I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

DANIELLE JACON AYRES PINTO

AIRES JOSE ROVER

FABIANO HARTMANN PEIXOTO

D597

Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto

Aires Jose Rover

Fabiano Hartmann Peixoto – Florianópolis: CONPEDI, 2020.

Inclui bibliografia

ISBN: 978-65-5648-078-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Constituição, cidades e crise

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. I Encontro Virtual do CONPEDI (1: 2020 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

I ENCONTRO VIRTUAL DO CONPEDI

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS I

Apresentação

O I ENCONTRO VIRTUAL DO CONPEDI, ocorrido entre os dias 23 e 30 de junho de 2020, foi realizado exclusivamente a partir da utilização das novas tecnologias de informação e comunicação. Foi o maior sucesso nesses tempos de pandemia. Mais do que nunca se viu a tecnologia servindo como instrumento de ação no campo do conhecimento e da aprendizagem, o que este GT sempre defendeu e esteve atento discutindo os limites e vantagens dessa utilização. Os artigos apresentados, como não podia deixar de ser, mostraram que os temas relacionados às novas tecnologias estão cada vez mais inseridos na realidade jurídica brasileira e mundial. Diversos fenômenos do cenário digital foram abordados ao longo dos trabalhos e demonstraram que a busca por soluções nessa esfera só pode ser pensada de forma multidisciplinar.

Assim, vejamos as principais temáticas tratadas, em sua sequência de apresentação no sumário e apresentação no GT. No primeiro bloco temático temos:

• Lei geral de proteção de dados

• proteção da intimidade, privacidade e aos dados sensíveis dos empregados

• anonimização e pseudoanonimização dos dados pessoais

• monetização de dados pessoais na economia informacional

• modelos regionais de obtenção de dados em aplicações na internet

• problemática dos brinquedos conectados

No segundo bloco:

• inteligência artificial e uma justiça preditiva

• neurociências no brexit

• confiança em sistemas de inteligência artificial

• chatbot, normas do bacen e fintechs de crédito

No terceiro bloco:

• internet como ferramenta de participação

• deliberação democrática digital

• ressocialização digital dos idosos

• gestão pública sustentável

• governança eletrônica na administração pública brasileira

• teoria do processo na era digital

No quarto e último bloco:

• a tecnologia e o princípio do contraditório

• vulnerabilidade aos cibercrimes

• fakenews

• pandemia e telemedicina

• pagamentos instantâneos e transações eletrônicas bancárias via whatsapp

Com esses estudos de excelência os coordenadores desse grupo de trabalho convidam a todos para a leitura na integra dos artigos.

Aires José Rover – UFSC

Fabiano Hartmann Peixoto - Universidade de Brasília

Danielle Jacon Ayres Pinto – IMM/ECEME e UFSC

Nota técnica: Os artigos do Grupo de Trabalho Direito, Governança e Novas Tecnologias I apresentados no I Encontro Virtual do CONPEDI e que não constam nestes Anais, foram selecionados para publicação na Plataforma Index Law Journals (https://www.indexlaw.org/), conforme previsto no item 8.1 do edital do Evento, e podem ser encontrados na Revista de Direito, Governança e Novas Tecnologias. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

A LEI GERAL DE PROTEÇÃO DE DADOS E A NECESSIDADE DE ANONIMIZAÇÃO E PSEUDOANONIMIZAÇÃO DOS DADOS PESSOAIS CONFORME INSERIDO NA LEI Nº 13.709/18.

THE GENERAL DATA PROTECTION ACT AND THE NEED FOR ANONYMISATION AND PSEUDO-ANONYMISATION OF PERSONAL DATA AS INSERTED IN THE LAW #13.709/18.

José Fernando Vidal De Souza [1]
Rodolfo Luiz Azevedo da Costa [2]

Resumo

A pesquisa examina a Lei 13.709/18 (LGPD), a partir dos conceitos de dados pessoais e tráfego de pacote de dados na rede, mediante a análise do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, que serviu de inspiração para a legislação pátria, bem como o nosso Marco Civil da Internet. Depois, apreciam-se as figuras da anonimização e pseudoanonimização realizada por pessoa natural ou por pessoa jurídica. Utilizou-se do método hipotético-dedutivo, fundado em pesquisa bibliográfica com a consulta a material bibliográfico e à legislação. Ao final, busca-se apresentar uma análise crítica para proteção dos dados pessoais dos usuários.

Palavras-chave: Lgpd, Dados pessoais, Anonimização, Pseudoanonimização, Proteção à privacidade

Abstract/Resumen/Résumé

The research examines Law #13.709/18 (LGPD), based on the concepts of personal data and data packet traffic on the network, through the analysis of the European Union's General Data Protection Regulation (GDPR), which served as inspiration for home legislation, as well as our Civil Marco de Internet. Then, the figures of anonymization and pseudo-anonymization performed by natural persons or legal entities are appreciated. We used the hypothetical-deductive method, based on bibliographic research with consultation of bibliographic material and legislation. At the end, it seeks to present a critical analysis to protect users' personal data.

Keywords/Palabras-claves/Mots-clés: Lgpd, Personal data, Anonymization, Pseudo-anonymization, Protection of privacy

[1] Pós-doutor (CES Universidade de Coimbra e UFSC). Mestre e Doutor em Direito (PUC-SP) Especialista Ciências Ambientais (USF). Bacharel em Direito e Filosofia (PUCCAMP). Professor da UNINOVE. Promotor de Justiça MPSP.

[2] Mestrando em Direito (UNINOVE). Especialista em Direito Civil e Processual Civil (Universidade Cândido Mendes). Bel. Direito (Universidade Estácio de Sá) e Teologia (Associação Educacional Universitária da Região dos Lagos-RJ). Advogado.

Introdução

O surgimento do ciberespaço e o seu crescimento estão a permitir que as sociedades se expandam de forma constante e, para muitos, de maneira assustadora, o que implica dizer que os seus meandros se tornaram mais turvos.

De fato, a difusão da internet, nos diversos campos do cotidiano da vida e da sociedade em geral, aliado à crescente adoção de tecnologias de comunicação e informação, está a promover mudanças que afetam vários ramos do direito, assim como o agir dos cidadãos.

Assim, se antes vários elementos eram identificados como próprios do campo digital, na atualidade, passaram a ingressar em nossas vidas e nas diversas áreas do direito, a ponto de apresentarem novas maneiras de pensar e de conviver, tornando-se praticamente impossível a análise de determinados fenômenos e de algumas áreas do direito, sem a correta compreensão de tais elementos trazidos pelas tecnologias de informação e comunicação.

O presente artigo de natureza exploratória, pautado em revisão bibliográfica, se desenvolve com o uso do método hipotético-dedutivo, fundado em pesquisa bibliográfica, na qual são examinados os aspectos relevantes sobre o conceito de dados pessoais e o tráfego de pacote de dados na rede.

