FACULDADE ARI DE SÁ

CURSO DE DIREITO

KARINE BRUNO DE SIQUEIRA ANDRADE

A RELAÇÃO ENTRE O DIREITO AO ESQUECIMENTO NA INTERNET E A LEI GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO BRASILEIRO

FORTALEZA

2022

KARINE BRUNO DE SIQUEIRA ANDRADE

A RELAÇÃO ENTRE O DIREITO AO ESQUECIMENTO NA INTERNET E A LEI GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO BRASILEIRO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Direito da Faculdade Ari de Sá.

Orientador: Prof. Alexsandro Machado Mourão

FORTALEZA

2022

Dados Internacionais de Catalogação na Publicação
Faculdade Ari de Sá
Gerada automaticamente mediante os dados fornecidos pelo(a) autor(a)

A554a Andrade, Karine Bruno de Siqueira .

A RELAÇÃO ENTRE O DIREITO AO ESQUECIMENTO NA INTERNET E A LEI GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO BRASILEIRO / Karine Bruno de Siqueira Andrade. – 2022.

48 f.

Trabalho de Conclusão de Curso – Faculdade Ari de Sá, Curso de Direito, Fortaleza, 2022.

Orientação: Prof. Dr. Alexsandro Machado Mourão.

1. Direito ao apagamento. 2. Governança da internet. 3. Esquecimento. 4. Proteção de dados. I. Título.

CDD 340

KARINE BRUNO DE SIQUEIRA ANDRADE

A RELAÇÃO ENTRE O DIREITO AO ESQUECIMENTO NA INTERNET E A LEI GERAL DE PROTEÇÃO DE DADOS NO CONTEXTO BRASILEIRO

Trabalho de Conclusão de Curso apresentado como requisito parcial à obtenção do título de Bacharel em Direito da Faculdade Ari de Sá.

Orientador: Prof. Alexsandro Machado Mourão

Aprovada em: ___/___/___

BANCA EXAMINADORA

_____
Prof. Dr. Alexsandro Machado Mourão
Faculdade Ari de Sá

_____
Prof. Dr. Maria Alessandra Brasileiro de Oliveira
Faculdade Ari de Sá

_____
Prof. Me. Deubia Gabriela Oliveira Cavalcanti Mourão
Universidade de Fortaleza

AGRADECIMENTOS

A Deus, pela presença irrefutável em minha vida e por me ajudar a ultrapassar todos os obstáculos encontrados ao longo do curso.

Aos meus pais e irmãos, que me incentivaram nos momentos difíceis e compreenderam a minha ausência enquanto eu me dedicava à realização deste trabalho.

Aos professores, especialmente ao meu orientador Alexandro Mourão, pelas correções e ensinamentos —que me permitiram apresentar um melhor desempenho no meu processo de formação profissional.

“Sonhos determinam o que você quer.
Ação determina o que você conquista.”

Aldo Novak

RESUMO

A presente pesquisa busca investigar: quais os limites do exercício do esquecer frente ao direito à informação. Para resolver tal problemática, essa pesquisa terá como objetivo geral apontar as quais os limites normativos para o exercício do esquecimento no ordenamento jurídico interno assim como a LGPD; Verificou-se que o conflito de interesse acontece quando alguém está acessando, recebendo ou divulgando esses fatos no exercício de seu direito legal à liberdade de expressão e outra pessoa de quem a informação diz respeito no exercício de outro direito legal, tentando ocultá-los para sempre que é a essência do esquecer, um aspecto da promulgação da proteção de dados pessoais no sistema jurídico.

Palavras-Chave: Proteção de dados. Governança da internet. Direito de apagamento Mídia social.

ABSTRACT

This research seeks to investigate: what are the limits of the exercise of forgetting in the face of the right to information? To solve this problem, this research will have the general objective of pointing out the normative limits for the exercise of forgetting in the internal legal system, relation in LGPD; It was verified that the conflict of interest happens when someone is accessing, receiving or disclosing these facts in the exercise of their legal right to freedom of expression and another person to whom the information concerns in the exercise of another legal right, trying to hide them for whenever it is the essence of forgetting, an aspect of the enactment of personal data protection in the legal system.

Keywords: Data protection. Internet Governance. Right of Removal Social Media.

