1 INTRODUÇÃO

Os direitos da personalidade buscam proteger e garantir o respeito à vida, à integridade física, bem como aos demais bens necessários ao desenvolvimento da personalidade humana. São direitos tidos como essenciais, intrínsecos ao ser humano e indissociáveis; portanto, vitais para o seu desenvolvimento (BITTAR, 2014).

A partir da identificação do seu âmbito de proteção, é possível afirmar que existe uma pluralidade de direitos da personalidade, observa-se: o direito à integridade física e psíquica; o direito à vida; o direito à liberdade e à igualdade; o direito à imagem, à hora, ao nome; e o direito a zelar pela privacidade e pela intimidade. Desse modo, observa-se que qualquer direito que tenha como conteúdo matéria relativa à identificação do ser humano como pessoa, é um direito da personalidade.

O direito à privacidade é um direito da personalidade. Sua origem retorna ao direito norte-americano, no final do século XIX, após a publicação do artigo intitulado *The right to privacy*. Warren e Bradeis infundiram a ideia de que a privacidade correspondia ao direito de ser deixado em paz, um direito de completa imunidade, que visava a proteger a personalidade violada de cada indivíduo. Essa concepção incorporava um *insight* psicológico, em que a imagem que o indivíduo tem de si mesmo pode ser distorcida quando suas informações são disponibilizadas a terceiros (FESTAS, 2009).

Na Europa, a privacidade começou a ser tratada pelo direito na segunda metade do século XX, após a disseminação do computador- um pouco mais tarde do que nos Estados Unidos. Portanto, o paradigma que faz emergir a preocupação com a privacidade na Europa é tecnológico. A tutela refere-se aos dados pessoais e o seu controle pelo indivíduo contra a interferência de outros (PEIXOTO; EHRHARDT JÚNIOR, 2020).

Em virtude do surgimento de novas violações ao direito de personalidade, Hubmann verificou a necessidade de técnicas de abordagem de possíveis âmbitos do direito geral de personalidade. Desse modo, traçaram-se três círculos de proteção, dispostos de acordo com a natureza da personalidade, quais sejam: uma esfera individual, uma privada e uma secreta. Tais esferas correspondem aos círculos concêntricos, em que o conteúdo presente na esfera nuclear recebe uma maior proteção. (SIMÃO FILHO; CUNHA).

Em um contexto contemporâneo Ehrhardt Júnior, define que a privacidade é composta por três dimensões: uma espacial, uma dicisional e uma informacional. A dimensão espacial refere-se ao espaço vital físico para o desenvolvimento do indivíduo, é de onde todos os aspectos relacionados à privacidade se originam. A dimensão decisional protege o modo de vida do indivíduo, suas características e decisões, de modo que a pessoa possam se desenvolver dentro de uma esfera de liberdade individual que ela constrói. A dimensão informacional, relacionando-se à proteção dos dados individuais, por meio da autodeterminação pessoal e o direito de ser autor da própria vida. (PEIXOTO; EHRHARDT JÚNIOR, 2020).

Em relação à sua dimensão informacional, a privacidade deve ser analisada como algo abstrato e, ao mesmo tempo, a partir de contextos particulares, de modo que a violação ocorre quando uma interferência afeta uma determinada matéria individual. Nessa dimensão, a violação pode ocorrer por meio de coleta. de processamento e de disseminação de informações ou de uma invasão a um banco de dados. (PEIXOTO; EHRHARDT JÚNIOR, 2020)

Considerando essas três dimensões da privacidade, principalmente a dimensão informacional, insere-se a temática central do presente artigo. Na era da informação, a privacidade e os dados a ela correspondentes são constantemente ameaçados pelos tratamentos das bases de dados e pelos algoritmos que absorvem, conectam e transferem qualquer tipo de informação.

Para proteger a privacidade na sociedade da informação, onde os dados pessoais podem ser facilmente captados, cruzados, vendidos e até mesmo modificados, a Lei Geral de Proteção de Dados, normatizou técnicas para tornar os dados não identificáveis. Portanto, por meio das técnicas de anonimização, um dado pessoal perde a possibilidade de se associar, direta ou indireta, ao indivíduo.

