bricio Luis da Anunciação. **A lei geral de proteção de dados como instrumento de concretização da autonomia privada em um mundo cada vez mais tecnológico.** Revista Jurídica, [S.l.], v. 3, n. 56, p. 354 - 377, jul. 2019. ISSN 2316-753X. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/3581/371371972>. Acesso em: 23 abr. 2020. doi:http://dx.doi.org/10.21902/revistajur.2316-753X.v3i56.3581.