Para tanto, parte-se da análise comparativa do Regulamento Geral sobre a Proteção de Dados (GDPR) da União Europeia, com a Lei Geral de Proteção de Dados Pessoais (LGPDP) do Brasil, examinando como esses países atuam com as respectivas legislações em relação à regulação e resolução de demandas oriundas do mundo virtual.

Destaca-se que a lei brasileira (LGPDP) considera usuário, no tratamento de dados pessoais, a pessoa natural ou a 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. Assim sendo, os usuários que tiverem seus dados pessoais captados e manuseados por inúmeras empresas e entes públicos contarão com o tratamento de proteção imposto na lei, consistente nas figuras da anonimização e pseudoanonimização.

Desta maneira, o artigo também se propõe a refletir sobre as principais técnicas de anonimização e pseudoanonimização, reconhecendo-as como ferramentas regulatórias utilizadas para possibilitar a análise de dados, além da ferramenta da reidentificação, por vezes, muito criticada pela doutrina, devido à possibilidade constante de sua desatualização, mas que não deixam de ser um avanço para a proteção do usuário.

Com isso objetiva-se estudar a anonimização e pseudoanonimização dos dados pessoais dos usuários, em busca das melhores técnicas para alcançar, de forma segura, a partir de um modelo de regulação da internet e do ciberespaço, por meio de normas, que se apresentam como transfronteiriças, tudo para garantir a transmissão das informações com segurança e precisão.

2 - Os Dados Pessoais que trafegam na internet e a sua proteção.

Sabe-se que a sociedade informacional é imersa em uma 'big data', assim entendida como um conceito que representa o grande volume, velocidade e variedade de dados produzidos na atualidade e que requer atualizações para a resolução de problemas demarcados pela necessidade de gerenciamento dos dados, sendo que a coleta de dados é realizada por atores múltiplos, que correm determinados riscos.

Nesse sentido, conforme explicam Cíntia Lima e Kelvin Peroli (2019, p. 72-73), "a coleta dos dados pessoais, por atores múltiplos contempla um risco: a violação de direitos fundamentais, como a identidade, a privacidade e a liberdade (a construção de um *Big Brother* pelo desenvolver de uma *Telescreen*)".

Nesse modelo de sociedade atual e informacional descrito pelos mencionados autores os serviços e garantias à privacidade e intimidade são expostos à publicidade na Internet a todo instante, sendo que direitos como o de esquecimento são impactados pela perpetuidade da disseminação dos dados, bem como os dados pessoais, são envoltos no contexto da disseminação e utilizados pelo marketing agressivo e comportamental da internet (LIMA e PEROLI, 2019, p.73).

Por isso, o direito à proteção de dados pessoais e privacidade deve se ater aos aspectos transfronteiriços do espaço digital para que o *enforccement* sobre a sua garantia seja realizada de maneira que a difusão dos conteúdos esteja regulada e dependa de seu âmbito de circulação, seja pelos seus diferentes diplomas de defesa e proteção dos dados pessoais, seja pelo consentimento informado e expresso que deve ser fornecido, conforme assevera a Lei Geral de Proteção de Dados Pessoais, tal qual a 'GDPR' da União Europeia e a Us Privacy Shield, dos Estados Unidos.

Além disso, recentemente, veio à luz as tramas de espionagens dos governos americanos e britânicos, por meio das revelações feitas pelo analista de sistemas, Edward Joseph Snowden, ex-funcionário da CIA e da NSA, aos jornais The Guardian e The Washington Post, detalhando um plano de vigilância global, o Programa Governamental-

PRISM, desenvolvido pelo Acordo da Five Eyes Alliance entre Austrália, Canadá, Nova Zelândia, Reino Unido e Estados Unidos, que possibilitou a coleta de dados diretamente de provedores de serviços de Internet estadunidenses, demonstrando ao mundo a fragilidade dos sistemas de proteção de dados pessoais na sociedade informacional.

As revelações de Edward Joseph Snowden escancararam o problema, marcado pelo antagonismo de interesses entre aqueles que atuam no espaço digital, tendo de um lado os usuários hipossuficientes, desavisados ou inocentes e, de outro lado, as grandes empresas, que buscam lucros com as inúmeras informações, os entes públicos e os agentes políticos, com os seus mais variados e escusos interesses. Tudo isso foi muito bem abordado em uma matéria jornalística, elaborada por Gellman e Poitras (2013), para o hebdomadário americano The Washington Post, publicada em 06/06/2013 e que explica, de forma detalhada, toda a espionagem e o acordo firmado entre as agências de espionagens dos referidos países.

Tem-se, pois, que o direito à proteção de dados pessoais consiste em um direito do sujeito cujos dados pessoais se referem e no qual o direito de exercer sobre ele o controle, bem como acesso a essas referidas informações pessoais, seja desse acesso à retificação, como modificações e tratamento, estão ambos no âmbito do direito da personalidade como assevera (FINOCHIARO, 2012, p. 01-06).

Desta maneira, quando falamos de privacidade, em sua proteção pelo direito em si, a expectativa do indivíduo é que esta seja normativa, ou seja, o usuário, em seu íntimo, visualiza e projeta a proteção como normativa, como sendo este devidamente regulado por leis.

Nesse sentido, Helen Nissebaum (2004, p. 101-139) enfatiza a privacidade como integridade contextual, que deve ser respeitada quando as normas de adequação, que descrevem quais são as informações apropriadas sobre determinado indivíduo em um dado contexto, e as normas de distribuição, que abordam os valores inclusos nos fluxos de transferência de informações entre as partes.

Para a autora, tais normas devem ser respeitadas, pois são valores atinentes à defesa da limitação do fluxo de informações, exemplificativamente, a prevenção de danos baseados na informação, a assimetria informacional, a autonomia, a liberdade, a democracia, a preservação de relacionamentos, bem como a liberdade de expressão, a eficiência e a segurança, que são valores citados, eis que identificados como protegidos no fluxo livre das informações, devendo, portanto, ser ponderados, diante do contexto em que estão inseridos. Enfim, por outras palavras, valores pessoais, assim como a privacidade e o direito a proteção de dados devem ser respeitados e ponderados no conflito de normas e princípios.

Sendo assim, Cíntia Lima e Kelvin Peroli (2019, p. 76) destacam a expectativa do usuário da internet:

> Assim, se determinada expectativa cognitiva de usuários, ao passar dos tempos, se transforma em uma expectativa normativa, por alteração dos valores sociais, a ponderação, como referida, sofrerá modificação, porque a integridade contextual da matéria (como a privacidade), em relação às normas de adequação ou às normas de distribuição, por sua vez, se atualizaram, por meio, *v.g*, de alteração legislativa que tenha abarcado a passagem de uma expectativa antes cognitiva para normativa.

Além disso, as revelações trazidas à baila por Edward J. Snowden, ao jornal The Washington Post, na mencionada matéria jornalística de Gellman e Poitras (2013), datada de 06/06/2013, revela ainda que o programa PRISM permitiu a coleta de dados pessoais diretamente de provedores de serviços de internet nos EUA, o que demonstra uma rede de interesses contrapostos dos usuários, do ciberespaço e dos atores do mercado do mundo virtual, que se utilizam da arquitetura do espaço digital para a construção de um modelo de internet voltado aos seus interesses econômicos, a partir dos dados pessoais coletados em conjunto ao marketing direcionado e comportamental.