Na sociedade da informação, e, diante de um Ordenamento Jurídico que protege os dados pessoais, as técnicas anonimização representam uma alternativa mais fácil para as empresas utilizarem dados pessoais de usuários. Por exemplo, quando uma empresa precisa realizar levantamentos e apurações estatísticas do seu quadro de empregados, para que estes não sejam identificados, as informações pessoais precisam passar por um processo de anonimização.[1]

[1] Para exemplificar: uma empresa, por meio de uma apuração estatística, precisa identificar o número de empregados que recebem licença doença, sob a justificativa de gravidez por ano. Se nessa empresa tiver apenas uma empregada do sexo feminino e se ela tiver pedido licença-maternidade no último ano, facilmente seus dados

Contudo, a problemática surge porque quando um dado é anonimizado ele deixa de ser pessoal e sai da esfera de proteção da Lei Geral de Proteção de Dados, ficando vulnerável a possíveis violações e a uma possível reidentificação.[2]

Diante desse contexto, o presente artigo desenvolve-se a fim buscar compreender como a sociedade da informação tem interferido na privacidade dos indivíduos, por meio dos tratamentos de dados pessoais. Para tanto, adentra-se no contexto da Lei Geral de Proteção de Dados, para asseverar acerca da anonimização e identificar se este é um meio viável para retirar as informações pessoais de determinados bancos de dados, bem como demonstrar se essa retirada realmente é capaz de resguardar a intimidade e privacidade do indivíduo, diante de uma futura reidentificação. Desse modo, parte-se do seguinte questionamento: as técnicas de anonimização de dados, de acordo com a LGPD, são capazes de proteger a privacidade e a intimidade do titular, a fim de evitar com que os dados sejam reidentificados?

A presente pesquisa utilizou uma metodologia de caráter qualitativa, por meio do método de abordagem dedutivo e da técnica de pesquisa bibliográfica e de análise legislativa, para traçar o panorama nacional da anonimização de dados, bem como para demonstrar, por meio de uma exposição bibliográfica, a realidade brasileira e as possíveis necessidades de mudanças práticas e de estudos acadêmicos sobre a temática em deslinde para o aprimoramento do Direito.

A pesquisa não tem o intuito de esgotar a temática ou apresentar uma solução prática à problemática apresentada, mas, sim, adentrar à discussão das possíveis repercussões

---

serão identificados. Tal identificação pode gerar informações discriminatórias, o que proibido pela legislação pertinente. Por isso, a LGPD institui a anonimização para tratar dados de natureza pessoal.

[2]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; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; [...] X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: 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;
de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; [...]. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, Presidente da República. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 20 ago. 2023.

jurídicas que podem surgir na esfera de proteção dos direitos da personalidade, como a privacidade, no que tange à proteção dos dados pessoais.

2 A SOCIEDADE DA INFORMAÇÃO E AS INTERFERÊNCIAS NOS DIREITOS DE PERSONALIDADE

De acordo com Tércio Sampaio Ferraz Júnior, a contemporaneidade passou por um intenso e rápido processo de transformação, o qual gerou mudanças no ambiente, nas máquinas, no homem e principalmente nos processos de informação. De acordo com o autor, a informação passou a ser tratada a partir de equipamentos técnicos que utilizam fórmulas matemáticas- algoritmos- para movimentar imagens, textos e falas, ou seja, qualquer tipo de informação (FERRAZ JÚNIOR, 2014).

Willis Santiago Guerra Filho entende que a sociedade da informação substituiu a sociedade pós-moderna e pós-industrial. Esse novo contexto social pressupõe a existência de um novo paradigma, o qual é representado pela informação (GUERRA FILHO, 2018). Esse novo paradigma é caracterizado pela tecnologia e pela sua alta penetrabilidade em todas as formas de interação humana, bem como pelo predomínio da lógica das redes e pela crescente convergência de tecnologias (CASTELLS, 2011).

Ao longo do seu desenvolvimento, a sociedade da informação, entre o final do século XX e início do século XXI, sofre um forte impacto, por meio do surgimento da internet. Tal inovação modificou a dinâmica das relações sociais e deu uma nova roupagem à abordagem da informação, unificando todas as formas de comunicação em um único meio- a internet (FLORÊNCIO, 2019).

Com o aumento da utilização da internet surge a *big data*, que é tecnologia desenvolvida para possibilitar uma navegação mais rápida e eficiente na imensidão dos dados produzidos diariamente em todo o mundo. De acordo com Viktor Mayer-Schonberger, a *big data* consiste em um gigantesco conjunto de dados digitais mantidos por grandes organizações e corporações, que são constantemente analisados por meio de algoritmos. Desse modo, essa tecnologia pode ser utilizada para identificar tendências de grupos de usuários e criar novas formas de valor, mas também para identificar e individualizar pessoa, a fim de prever decisões

relacionadas à publicidade e a oferta de produtos ou criar situações discriminatórias (MAYER-SCHÖNBERGER; CUKIER, 2013).