Por tudo isso é que, cada vez mais, há a liberdade dos provedores de serviços de internet para desenvolverem modelos de privacidade como padrão para prestação de seus serviços, visando garantir a aplicabilidade dos princípios à proteção de seus usuários, nos moldes da GDPR europeia.

Neste particular, um exemplo sobre a navegação e sobre dados pessoais lançados na internet se refere ao espaço transfronteiriço, constitutivo da Internet e do ciberespaço. Neste particular, tem-se a regra prevista no artigo 3º, 1, do Regulamento da GDPR, cuja redação é a seguinte: "o presente regulamento aplica-se ao tratamento de dados pessoais efetuado no contexto das atividades de um estabelecimento de um responsável pelo tratamento ou de um subcontratante situado no território da União, independentemente de o tratamento ocorrer dentro ou fora da União".

Com isso, se entende que os dados pessoais e da proteção transfronteiriça de dados de titulares residentes na União Europeia se aplica aos controladores e aos operadores não estabelecidos no referido território geográfico. De fato, o Regulamento da GDPR entrou em vigor em 28 de maio de 2018 e integra a nova legislação da União Europeia e se aplica a todos os 28 Estados-membros e a qualquer país que venda produtos ou serviços dentro daquele território.

Além disso, quando se tratar de dados pessoais decorrentes do oferecimento de bens ou serviços essa norma também deve ser respeitada, seja pelo responsável residente na União Europeia, seja por um subcontratante não estabelecido nesse território, o que equivale dizer

que os agentes estrangeiros de tratamento de dados devem indicar representantes legais na União Europeia, como determina o art. 3º, 2 do mencionado Regulamento.

Por isso, toda empresa que pretende estabelecer transações comerciais com a União Europeia deve obedecer a novel lei, cujo objetivo maior não é outro senão o de certificar que o direito dos cidadãos à proteção de dados pessoais para se manter ativo na era digital. A busca, essencialmente, é promover um maior controle sobre as pessoas e os seus dados pessoais, bem como construir uma maior confiança na utilização dos tais dados pelas marcas e pelas empresas.

Essa norma se revela, pois, como um grande avanço, eis que as empresas ou órgãos das grandes empresas interessados (*stakeholders*) nos dados pessoais dos usuários de serviço de internet da União Europeia estão obrigados a se adequarem ao patamar de proteção mínima imposto pela norma.

A importância de tal regra pode ser constatada a partir das revelações feitas pelo jornal americano The New York Times, sobre o programa PRISM que permitiu a coleta de dados pessoais diretamente de provedores de serviços da Internet nos EUA, o que demonstra uma rede de interesses, de cunho político, financeiro, ou outro interesse qualquer, tal como destacam Cíntia Lima e Kelvin Peroli (2019, p. 78), todos esses interesses são contrapostos aos interesses dos usuários da internet e do ciberespaço, ou seja, de um lado, os interesses dos usuários e, de outro lado, os atores do mercado financeiro virtual, assim entendido aqueles que se utilizam do formato da plataforma da internet, com fins totalmente comercial e econômico.

Por essa razão, a GDPR europeia criou uma garantia fundamental na proteção de dados pessoais, em seu art. 33, 1, que se revela como a notificação obrigatória, em caso de violação de dados pessoais, da seguinte forma:

> Em caso de violação de dados pessoais, o responsável pelo tratamento notifica desse fato a autoridade de controle competente nos termos do artigo 55.o, sem demora injustificada e, sempre que possível, até 72 horas após ter tido conhecimento da mesma, a menos que a violação dos dados pessoais não seja suscetível de resultar num risco para os direitos e liberdades das pessoas singulares. Se a notificação à autoridade de controle não for transmitida no prazo de 72 horas, é acompanhada dos motivos do atraso.

Com isso, tem-se que uma vez notificado o responsável apresentará a sua defesa à autoridade de controle, no prazo de 72 horas, a menos que seja capaz de demonstrar em conformidade com o princípio da responsabilidade, que a eventual violação não é suscetível de implicar um risco para os direitos e liberdades das pessoas singulares.

Outra ferramenta muito comentada sobre a proteção de dados pessoais foi a '*Privacy Shield'*, estabelecida entre os EUA e a União Europeia, adotada em julho de 2016. Trata-se de

um modelo das disposições da GDPR europeia, com o objetivo de permitir a continuidade da transferência dos dados pessoais dos residentes na União Europeia e EUA, com as organizações sediadas neste país, em especial o Facebook e o Google, incluindo salvaguardas às autoridades estadunidenses quanto ao tratamento dos dados pessoais dos titulares da União Europeia.

Dessa maneira, a transferência desses dados pessoais pôde ser realizada para além das propostas previstas pela GDPR europeia (Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho), cuja edição é de 27 de abril de 2016, com a utilização da Privacy Shield que permitiu a interação entre os americanos e a comunidade europeia para o tráfego e o tratamento de dados pessoais, algo que não seria possível, sem a existência de uma lei que regulasse a proteção dos dados de seus usuários, não perdendo de vista que o referido mencionado Regulamento só entrou em vigor, conforme já destacado, em 28 de maio de 2018.

Embora pareça um acordo entre as partes, o programa Privacy Shield foi assumido com a imposição de ser observada uma *compliance* entre as partes. Assim, as organizações devem obter certificados dos EUA sobre *compliance* e governança corporativa, bem com declararem, publicamente, o compromisso de adesão aos princípios elementares da Privacy Shield, divulgando suas políticas de privacidade de acordo com os princípios e implementando tais dispositivos de forma integral, sob pena de incorrerem nas disposições da Section 5 do 'Federal Trade Commission Act.

A 'Privacy Shield' ainda na lição de Cíntia Lima e Kelvin Peroli (2019, p. 81) se: "impõe como direito dos titulares de dados pessoais: o direito de ser informado sobre o tipo e a finalidade do tratamento dos dados, a pretensão da organização pela transferência dos dados" e, como sua finalidade, deve haver consentimento quanto às configurações, sendo que "o direito de que sejam os dados pessoais utilizados apenas para a finalidade pactuada, devendo haver novo consentimento quando de reconfigurações", bem como "o direito de que sejam coletados apenas os dados essencialmente necessários para a finalidade pactuada". Ademais, realizadas reclamações, todas essas serão investigadas e o titular recebará notificação sobre o ocorrido.