A *big data* tem uma conceituação ampla e ainda cientificamente imprecisa, mas não restam dúvidas de que consiste em um conjunto de dados capazes de trazer diversos benefícios para a sociedade, mas também alguns riscos para o indivíduo, advindos do uso inadequado dos dados pessoais, o que pode implicar em ameaças à privacidade e à intimidade, bem como aos demais direitos da personalidade (FLORÊNCIO, 2019)

A partir desse novo contexto social, pautado no fluxo de informações, pode-se inferir que as violações aos direitos da personalidade agravam-se. Devido ao desenvolvimento da inteligência artificial, por meio dos algoritmos, aumentam-se as formas de parametrizar dados e informações pessoais fornecidas de forma consciente ou inconsciente pelos indivíduos na internet.[3]

A proteção de dados busca tutelar a autodeterminação informativa, uma vez que não existe um direito fundamental à proteção de dados. A autodeterminação informativa foi criada para garantir a liberdade das pessoas em relação às suas informações pessoais, permitindo o livre desenvolvimento da personalidade por meio da possibilidade de dispor sobre o uso dos seus dados (SAWARIS, 2017).

O direito sobre as informações pessoais é uma liberdade positiva. É o direito de o indivíduo controlar sua informação. É a capacidade de exercer controle dos dados sociais, pouco importando se eles são públicos ou privados, de autodeterminar essas informações pessoais. A pessoa tem o direito de exercer o controle sobre o seu dado pessoal (SAWARIS, 2017).

---

[3] "Há uma década e meia atrás, era noticia que o Walmart estava usando a analise preditiva para antecipar as necessidades de estoque em face de eventos climáticos severos futuros. Atualmente, camapnhas de varejo (gerenciamentos de estoques),publicidade (mecanismos de recomendação on-line), seguros (melhor estratificação de risco), financeiro (estratégia de investimentos, dectecção de fraudes),imobiliárias, de entretenimento e política, rotineiramene adquirem, integram e anlisam grandes quantidades de dados pra mehorar se desempenho. O outro paradigma do big data é uma ameaça a proteção de dados pessoais,outrossim, pela característica da possibildiade de associação de dados. [...]. Por exemplo, saber o CEP de um individuo permite localizá-lo de 1 em 30.000 [...]. Por sua vez, a vinculação de um CEP a uma data de nascimento reduz o conjunto a aproximadamente 1 em 80. Já a inclusão do gênero e ano de nascimento nessa associação é capas de especificar um determinao individuo." FLORÊNCIO, Juliana Abrosio. Proteção de dados na cultura do algoritmo. Tese (doutorado em direito)- Pontifícia Universidade Católica de São Paulo. 320 f. São Paulo, 2019. Disponível em: https://sapientia.pucsp.br/bitstream/handle/22255/2/Juliana%20Abrusio%20Flor%C3%AAncio.pdf. Acesso em 17 dez. 2022.

Estefano Rodotà sustenta e defende que a proteção de dados busca corresponder verdadeiro direito fundamental, uma vez que em nome da expressão da liberdade e da dignidade humana está intrinsecamente ligada à impossibilidade de transformação dos seres humanos em objetos constantemente vigiados e, consequentemente, manipulados (2008).

Como expõe Ana Frazão, da exploração de dados pessoais decorrem problemas que não estão ligados apenas à privacidade ou à intimidade, uma vez que há vários desdobramentos da personalidade que entram em risco pela movimentação de dados, como a individualidade, autonomia e o livre desenvolvimento da personalidade, podendo inclusive alcançar a própria democracia (2019).

O Professor Fabiano Menke entende que, na sociedade da informação, há uma distinção entre sigilo da informação e a proteção de dados dos pessoais. De acordo com o professor, o problema não está apenas em impedir que um dado sobre a intimidade de determinada pessoa seja exposto, mas está no tratamento que a base de dados dará àquela informação e como isso ferirá a liberdade da pessoa, ou seja, como interferirá na sua autodeterminação informativa (2020).

Ademais, os ferramentais aplicados pelos algoritmos são capazes de cruzar dados, para identificar determinado tipo de comportamento e preferências a partir de informações fornecidas, fazendo surgir, assim, uma relação não espontânea de conhecimento. Desse modo, criam-se atalhos que permitem o controle para moldar o comportamento do indivíduo, fazendo com que uma decisão seja tomada por já saber antecipadamente o que o outro quer (MENKE, 2020).

Portanto, proteção de dados busca controlar também esse fluxo informacional não espontâneo, visando à manutenção de liberdade do indivíduo de manipular os seus dados, decidindo o que e como deseja compartilhar, uma vez a circulação de informações pessoais na internet e na *big data* é inevitável.

A autodeterminação informativa também é um dos fundamentos da Lei Geral de Proteção de Dados, estando presente nos seus artigos 1º e 2º[4]. Atualmente, por causa das formas

[4] "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. Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - **a autodeterminação informativa**; III - a liberdade de expressão, de informação, de

de tratamento dos dados pessoais, existe uma crise da autodeterminação informativa e uma crise do consentimento, de modo que se perde a noção dos próprios limites do consentimento, pois, muitas vezes, o consentimento é fornecido sem a total consciência (FLORÊNCIO, 2019).