Desta maneira, em relação ao trafego de dados e a transferência de dados entre países, esta será permitida, da seguinte maneira, como explicam Cíntia Lima e Kelvin Peroli (2019, p. 83): (i) quando o pais ou organismo internacional proporcionar o nível protetivo adequado ao previsto na lei, avaliado pela autoridade garante, (ii) quando o agente responsável pelo tratamento oferecer e comprovar garantias de cumprimento das disposições

da lei quanto a proteção de dados, avaliadas pela autoridade garante ou suas designadas agencias de certificação das cláusulas, normas corporativas, códigos de conduta, selos e certificados, (iii) quando a transferência for necessária ao cumprimento de cooperação jurídica internacional entre órgãos públicos de inteligência, investigação e persecução, (iv) quando necessária para a proteção da vida ou da incolumidade física do titular ou de terceiros, (v) para a execução de política pública ou atribuição legal do serviço público, (vi) quando tiver o titular fornecido consentimento especifico e em destaque à transferência, (vii) para o cumprimento da obrigação legal ou regulatória do controlador, (viii) quando necessária para a execução do contrato ou procedimentos preliminares ao contrato, a pedido do titular dos dados, (ix) para o exercício de direito em processo judicial, administrativo ou arbitral, (x) para os demais casos que se façam por necessários, em referência aos compromissos assumidos pelos Estado em acordos de cooperação internacional ou autorizadas pela autoridade nacional.

Em suma, tem-se que em relação aos dados pessoais, consideram-se as normas regulatórias acima identificadas para efeito da proteção de dados pessoais, bem como as soluções técnicas para a efetivação da anonimização, são os mesmos a serem pautados na pseudoanonimização. Neste, porém, visa-se a separação dos dados de seus proprietários, cuja reidentificação se torne possível havendo uma informação externa pela qual pode ocorrer uma interseção entre os dados, ou onde a fragilidade da pseudoanonimização quanto os dados suplementares, que são aqueles capazes de intersecionar com os seus titulares, a proteção não se revela suficientemente segura, e nenhum dos requisitos acima forem respeitados de forma condizente com as normas regulatórias, as normas de *compliance* e de governança corporativa que seus entes e organizações internas publicamente aceitaram e admitem como favoráveis.

3 - O tráfego e a proteção de dados pessoais na internet no território brasileiro.

No Brasil foi aprovada em 18 de agosto de 2018, a Lei nº. 13.709/2018, que dispõe sobre a transferência dos dados pessoais dos titulares localizados no Brasil, que é admitida quando o Estado ou organismo internacional proporcionar grau de proteção adequado ao previsto pela lei brasileira, conforme descrito no artigo 33, inciso I.

Além disso, "quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos na lei", mediante os requisitos ditados pelo inciso II do art. 33, ou seja, o agente de tratamento deverá oferecer e comprovar garantias de nível protetivo correspondente ao nível de proteção

internacional, que poderá ocorrer por meio de cláusulas contratuais específicas, clausulas-padrão, normas corporativas, selos, códigos de conduta e certificações.

A Lei 13.709/2018, de acordo ainda com o artigo 3º, aplica-se a qualquer operação de tratamento realizado no Brasil, desde que os dados tenham sido coletados em território nacional, haja vista que o objetivo do tratamento de dados pessoais de indivíduos localizados no país, ou a oferta ou fornecimento de bens ou serviços, bem como sobre os dados coletados no território nacional e que sejam objeto de tratamento no exterior, em virtude do uso compartilhado de dados.

A Lei Geral de Proteção de Dados (Lei 13.709/2018), no entanto, não se aplica aos dos dados de origem estrangeira, 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 na mencionada lei, tal como determina o art. 4º, inciso IV.

Ao refletirmos sobre a Lei Geral de Proteção de Dados (LGPD), temos que nos debruçar também sobre o Marco Civil da Internet (Lei 12.965/2014), que estabeleceu garantias principiológicas para que a lei específica tivesse a atual abrangência e eficácia.

De fato, o Marco Civil da Internet estabeleceu regras que visam orientar os direitos e deveres dos usuários, provedores de serviços e conteúdos e demais envolvidos com o uso da Internet no Brasil.

Entretanto, é preciso ter claro que as declarações de Edward Joseph Snowden, em maio de 2013, referente à construção de programas de vigilância que causaram grande impacto no mundo, inclusive no Brasil, pois se descobriu que a Agência Nacional de Segurança Nacional (NSA) espionou várias personalidades brasileiras, dentre elas, a então Presidente da República, Dilma Rousseff.

Tais fatos causaram dificuldades no âmbito da construção da lei pátria e da sua efetiva aplicabilidade, além de questionamentos sobre a inconstitucionalidade de alguns de seus dispositivos.

Contudo, Maurício Santoro e Bruno Borges (2017), observam que:

> Durante 2013 e 2014, o Brasil trabalhou em conjunto com outros países, especialmente a Alemanha - também um dos principais objetivos da NSA - e co-patrocinou duas resoluções na Assembleia Geral da ONU (69/166 e 68/167), ambas intituladas "O direito à privacidade na era digital". Os dois textos são semelhantes, mas o segundo é mais abrangente, levando em consideração as discussões em outras instituições das Nações Unidas, como o Conselho de Direitos Humanos e o trabalho do Escritório do Alto Comissariado para os Direitos Humanos, observando como eles estão construindo. uma estrutura global para lidar com a Internet. Sem nomear a

> NSA ou o governo americano, a resolução enfatiza que a vigilância em massa e a violação da privacidade são ameaças às liberdades democráticas. Ele enfatiza que os Estados e as empresas têm a obrigação de respeitar e proteger os dados pessoais. A segunda resolução também menciona metadados - uma especificação importante, uma vez que a última geralmente não é bem definida nas legislações nacionais.

Tudo isso ensejou a construção do art. 8º, caput da lei nº 12.965/2014 que determina o seguinte: "a garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet", mas para tanto, o usuário possui uma série de direitos, consoante se verifica da leitura do art. 7º da mencionada lei:

> 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;
> 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.

Assim sendo, no Brasil, embora o Marco Civil da Internet (Lei 12.965/2014) não tenha disposto de forma minuciosa sobre as sanções aplicáveis ao descumprimento de medidas de proteção de dados pessoais, ele garante a "indenização pelo dano material ou moral decorrente de sua violação", nos moldes do art. 7º, I, bem como a responsabilidade dos

provedores de conexão e de aplicação de internet por danos decorrentes de conteúdo gerado por terceiros, nos moldes dos artigos 18 e 19.

Por fim, para se empreender um "*enforccement"* efetivo à proteção de dados pessoais, a lei instituiu sanções administrativas de impacto financeiro e de imagem, que são aplicáveis através da Autoridade Nacional de Proteção de Dados, que após a realização de procedimentos administrativos, que podem render sanções dos seguintes tipos, de acordo com o artigo 52 da Lei Geral de Proteção de Dados, como por exemplo: (i) a advertência com prazo para adoção de medidas corretivas; (ii) multa simples ou diária de até 2% (dois por cento) do faturamento do último exercício financeiro de pessoas jurídica, excluídos os tributos, sendo limitada ao total de 50 (cinquenta) milhões de reais por inflação; (iii) publicização da infração; (iv) bloqueio dos dados pessoais até a regularização da proteção e (v) eliminação dos dados pessoais.