Contudo, entende-se que, na contemporaneidade, a sociedade não flui sem dados, pois esses são elementos necessários de a existência e manutenção da sociedade da informação. Por isso, a necessidade da legislação tutelar tais dados. Dessa forma, busca-se inquirir como em que medida os dados pessoais podem ser tratados, bem como a definição dos limites desse tratamento (FLORÊNCIO, 2019).

3 O TRATAMENTO DE DADOS PESSOAIS NA LGPD: ANÁLISE DO PROCESSO DE ANONIMIZAÇÃO

A definição dos dados pessoais na Lei Geral de Proteção de Dados perpassa pela compreensão de suas duas perspectivas, quais sejam: a expansionista e a reducionista, as quais são a base da política regulatória da proteção de dados. A conceituação restrita compreende como dado pessoal a representação de fatos sobre uma pessoa identificada, ou seja, refere-se a alguém que se conhece e se individualiza em uma coletividade. A identificação ocorre por meio de elementos informativos, os quais mantém uma relação particular com o indivíduo. São exemplos: o nome, sobrenome, endereço, número do CPF (MACHADO; DONEDA, 2018).

A conceituação ampla entende que o alcance da informação vai além da pessoa natural. São dados que não estão relacionados apenas a identificadores diretos ou indiretos, mas têm o potencial de identificar uma pessoa a partir de um cruzamento ou uma suplementação de informações, mesmo que o agente responsável pelo tratamento não possa identificar. Este é o conceito utilizado pela legislação europeia e seguindo pela legislação brasileira. Portanto,

---

comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.” (grifou-se). BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 17 dez. 2022.

também é informação pessoal aquela relativa a uma pessoa identificável (MACHADO; DONEDA, 2018)[5] .

A partir do conceito de dados pessoais na legislação brasileira, é possível compreender o que não é um dado pessoal ou o que é um dado anônimo ou anonimizado. A Lei em comento, em seu artigo 5º, inciso XI, trata da anonimização de dados, conceituando-o os meios técnicos disponíveis para desassociar dados, direita ou indiretamente, a um indivíduo. [6] A LGPD não se aplica aos dados anônimos ou anonimizados, ficando estes, portanto, fora do seu âmbito de proteção.[7]

O dado anônimo também é caracterizado pela permanência e irreversibilidade, de modo que não pode voltar a ser associado a uma pessoa identificada ou identificável em nenhum momento ou circunstância.

De acordo com a LGPD, essa anonimização ocorre por meio de um tratamento, onde um controlador responsável terá que decidir o que será retirado, para ser anonimizado, e o que permanecerá na base de dados por ser uma informação referente a uma pessoa identificada. Por isso, depois que as informações entram na base de dados, terá que existir um

---

[5] "Por exemplo, se provedor de aplicação de internet, além de processar dados de tráfego, armazenar registros de endereço IP de terminais que acessaram seu sítio eletrônico, não obstante a ausência de identificação imediata, os usuários da internet podem ser identificados mediante requerimento judicial de acesso a registros de conexão e dados cadastrais armazenados pelos respectivos provedores de conexão. Esse é, a propósito, o entendimento adotado na União Europeia, tanto pelo Grupo de Trabalho de Proteção de Dados do Artigo 2923 como pelo Tribunal de Justiça da União Europeia (TJUE) nos casos C-70/10, Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), e C-582/14, Patrick Breyer v. Bundesrepublik Deutschland. No primeiro, a menção à caracterização do endereço IP como dado pessoal é feito em sede de obiter dictum, mas no Breyer case compõe de fato as razões de decidir (ratio decidendi) do julgado a qualificação do endereço IP (dinâmico) como "informação relativa a pessoa natural identificada ou identificável)." MACHADO, Diego; Doneda, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonanonimização de dados. **Revista dos Tribunais**, São Paulo, v.998,p.99-128. 2018. Disponível em: phttps://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados). Acesso em: 20 dez. 2022.

[6] "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; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento**;[...]; **XI - anonimização: 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**; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;[...]." (grifou-se)

[7] "Art. 12. 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."

procedimento legalmente fundamentado e documentado, para justificar o tratamento utilizado, seja este para anonimizar o dado ou não.[8]

Nesse contexto, Paulo Ohm levanta alguns questionamentos, aos quais se filia este artigo, a respeito do cumprimento das garantias da LGPD no momento da anonimização dos dados pessoais, observa-se: um indivíduo leigo em tecnologia estaria exposto a uma reidentificação? É possível proteger as informações pessoais apenas removendo os dados identificados ou identificáveis? Os dados podem ser considerados anônimos, uma vez que foram disponibilizados nas redes e tratados por uma terceira pessoa? Como o indivíduo leigo consegue saber que a anonimização dos seus dados pessoais realmente ocorreu? (2010).