4 - Da necessidade de tratamento dos dados pessoais – anonimização e pseudoanonimização dos dados pessoais conforme assevera a Lei n. 13.709/18.

Para a compreensão do termo, por primeiro, é necessário ter claro que a anonimização, nas palavras de Celso Lafer (1988, p. 271-272) é um dos instrumentos que torna a liberdade de expressão desarraigada de preocupação social, pois a identificação on-line torna o indivíduo inserido na esfera social do espaço digital. A anonimização, assim, é uma forma de torná-lo só, mesmo no ciberespaço, protegendo a sua vida privada e os seus dados pessoais. Por isso, o autor destaca a importância do pensamento de Hannah Arendt, em especial o seu olhar sobre a necessidade da intimidade e à liberdade do juízo.

Deve-se ter claro, no entanto, que o conceito de liberdade para Hannah Arendt é extremamente complexo e difuso, exigindo a análise de várias de suas obras para a correta compreensão. Ademais, deve-se ter claro que a filósofa não enxerga a liberdade como fruto do livre arbítrio, oriundo de uma concepção cristã e liberal, mas uma concepção proveniente da política.

Nesse sentido, Hannah Arendt (1995, p. 335) explica o seguinte:

> A liberdade filosófica, a liberdade da vontade, é relevante somente para as pessoas que vivem fora das comunidades políticas, como indivíduos solitários. As comunidades políticas, nas quais os homens se tornaram cidadãos, são produzidas e preservadas por leis: e tais leis, feitas pelos homens, podem variar muito e podem dar forma a inúmeros tipos de governos, todos eles, de uma maneira ou de outra, tolhendo a vontade livre de seus cidadãos.

Percebe-se que a filósofa promove uma distinção entre a liberdade interior e a liberdade política. Para ela a liberdade não é fruto do livre arbítrio, que se relaciona com a interioridade humana, mas com o agir engajado de estar mundo para promover mudanças, por meio do diálogo. Por isso, para ela, também é importante a questão do totalitarismo, eis que este impede a pluralidade humana e faz imperar a homogeneidade da fala do governo que exerce o poder e inviabiliza o diálogo, determinando o cumprimento de normas e leis.

Enfim, em Hannah Arendt o conceito de liberdade é a ação e não a sua motivação ou fim, ou seja, ela se aproxima do conceito de *virtù* de Maquiavel, mas com esse não se confunde, pois para o filósofo florentino a liberdade tem a liberdade como o agir diretamente associado à ideia de resultado final da ação ou, por outras, palavras a ação deve ser uma ação eficaz, que atinja o seu objetivo e essa deve ser, no seu entender, a busca do governante.

Depois, também é necessário se compreender o que Hannah Arendt pensa como intimidade. Para a filósofa alemã (2001, p. 48):

> O que hoje chamamos de privado é um círculo de intimidade cujos primórdios podemos encontrar nos últimos períodos da civilização romana, embora dificilmente em qualquer período da antiguidade grega, mas cujas peculiaridades multiformidade e variedade eram certamente desconhecidas de qualquer período anterior à era moderna.

É por isso que Celso Lafer (1988, p. 264) explica que "a moderna descoberta da intimidade parece constituir uma fuga do mundo exterior como um todo para a subjetividade interior do indivíduo".

Com os dois conceitos mencionados, Hannah Arendt propõe que no mundo das aparências, da esfera pública e da esfera social, nunca se está sozinho, pois sempre estamos ocupados em demasia para pensar, mas para se instaurar um diálogo exige-se um provisório desligamento, certo afastamento do mundo exterior, inerente a todas as atividades mentais. Como consequência, o direito de estar só, é o que permite parar para pensar o significado das coisas.

Enfim, para o exercício da liberdade, é pressuposto a existência da intimidade e como explica Paulo José da Costa Jr. (1995, p.12-13): “a intimidade interior reveste-se de natureza física e material. O indivíduo afasta-se da multidão. Recolhe-se ao seu castelo. Desce às profundezas de sua alma e sai em busca do seu ser”. Contudo, continua o autor, “nada impede que o solitário físico venha a manter contato com a vida social, através dos meios de comunicação de que disponha” ou, ainda, “trazendo para junto dele, na sua fantasia, o diálogo silente dos vivos e dos mortos”.

Além disso, é necessário se atentar às palavras de Nicholas Negroponte (1995, p. 215) que, há 25 anos, já vaticinava:

> Sou otimista por natureza. Contudo, toda tecnologia ou dádiva da ciência possui seu lado obscuro. Na próxima década, veremos casos de abuso de propriedade intelectual e invasão de nossa privacidade. Enfrentaremos o vandalismo digital, a pirataria de software e o roubo de dados.

Ora, diante de tais ensinamentos, percebe-se que a Lei nº. 13.709/2018 define em seu art. 5º, inciso IX, a anonimização como "a utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo".

Com isso, percebe-se que a anonimização é um elemento para a garantia da liberdade de expressão, tanto em países totalitários, que mitigam direitos preconizados fundamentais, como na democracia, na qual se faz necessária quando a vontade de uma maioria interfere na viabilidade da liberdade de expressão de uma minoria, em virtude dos riscos de retaliação. Esse conceito possibilita a liberdade de expressão na plenitude das faculdades de juízo de um indivíduo, evitando-se a vindita do corpo social que o cerca.

Daí trazermos à baila dois casos emblemáticos sobre a anonimização. O primeiro, ocorrido na França onde, segundo Paulo José da Costa Jr. (1995, p. 13), pela primeira vez o Tribunal Civil de Sena acolheu a tese da proteção à vida privada, em 16 de junho de 1858. Nesse caso uma mulher encarregou dois artistas de retratarem-na em seu leito de morte. Como explica o autor: "o desenho foi abusivamente exposto e colocado à venda em um estabelecimento comercial". O tribunal determinou a apreensão do desenho e das provas fotográficas e concluiu que: "por maior que seja uma artista, por histórico que seja um grande homem, tem sua vida privada distinta da pública, seu lar separado da cena e do fórum" e, portanto, "podem desejar morrer na obscuridade, quando ou porque viveram no triunfo."

O segundo caso é o denominado McIntyre vs. Ohio Elections Commission, julgado pela Suprema Corte dos EUA, no qual se discute a dualidade da anonimização, pois elucida que não somente os ilícitos devem ser memorados, mas também a sua necessidade em face da tirania, mesmo diante dos sistemas democráticos. Assim, a Suprema Corte americana se pronunciou da seguinte maneira:

> O anonimato é um escudo sobre a tirania da maioria, Assim, exemplifica o propósito por detrás da "Bill of Rights", e da "First Amendment", em particular para proteger indivíduos impopulares de retaliação e suas ideias de supressão pelas mãos de uma sociedade intolerante. No entanto, o direito de permanecer anônimo pode ser um abuso quando protege uma conduta fraudulenta.