Quando um dado, vinculado à identidade real de um indivíduo, é associado e uma identidade virtual acarreta a quebra do anonimato, pois abre a possibilidade de uma reidentificação. Por isso, deve-se refletir se essas informações são realmente retiradas e como foi o processo de retirada, uma vez que esta acontece por meio de terceiros, os quais já tiveram acesso aos dados pessoais (NEGRI; GIOVANINI, 2020).

Diante dessas possíveis falhas no tratamento para anonimizar dados pessoais, a proteção dessas informações passou a ser analisada com base em *accountability*[9], ou seja, a preocupação virou-se para como as bases ou as empresas tratam os dados e como prestam conta desse tratamento. Os fundamentos para proteção dos dados pessoais agora precisam estar dispostos em relatórios de impactos e auditorias de algoritmos. Tais cuidados precisam estar

---

[8] "Art. 18. **O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição**:I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º desta Lei. § 1º O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional. § 2º O titular pode opor-se a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.[...].§ **6º O responsável deverá informar, de maneira imediata, aos agentes de tratamento com os quais tenha realizado uso compartilhado de dados a correção, a eliminação, a anonimização ou o bloqueio dos dados, para que repitam idêntico procedimento, exceto nos casos em que esta comunicação seja comprovadamente impossível ou implique esforço desproporcional.** § 7º A portabilidade dos dados pessoais a que se refere o inciso V do caput deste artigo não inclui dados que já tenham sido anonimizados pelo controlador.§ 8º O direito a que se refere o § 1º deste artigo também poderá ser exercido perante os organismos de defesa do consumidor."

[9] Termo utilizado para se referir a um conjunto de práticas para prestar contas e responsabilizar os responsáveis por possíveis falhas.

documentados e fundamentados desde a concepção até o descarte das informações (FLORÊNCIO, 2019).

4 ANONIMIZAÇÃO DE DADOS PESSOAIS PARA PROTEÇÃO DOS DIREITOS DA PERSONALIDADE: RISCOS E OBJEÇÕES

As principais discussões críticas, a respeito da proteção dos dados pessoais no contexto da sociedade de informação, encontram-se na fragilidade legal do consentimento e na insuficiência das informações prestadas no momento da coleta de dados. Tal situação agrava-se quando se considera a falibilidade de anonimização desses dados, uma vez que este tratamento pode permitindo a reidentificação do titular, por meio de uma falha no processamento ou por meio de um cruzamento de informações de dados já anonimizados e não protegidos (DONEDA, 2016).

De acordo com Sólon Barocas e Helen Nissenbaum, o principal intuito dos processos de anonimozação é neutralizar as preocupações com a identificação dos titulares de dados, em nome da proteção de direitos da personalidade. Contudo, entendem os autores que essas técnicas apresentam falhas em relação à proteção da privacidade, por dois motivos, quais sejam: por não preocuparem com o direcionamento dos dados que serão considerados anônimos, ou seja, com o destino que será dado a informação, considerando-se que estará mais na esfera de proteção de dados; e por não informar de forma precisa ao titular dos dados as questões relacionadas ao consentimento desse tratamento. Portanto, os mecanismos de notificação e transparência ainda são insuficientes (2015).

Danilo Doneda e Diego Machado apontam ainda, como objeção à anonimização, para a proteção da privacidade do indivíduo, os riscos do cruzamento de dados, já anonimizados, conseguirem identificar o titular. Por meio da aplicação da teoria do mosaico, pode ocorrer a associação de dados neutros ou anonimizados de base com os dados neutros de uma outra base, e assim permitir que esses produzam dados sensíveis (2018).

Bruno Bioni afirma que não se deve considerar a anonimização um processo infalível, uma vez que as técnicas empregadas para anonimizar dados são meramente circunstanciais, além de dependerem de um processo objetivo e subjetivo, o qual é exercido pelo responsável

pelas técnicas de tratamento, ou seja, por uma terceira pessoa, estranha ao titular do dado (BIONI, 2020)

Ademais, apontam-se, pelo menos, seis fatores de risco no processo de anonimização que podem identificar um dado ou torná-lo identificável, quais sejam: o volume de dados; a natureza e cadeia de atividade de tratamento; o gerenciamento de identidades; e a segmentação, cláusulas contratuais e atualização contínua (RUBINSTEIN; HARTZOG, 2015).

Em relação ao volume de dados, entende-se que devido à grande quantidade de dados processados, a chance de uma reidentificação aumenta. Por isso, as bases que coletam tais informações devem sempre apresentar a técnica e os meios capazes de comprovar e assegurar, ao titular dos dados, que suas informações pessoais serão anonimizados de forma proporcional e razoável (BIONI, 2020).