Em razão de tais fatos, Jonathan Zittrain (2006, p. 1974), define a internet como a tecnologia com capacidade geracional, ou seja, um sistema capaz de produzir mudanças

inesperadas, por meio de contribuições variadas, conceito este que pode ser retratado diante da ideia de atualização da realidade, pelo aumento da potência considerada da virtualidade como preceitua Pierre Lévy, que se dedica a analisar as técnicas de transmissão e tratamento de mensagens, como modalidades de comunicação e possibilidade de redefinir organizações.

Com efeito, Pierre Lévy (2001, p. 195) observa em época de globalização e de conflitos mundiais diversos, de tempo instantâneo, da informação fragmentada, "das mídias triunfantes e da tecnociência multiforme e onipresente, quem não sente que é preciso repensar os objetivos e os meios da ação política?". Por isso, continua o seu pensar enfatizando a necessidade de atenção às escolhas técnicas a partir das decisões democráticas para alteração da política. No entanto, dá ênfase à possibilidade de novas reinterpretações, desvios e conflitos tecnociência diante da produção do coletivo. Assim explica o seguinte:

> As sociedades ditas democráticas, se merecem seu nome, têm todo o interesse em reconhecer nos processos sociotécnicos fatos políticos importantes, e em compreender que a instituição contemporânea do social se faz tanto nos organismos científicos e nos departamentos de pesquisa e desenvolvimento das grandes empresas, quando no Parlamento ou na rua. Ao lançar o catálogo ou trabalhar nas manipulações genéticas, contribui-se da mesma forma para forjar a cidade do mundo quanto votando. Mas esta produção é sempre ambígua, polissêmica, aberta à interpretação. O Minitel francês, de grande rede estatal que era ao ser lançado, foi rapidamente reinterpretado por grande número de usuários como um suporte de troca de mensagens interativa onde foram inventadas novas formas de comunicar, mas estas trocas de mensagens foram desviadas pelos vendedores de ilusões cor-de-rosa que, por sua vez, etc. (LÉVY, 2001, p. 195-196)

Com essas observações, observa-se que nos países não democráticos a anonimização é efetiva, pois expõe as ideias negadas pelo sistema nacional, de forma a descaracterizar os seus agentes e destituí-los de responsabilidade perante os conteúdos espraiados. Neste sentido, não se pode deixar de lembrar que o ciberespaço é a plataforma sobre a qual a anonimização se conecta com o ímpeto da publicização de ideias contra a restrição da liberdade de expressão, além de ser o espaço onde os discursos anônimos são defendidos pela difusão de ideias, para a proteção da autonomia individual, da liberdade de expressão e da privacidade.

Neste sentido, como explicam Cíntia Lima e Kelvin Peroli (2019, p. 69):

> Em 29 de julho de 2017, a Lei Federal Russa nº 241-FZ, que entrou em vigor no dia 1º de janeiro de 2018, previu a proibição da anonimização sobre as mensagens instantâneas na Internet. Os provedores de acesso podem apenas prover esse tipo de conteúdo mediante a identificação telefônica de seus usuários, por meio de um acordo para a identificação realizada entre o provedor de acesso à Internet e a operadora de telefonia. Os provedores de acesso á Internet também devem proibir o acesso de usuários a aplicações se há suspeita que o conteúdo possua informações que violem a legislação russa, havendo o banco de dados do Serviço Federal de Supervisão em Assunto de Comunicações, dos conteúdos proibidos. A sanção aplicada por não se atender ao requerimento da lei é o bloqueio dos próprios provedores.

Entretanto, se de um lado a liberdade de expressão deve ser garantida na internet, de outro lado, a anonimização e originalidade estão sujeitas a restrições, como a violação de direitos autorais e conteúdos com restrições de idade, que limitam a liberdade de expressão e a disponibilidade de conteúdo, eis que tais temáticas são regidas por legislações nacionais e internacionais, garantindo, por exemplo, os direitos autorais ou imposição restrições para conteúdos pornográficos, para pessoas menores de 18 anos.

No Brasil, porém, o anonimato como exercício do direito da liberdade de expressão e manifestação do pensamento é vedado pelo artigo 5º, inciso IV, da Constituição Federal. Aliás, tal preceito já era previsto pela antiga Lei de Imprensa (lei 5.250/1967), revogada pela ADPF nº 130/DF, de 2009. Já no Marco Civil da Internet (Lei 12.965/2014), os comentários anônimos devem ser rastreáveis pelo endereço IP. Portanto, em verdade, tais comentários são pseudoanônimos, como revela o §1º do artigo 10, da mencionada lei.

Além disso, Paul Ohm (2010, p. 1707) enfatiza a anonimização pode se revelar como o processo pelo qual uma informação é manipulada em um banco de dados, a fim de criar dificuldade na reidentificação ou desanonimização dos sujeitos dos dados ou, ainda, quando o dado é desanonimizado e a pessoa o reindentifica como dado anônimo para conectá-lo com informações externas.

Neste particular várias técnicas são largamente utilizadas para o processo de anonimização, tais como as '*release-and-forget'*, também conhecida como de-identificação (*deidentification*) e a denominada remoção de informações pessoalmente identificáveis, as 'Personally Identifiable Information – PII*'*, nas quais um agente de tratamento libera os registros de forma pública ou de forma privada para um terceiro ou membro de sua própria organização e, depois, os esquece, não realizando tentativas de acompanhar o que se sucede como tais dados. Porém, como observam Cíntia Lima e Kelvin Peroli (2019, p. 70) antes de liberá-los são realizadas algumas modificações nas informações para anonimizá-las, seja por meio de "técnicas para processos de supressão (a supressão dos nomes dos sujeitos, por exemplo)", seja pelo emprego da "generalização da base de dados (como a generalização de datas de nascimento em um banco de dados para conter tão somente o ano de nascimento dos sujeitos), que detém grau mais elevado de utilidade aos agentes de tratamento que as técnicas de supressão."

Nessa esteira de raciocínio temos ainda aquilo que Paul Ohm (2010, p. 1752-1753) denomina de '*release-and-forget'*, ou seja, técnica amplamente utilizada que promete a privacidade, mas permite a disseminação dos dados, para as mais diversas utilidades dos

agentes de tratamento, pois entende não ser possível uma anonimização perfeita, em face da conexão com as informações externas, que são extremamente utilizadas no cenário digital.

No cenário da regulação há ainda a dificuldade do cumprimento (*enforccement*), por isso Paul Ohm (2010, p. 1762) destaca a figura da reidentificação ou desanonimização, como sendo uma das medidas legislativas que poderiam ser adotadas pelas autoridades em face aos softwares dos agentes que se utilizam de dados anônimos. Nesse particular, ele destaca a importância da 'Data Governance', para garantia protetiva dos dados pessoais, com a exigência da fiscalização dos dados considerados anônimos. Estes devem ser objeto de cuidados específicos, pois os agentes de tratamento, por meio da utilização de informações externas ao contexto dos dados anônimos, podem chegar à reidentificação ou desanonimização dos dados.