Em relação à natureza dos dados, entende-se o valor de tais informações podem definir se futuramente elas podem ser reidentificadas. Desse modo, quanto mais importante a informação, maior a chance de uma possível reidentificação por parte de um escrutínio de terceiros. Por isso, as bases que coletam dados devem, antecipadamente, cientificar aos titulares a possibilidade de uma desanonimização. A cadeia de atividade de tratamento de dado também influencia nos riscos de uma reidentificação, pois quanto maior e mais complexa a cadeia de participantes no tratamento da anonimização, maiores serão os riscos; tanto porque se aumenta o volume das informações, como porque se aumenta o número de pessoas envolvidas (BIONI, 2020).

Em relação ao gerenciamento de identidades de segmentação, constata-se que, para que a proteção das informações durante o processo de anonimização ocorra de forma correta, importar controlar as pessoas que têm acesso a tais informações, pois a depender de quem acessa dados anonimizados ou pseudononimizados. poderá identificá-los. Bruno Bioni assevera que por cauda desse risco, deve-se segregar fisicamente e logicamente as bases de dados de uma organização. Os riscos também diminuem quando se reduz o número de atores envolvidos no processamento (2020).

As cláusulas contratuais presentes nos processos de coleta e compartilhamento de dados, deve, cada vez mais, especificar as possibilidade de reidentificação depois de uma anonimização, sendo também comum a existência de clausulas que proíbam as próprias partes de reverter o processo, clausulas que delimitem o papel da cada agente, bem como clausulas

que imponham a destruição dos dados quando concluída a atividade de tratamento (BIONI, 2020)

Por fim, Danilo Doneda e Diego Machado, acrescentam que ainda existem três consequências de uma reidentificação advindas de falhas em um processo de anonimização, quais sejam: a distinção, a possibilidade de ligação e a interferência (2018).

A distinção consiste na capacidade de isolar os registros que destacam e podem identificar uma pessoa em uma base de dados. A possibilidade de ligação é a capacidade que os sistemas de dados têm de estabelecer conexões entre dois registros diferentes relativos à mesma pessoa. A interferência consiste na redução do valor de um atributo a partir dos valores contidos em um conjunto de outros atributos quando possivelmente cruzados em bases de dados diferentes (MACHADO; DONEDA, 2018)

De acordo com os estudos aqui apresentados sobre as possíveis falhas, bem como de acordo com os riscos de uma reidentificação e suas consequências na identificação do indivíduo, resta consubstanciado que a anonimização de dados não é robusta, de modo que não é capaz de trazer uma tutela totalmente segura para a privacidade do individuo na sociedade da informação.

Contudo, resta analisar algumas questões referentes à pseudoanonimização. A título de conceituação, anonimização e pseudoanonimização não são expressões correlatas, uma vez que a primeira centra-se em técnicas para transformar um dado pessoal em um dado anônimo, de impossível identificação e individualização. Por sua vez, a pseudoanonimização é uma técnica de anonimização para disfarçar ou maquiar a identidade de uma informação, podendo substituir um atributo da personalidade por outro ou por meio de uma criptografia (MACHADO; DONEDA, 2018). [10]

[10] "A criptografia consiste na técnica da escrita secreta com o objetivo de esconder o significado de uma mesnagem, constituindo um mecanismo de confidencialidade em segurança computacional. São utilizados para cifrar informações, de modo que apenas o titular da informação ou quem tenha a chave criptgrafica, possa ter acesso ao seu conteúdo. A técnica consiste em garantir que apenas emissor e destinatário (as "pontas") da comunicação tenham acesso à chave criptográfica necessária para decifrar as informações enviadas. [...].Na linguagem da segurança computacional, a criptografia ponta a ponta é um protocolo criptográfico52 que reduz a superfície de ataque ao sistema diminuindo "a ameaça de pontos intermediários ou atacantes internos que operam o serviço e desfrutam de acesso privilegiado". Ou seja, no contexto das comunicações de dados que opera na internet, esse tipo de protocolo é concebido para resguardar a confidencialidade das informações trocadas entre emissor e destinatário não somente de sujeitos externos, como também do próprio intermediário, provedor de serviço de internet – e.g., WhatsApp e Facebook Messenger – que faz parte da arquitetura da rede e das comunicações em meio digital como hoje conhecemos." MACHADO, Diego; Doneda, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonanonimização de dados.

Portanto, a pseudoanonimização é um processo de disfarce de identidade que afeta principalmente os identificadores diretos; como nome, endereço residencial e eletrônico, número de telefone. Desse modo, para que uma informação pseudonimizada seja conectada ou titular dos dados, é preciso a existência de informações complementares. Aos dados pesudoanimizados são aplicados os ditames da LGPD, pois há uma preservação da identidade do titular, mesmo que de forma modulada (MACHADO; DONEDA, 2018).