Diante de tais considerações, o "caput" do artigo 12, da Lei Geral de Proteção de Dados, a LGPD (Lei 13/709/2018) dispõe que "os dados anonimizados não serão considerados dados pessoais para os fins desta Lei, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis, puder ser revertido", ou seja, a regra é que dados anônimos não são considerados dados pessoais, exceto aqueles em que o processo de desanonimização puderem ser revertidos, aí se estabeleceu a proteção de dados que possam sofrer o processo próprio de reidentificação, ou mediante esforços razoáveis de reversão. Nesta última hipótese, no entanto, o §1º do art. 12 esclarece que: "a determinação do que seja razoável deve levar em consideração fatores objetivos, tais como custo e tempo necessários para reverter o processo de anonimização, de acordo com as tecnologias disponíveis, e a utilização exclusiva de meios próprios".

Não obstante isso, os dados "utilizados para formação do perfil comportamental de determinada pessoa natural, se identificada", são considerados como dados pessoais, nos moldes do art. 12 §2º da referida lei.

Com efeito, Patrícia Peck Pinheiro (2018, p. 25-26) também fala na figura de um terceiro gênero na proteção de dados previsto na Lei Geral de Proteção de Dados (LGPD), que seriam os dados anonimizados, relativos a um titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do tratamento.

Assim, Danilo Doneda (2011, p. 43-44) complementa essa ideia ao destacar que esse dado anonimizado seria uma espécie de antítese do dado pessoal, desqualificado a par do implemento do procedimento técnico chamado de anonimização.

Após a colocação de tais problemas fica mais fácil a compreensão dos termos empregados pela Lei nº 13.709, de 14 de agosto de 2018, ao estabelecer que o dado anonimizado é aquele dado "relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (art 3º, inciso III), ao passo que a pseudonimização "é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro" (art. 13§ 4º).

Assim, o processo técnico denominado de "anonimização", inserido no artigo 5º, IX, da Lei Geral de Proteção de Dados, nada mais representa do que a dissociação entre determinado dado pessoal e o seu respectivo titular, por meio de inúmeros procedimentos específicos que podem ser implementados para sua concretização, quase sempre a partir da supressão de determinado elementos identificadores que constam de uma base de dados, por meio de supressão do dado, generalização, randomização e pseudoanonimização.

Nesse contexto, é importante registrar que os bancos de dados digitais contribuem de forma direta para com o acúmulo de dados e para a utilização indevida dos mesmos, pois não se tem a segurança da finalidade dada a qualquer tipo de informação que, eventualmente, possa servir para identificar o titular do dado. Nesse sentido, Richard A. Posner (2008, p. 248) já analisara a pertinência do estudo de ressignificação da vigilância com relação aos dados, à luz da sociedade da informação, ao revelar que:

> (...) até recentemente, as informações que as pessoas voluntariamente divulgavam a fornecedores, agências de licenciamento, hospitais, bibliotecas públicas, etc., estava disperso, fugitivo (porque o volume de registros em papel geralmente os faz serem descartados como assim que eles perdem seu valor para a empresa) e somente pesquisáveis com grande dificuldade. Portanto, embora alguém tenha voluntariamente divulgado informações privadas, informações em inúmeras ocasiões para diversos destinatários, uma delas retinha, na prática, muita privacidade. Porém, com a digitalização, as informações gravadas não apenas podem ser mantidas indefinidamente em baixo custo, mas também as informações mantidas por diferentes comerciantes, seguradoras e agências governamentais podem ser prontamente reunidas, abrindo caminho para reunir todas as informações registradas relativas a um indivíduo em um único arquivo digital que pode ser facilmente recuperado e pesquisado. Deveria em breve será possível - talvez já seja possível - criar dossiês eletrônicos abrangentes para todos os americanos, semelhante ao tipo de dossiê que o FBI compila quando realiza investigações em segundo plano de candidatos a emprego sensível no governo ou investiga crimes suspeitos. A diferença é que o dossiê digitalizado, que eu imagino, seria atualizado continuamente (...).

Diante disso, Guilherme Martins e José Luiz Faleiros Júnior (2019, p. 61) explicam que o chamado grau de identificação de um dado pessoal será o parâmetro utilizado na aferição do processo de anonimização.

Já Bruno Bioni (2019, p. 71) assevera, com maior clareza, o iter da anonimização, referente à identificação do dado a ser, por exemplo, suprimido ou generalizado, vejamos: (i) supressão do CPF, por ser um identificador capaz de diferenciar até mesmo pessoas homônimas, sendo um identificador único, logo, a sua disponibilização, ainda que parcial, dos seus cinco primeiros dígitos, não seria prudente; (ii) generalização do nome completo constando apenas o prenome, desde que fosse observado que os nomes da base de dados não são comuns, cujo objetivo seria evitar que um nome possa ser atribuído a um indivíduo em especifico; (iii) generalização da localização geográfica, em vez de disponibilizar o número completo do CEP, seriam divulgados apenas os seus primeiros dígitos, para quebrar o vínculo de identificação da informação com um sujeito; e, por fim, (iv) a generalização da idade, uma vez que divulgar a idade exata, seria viabilizar a categoria dos indivíduos como jovens adultos ou idosos e, por outro lado, inviabilizaria a individualização de dados ao universo de pessoas que se enquadram na mesma faixa etária.

Enfim, os casos de anonimização e pseudoanonimização em nenhum momento podem permitir que se faça a reversão a ponto de se identificar os detentores de tais dados pessoais. A anonimização e pseudoanonimização consistem na verdadeira separação dos dados de seus proprietários, sendo que ambas exigem a obediência aos princípios gerais de proteção e aos direitos do titular apresentada na LGPD, em especial os arts. 1º a 6º e 17 a 22 da referida lei.

5 - Conclusão

Ao examinar a temática digital ora exposta temos claro que a internet tem a possibilidade de permitir participação mais viva e intensa nas relações privadas, sociais e políticas dos cidadãos.

Contudo, se os atrativos e possibilidades podem ser infinitos, da mesma forma também podem ser os desvios, os abusos, as práticas ilícitas e o cometimento de delitos no mundo digital.

A interação com o mundo digital, pois, não pode mais ser ingênua e pueril, principalmente se tivermos em conta que o envio de um singelo e-mail, a mensagem enviada será decomposta em pacotes de dados, contendo endereços e cabeçalho, que percorrem uma grande variedade de caminhos e, depois, são reordenados e reunidos para a leitura do destinatário.

Portanto, é importante que aja a proteção dos infinitos dados que transitam pela internet.

Assim sendo não é à toa que a Lei do Marco Civil da Internet é fundada em três pilares, a saber: a) a neutralidade da rede; b) a liberdade de expressão; e c) a privacidade dos usuários.

Esses princípios são fundamentais para a compreensão do tratamento dispensado aos dados pessoais, com o objetivo de proteção dos direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Por isso, podemos perceber que a Lei Geral de Proteção de Dados, em seu artigo 5º, XI, busca a retirada dos dados pessoais coletados, por meio da anonimização, quaisquer informação que permita identificar e, evidentemente, expor a pessoa a qual tais dados dizem respeito.