As técnicas de pseudoanonimização também não estão livres dos riscos de uma identificação, inclusive Danilo Doneda questiona se essa forma de tratamento pode ser considerada uma técnica de anonimização, uma vez que é possível a identificação por parte do próprio titular e dos processadores do tratamento. O autor aponta que tendo em vista a força dos algoritmos é possível que esses dados possam ser descriptografados. Ademais, existe a possibilidade da existência de falhas relacionadas à extensão da chave criptográfica, bem como na segurança do gerenciamento dessa chave. (MACHADO; DONEDA, 2018)

Portanto, constata-se que as divergências na utilização da pseudoanonimização consistem no fato de ser considerada uma técnica de anonimização. Desse modo, um dado criptografado é um dado anonimizado; portanto, não protegido pela LGPD, o que levanta riscos para proteção desses dados pessoais que podem ser ligados aos aspectos da personalidade de um indivíduo.

5 CONSIDERAÇÕES FINAIS

Na sociedade da informação, os dados pessoais são supervalorizados, funcionando como uma mercadoria. Ocorre, que esse novo produto do mercado das informações, guarda valores que pertencem ao indivíduo e que, portanto, não podem ser renunciados, transmitidos ou alienados. Devido às características das informações que esses dados carregam, eles deveriam receber a mesma proteção jurídica que os direitos da personalidade recebem. Desse modo, entende-se que os dados pessoais que estão dispostos nas bases de processamentos

---

Revista dos Tribunais, São Paulo, v. 998, p.99-128. 2018. Disponível em: phttps://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados). Acesso em: 20 dez. 2022.

devem ser amplamente protegidos, tanto porque se referem às características que identificam o indivíduo, como porque também formam a própria personalidade do indivíduo.

Diante dos novos contornos instituídos pelos avanços tecnológicos, ver-se pungente a necessidade de o indivíduo gerir seus dados pessoais, determinando onde, como, com quem e porque deseja compartilhar. Ocorre que o poder de gerir e determinar as informações encontra-se, cada vez mais, limitado e ameaçado pelos ferramentais que movem os processos de inteligência artificial.

É evidente também a vulnerabilidade do indivíduo diante do conhecimento técnico das empresas e das bases que processam dados. Desse modo, o desequilíbrio informacional é mais um fator que coloca os direitos da personalidade dos indivíduos em perigo de uma constante ameaça.

Apesar dos esforços da Lei Geral de Proteção de Dados para resguardar e defender a autoderteminação informativa, a partir da análise doutrinária sobre o tratamento de dados, constatou-se que existem possibilidade viáveis de ocorrer reidentificação de um dado pessoal anonimizado. Esses riscos advêm tanto de falhas no processo de tratamento, como do crescente avanço tecnológico que torna os algoritmos, cada vez mais, capazes de cruzar dados e desvendar informações pessoais.

Portanto, conclui-se que, mesmo sendo uma questão contemporânea e ainda em desenvolvimento, os operadores do Direito devem acompanhar de perto as implicações práticas da aplicação legislativa, a fim de compreender as possíveis falhas e as consequências jurídicas. Os direitos ameaçados pelas falhas na anonimização de dados pessoais são de extrema relevância para o ordenamento jurídico e, principalmente, para indivíduo, uma vez que os direitos da personalidade são intrínsecos à pessoa humana e compõem a sua dignidade. Ferir a privacidade, em qualquer de suas esferas, desde a mais externa à mais intima pode trazer consequências irreversíveis para o indivíduo.

REFERÊNCIAS

BAROCAS, Solón; NISSENBAUM, Helen. **On Notice**: the trouble with notice and consent. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2567409. Acesso em: 21 dez. 2022.

BITTAR, Carlos Alberto. **Os direitos da personalidade**. 8.ed. São Paulo: Saraiva, 2014.

BIONI, Bruno. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos**, São Paulo, n. 53, p. 191-201, jan./mar.. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimiza%C3%A7%C3%A3o_e_dado.pdf?d=637250349860810398. Acesso em: 21 dez. 2022.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. *In:* **A Sociedade em rede**. São Paulo: Paz e Terra, 2000.

CUNHA, Tiago Barros; SIMÃO FILHO, Adalberto. A teoria dos círculos concêntricos e a preservação da privacidade humana no registro civil de pessoas naturais. *In*: V CONGRESSO BRASILEIRO DE DIREITO PROCESSO COLETIVO E CIDADANIA, 2017, Ribeirão Preto. Anais eletrônicos [...]. Ribeirão Preto: Universidade de Ribeirão Preto, 2017, p.265-282. Disponível em: https://revistas.unaerp.br/cbpcc/article/download/971/937/3931. Acesso em: 20 dez. 2022.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

FESTAS, David de Oliveira. **Do conteúdo patrimonial do direito à imagem**- contributo para o estudo do seu aproveitamento consentido e *inter vivos*. Coimbra: Coimbra Editora, 2009.