Mas não é só. A legislação atual impossibilita qualquer evidencia de reidentificação de tais dados, pois se preocupa com o risco de violações dos dados coletados, que possam colocar em risco a integridade, a intimidade e a vida privada do usuário da internet.

Admite-se, mas de maneira bastante restritiva, a utilização de dados pessoais em estudos de saúde pública, para a finalidade de realização de estudos e pesquisas, desde estes sejam mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico, assim como a figura da pseudonimização, que se apresenta como tratamento dispensado, por meio do qual, um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador, também, em ambiente controlado e seguro.

Assim, seguindo a legislação europeia e americana, o Brasil tem, na atualidade, uma legislação que se apresenta como protetiva ao usuário, em especial, com as figuras da anonimização e da pseudonimização, restando apenas a sua correta aplicabilidade, que se deve se dar por meio de rigoroso procedimento fiscalizatório.

Contudo algumas advertências ainda são necessárias. Os dados pessoais ou não podem ser dados sujeitos à anonimização ou a de pseudonimização. Os primeiros não podem ser associados direta ou indiretamente a uma pessoa, enquanto os segundos, por meio de relações adicionais na conexão, podem ser manipulados com mais liberdade desde que seja garantida a privacidade dos titulares da informação, tornando as operações de tratamento mais seguras, consoante a regra prevista no artigo 3º da LGPD.

Deve-se ter claro, no entanto, que o problema fulcral dessa temática é a complexidade, o volume, a velocidade e o dinamismo dos Big Datas que, na atualidade, estão a atuar, cada vez mais, de forma expandida, por meio de ferramentas analíticas e de desempenho elevado, com alta capacidade de eficiência, para buscar dados na rede mundial, com o objetivo de interpretá-los e reinterpretá-los e, eventualmente, identificar pessoas.

Dessa maneira, as figuras da anonimização e da pseudonimização podem não ser suficientes, se houver o emprego de técnicas e dados complementares. Por outras palavras, os dados anonimizados ou que aqueles que sofreram um processo de pseudonimização, por vezes, podem não garantir o sigilo esperado, eis que, eventualmente, não estão imunes a consultas, a cruzamento de informações, a análise de meios de identificação de padrões, etc.

Desta maneira todos aqueles que trabalham com tais dados devem adotar mecanismos mais severos de controle para evitar o vazamento de dados ou uso não autorizados de tais dados, em especial quando estão envolvidos dados pessoais.

A anonimização ou pseudonimização só é segura enquanto tais dados não enfrentam os processos de reversão, que permitem a identificação dos dados pessoais.

Assim sendo todo aquele que se dedicar a manejar dados, deve promover operação de tratamento, seja ela realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de evitar vazamentos e atos ilícitos variados, que atinjam os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Por isso, tais pessoas devem investir em segurança de dados que possam ir além da anonimização ou pseudonimização, tais como a criptografia, técnicas de diminuição de riscos de vulnerabilidade, ou detecção de códigos maliciosos ou software nocivo (malware), fraudes internas, mecanismos que dificultem o acesso não autorizado etc, tudo para garantir uma nova cultura fundada na proteção dos dados pessoais do usuário, como almeja a legislação ora comentada.

Referências:

ARENDT, Hannah. **A condição humana**. Trad. Roberto Raposo. 10. ed. Rio de Janeiro: Forense Universitária, 2001**.**

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense. 2019.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em 20.mar. 2020.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em 15.mar. 2020.

_____. **Lei nº 13.709, de 14 de agosto de 2018**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm Acesso em 10. mar.2020.

COMUNIDADE EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016**. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT. Acesso em 20.mar.2020.
COSTA JR., Paulo José**. O direito de estar só – Tutela Penal da Intimidade.** 2ª ed. rev. e atual. São Paulo: Revista dos Tribunais, 1995.
DONEDA, Danilo, **A proteção dos dados pessoais como um direito fundamental**. Joaçaba: Espaço Jurídico. v. 12. jul/dez. 2011, p. 91-108.
ESTADOS UNIDOS DA AMÉRICA. McIntyre vs. Ohio Elections Comm'n*, 514 US 334* (1995), Disponível em: https://supreme.justia.com/cases/federal/us/514/334/, Acesso em 10.fev.2020. Traduzido pelos autores.
FINOCHIARO, Guisella. **Privacy e protezione dei dati personali, Disciplian e strumenti operativi***",* Zanichelli: Bologna, 2012.
GELLMAN, Barton, POITRAS, Laura, **U. S., British intelligence mining data from nine U.S. Internet companies in broad secret program**, Washington D. C.: The Washington Post, 2013, Disponível em: https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-mine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html. Acesso em 04.fev.2020.
LAFER, Celso, **A reconstrução dos direitos humanos: um diálogo com o pensamento de Hannah Arendt**. São Paulo: Companhia das Letras. 1988.
LÉVY, Pierre. **As tecnologias da Inteligência – o futuro do pensamento na era da informática.** Trad. Carlos Irineu da Costa. 10ª reimp. Rio de Janeiro: Editora 34, 2001.
LIMA, Cíntia Rosa Pereira de; **PEROLI**, Kelvin. **Direito Digital – Complaince, Regulação e Governança**. São Paulo: Editora Quartier Latin. 2019.
MARTINS, Guilherme Magalhães; **FALEIROS JÚNIOR**, José Luiz de Moura. Direito & Internet IV – **Sistema de Proteção de Dados Pessoais**. São Paulo: Editora Quartier Latin. 2019.
NEGROPONTE, Nicholas. A vida digital. Trad. Sérgio Tellaroli. São Paulo: Companhia das Letras, 1995.
NISSIENBAUM, Helen, **Privacy as Contextual Integrity**, Washington Law Review, vol. 79, 2004.
OHM, Paul. **Broken Promises of Privacy. Responding to the Surprising Failure of Anonymizations**. UCLA Law Review: Califórnia. 2010.
PINHEIRO, Patricia Peck. Proteção de Dados Pessoais: comentários à Lei 14.709/2018 (LGPD). São Paulo. Saraiva. 2018.
POSNER, Richard A. **Privacy, surveillance, and law.** University of Chicago Law Review: Chicago. v. 75, 2008, p. 245-260.
SANTORO, Maurício; BORGES, Bruno. Brazilian Foreign Policy Towards Internet Governance. **Rev. bras. polít. int**., Brasília , v. 60, n. 1, e003, 2017 . Available from <http://www.scielo.br/scielo.php?script=sci_arttext&pid=S0034-73292017000100203&lng=en&nrm=iso>. access on 22 Mar. 2020. Epub Feb 06, 2017. https://doi.org/10.1590/0034-7329201600111.
ZITTRAIN, Jonathan, The Generative Internet. **Harvard Law Review**. Vol. 119. Cambridge. Massachesetts. Harward University Press. 2006. Disponível em: https://dash.harvard.edu/bitstream/handle/1/9385626/zittrain_generativeinternet.pdf?sequence=1. Acesso em 10.fev.2020.