FERRAZ JUÚNIOR, Tércio Sampaio. Direito e realidade: a erosão do real jurídico pelo mundo virtual. *In*: FERRAZ JÚNIOR, Tércio Sampaio. **O direito entre o futuro e o passado**. São Paulo: Noeses, 2014.

FLORÊNCIO, Juliana Abrosio. **Proteção de dados na cultura do algoritmo**. 2019. 320 f. Tese (Doutorado em Direito)- Pontifícia Universidade Católica de São Paulo, São Paulo, 2019. Disponível em: https://sapientia.pucsp.br/bitstream/handle/22255/2/Juliana%20Abrusio%20Flor%C3%AAncio.pdf. Acesso em: 21 dez. 2022.

FRAZÃO, Ana. Objetivos e Alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA , Milena D. (coord.). **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito brasileiro**. 1. ed. São Paulo: Thomson Reuters Brasil, 2019b. p. 99-129.

GERMANO, Luiz Paulo Rosek. **O direito de resposta proporcional ao agravo**- o pleno exercício da liberdade de expressão no Estado Socioambiental e Democrático de Direito. 2010. 274 f. Tese (Programa de Pós-Graduação em Direito)- Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre, 2010. Disponível em: https://tede2.pucrs.br/tede2/bitstream/tede/4105/1/425134.pdf. Acesso em 20 dez. 2022.

GUERRA FILHO, Willis Santiago. **A autopoiese do direito na sociedade informacional**. Rio de Janeiro: Lúmen Juris, 2018.

MACHADO, Diego; Doneda, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonanonimização de dados. **Revista dos Tribunais**,

São Paulo, v. 998, p.99-128. 2018. Disponível em: phttps://www.researchgate.net/publication/330401277_Protecao_de_dados_pessoais_e_criptografia_tecnologias_criptograficas_entre_anonimizacao_e_pseudonimizacao_de_dados). Acesso em: 20 dez. 2022.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big Data**- La revolución de lós datos masivos. Madri: Turner, 2013.

MENKER, Fabiano. **A proteção de dados na teoria geral dos direitos da personalidade**. Palestra proferida na Pontifícia Universidade Católica do Rio Grande do Sul para o Programa de Pós-graduação em Direito. Disponível em: https://www.youtube.com/watch?v=lkb_z6CSf-I&t=3810s. Acesso em 20 dez. 2022.

NEGRI, Sérgio Marcos Carvalho de Ávila; GIOVANINI, Carolina Fiorini Ramos. Dados não pessoais: a retórica da anonimização no enfrentamento à covid-19 e *privicywashing*. **Internet Lab**, v.1, n.2, dez. 2020. Disponível em: https://revista.internetlab.org.br/dados-nao-pessoais-a-retorica-da-anonimizacao-no-enfrentamento-a-covid-19-e-o-privacywashing/. Acesso em 21 dez. 2022.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *In*: **UCLA Law Review**, [s. l.], v. 57, n. 6, p. 1701–1777, 2010. Disponível em: https://www.uclalawreview.org/pdf/57-6-3.pdf. Acesso em: 21 dez. 2022.

PEIXOTO, Erick Lucena Campos; EHRHARDT JÚNIOR, Marcos. Os desafios da compreensão do direito à privacidade no sistema jurídico brasileiro em face das novas tecnologias. In: EHRHARDT JÚNIOR, Marcos; LOBO, Fabíola Albuquerque (coord.). **Privacidade e sua compreensão no direito brasileiro**. Belo Horizonte: Fórum, 2019.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUBINSTEIN, Ira S. e HARTZOG, Woodrow. **Anonymization and risk**. New York University Public Law and Legal Theory Working Papers 530, 2015. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol91/iss2/18/. Acesso em: 20 dez. 2022.

SAWARIS, Adriana. **Tutela do Direito à reserva sobre a intimidade e a vida privada no regulamento Nº 2016/679 da União Europeia**. 2017. 138 f. Dissertação (Mestrado em Ciências Jurídico-Civilistas)- Universidade de Coimbra. Coimbra, 2017. Disponível em: https://eg.uc.pt/bitstream/10316/81104/1/Dissertac%CC%A7a%CC%83o%20Adriana%20S.. pdf. Acesso em: 20 dez. 2022.

TEPEDINO, Gustavo. **Temas em Direito Civil**. 3. ed. Rio de Janeiro: Renovar, 2004.