SUMÁRIO

1 INTRODUÇÃO

A Constituição Federal da República Brasileira (CFRB/88) é reconhecida por trazer um rol de direitos e garantias fundamentais que visam tutelar os principais valores que compõe a sociedade. Assim, dentre os chamados direitos fundamentais, essa dispõe um grupo específico que visa tutelar a integridade física e psíquica da pessoa humana.

Nesse sentido, o chamado esquecimento, ainda que não tenha sido expresso na Constituição pode ser verificado a partir da técnica de interpretação do art. 5º, XX, que tutela o direito à vida privada, intimidade e honra. Já no âmbito normativo infraconstitucional, esse valor recebe guarita, dentre outros documentos, no Código Civil de 2002 (CC/02), em seu art. 21 que estabelece que a vida privada da pessoa natural é inviolável. Ademais, a chamada Lei Geral de Proteção de Dados Pessoais, Lei nº 13.709, de 14 de agosto de 2018, traz novas delimitações normativas para a proteção dos dados.

Tal como os direitos individuais exemplificados acima, o direito à informação e a publicidade também vão receber tratamento específico na Carta Magna tamanha a importância dessa categoria para as relações sociais, que essa o acesso a informação será um direito fundamental. Tal como, o constituinte originário estabelece que é um dever daquele que faz as vezes do Estado dar publicidade aos seus atos.

Todavia, quando do desenvolvimento das relações sociais, aparentes situações de conflitos podem ocorrer fazendo com esses princípios venham a ser vistos como em situação de colisão. Assim, o chamado esquecer vem sendo questionado sendo levado a demanda processuais em face de eventuais abusos do exercício do direito à informação.

Nesse sentido, essa pesquisa busca verificar quais os limites do exercício do esquecer frente ao direito à informação. Para resolver tal problemática, parte-se do pressuposto que é preciso considerar que mesmo em uma sociedade informacional é necessário garantir o direito de ser esquecido com vistas à proteção da dignidade da pessoa humana, é salutar que, em algumas situações, seja preservado o interesse público que decorre da preservação da informação, posto que a livre circulação de ideias é o corolário do funcionamento das democracias. Ademais, que

a colisão de direitos fundamentais é aparente, visto que, os princípios possuem o mesmo peso normativo.

Deste modo, A pesquisa terá como objetivo geral apontar quais os limites normativos para o exercício do esquecimento no ordenamento jurídico interno, relacionando à Lei Geral de Proteção de Dados; buscar compreender a construção epistemológica e jurídica do esquecimento; analisar os impactos da superexposição na sociedade, relevando a importância da legislação protetiva de dados e informações; descrever o entender dos Tribunais Superiores brasileiros quanto ao enfrentamento do Direito ao Esquecimento

Quando a metodologia, essa pesquisa se desenvolvido através de um uma pesquisa exploratória realizada a partir de uma revisão bibliográfica que, após inclusão utilização dos descritores, examinará o material (artigos científicos, texto normativo, decisões jurisprudenciais) pesquisado através da abordagem qualitativa. Quanto ao método, optou-se pela aplicação do dedutivo.

A demanda de julgados contendo a matéria do direito ao esquecimento vem aumentando nos tribunais, fazendo com que os estudos direcionados para compreensão jurídica desse princípio seja relevante. Quanto a relevância social, cumpre lembrar que o exercício desse direito também esteve correlato ao período dos pós Ditadura Militar e são fundamentais reflexões críticas profundas sobre seus impactos. Por fim, as pesquisas científicas que se debruçam sobre esse objeto ainda são escassas, o que faz esse objeto relevante. Assim, essa pesquisa se faz justificável.

2 A SOCIEDADE DA INFORMAÇÃO E O DESAFIO DA SUPEREXPOSIÇÃO

Pode-se dizer que a internet se tornou indispensável no cotidiano, o que devido a comunicação global e maior transparência, uma simples pesquisa no buscador “Google” podem ser listadas as informações pessoais de milhares de pessoas se tornando um verdadeiro empecilho para privacidade individual. Uma vez realizada a indexação desses dados, promove o esquecimento necessário para proteção da personalidade individual em sociedade.

2.1 COMPREENSÃO AXIOLÓGICA DO ESQUECIMENTO

O ato de esquecer dá aos indivíduos o direito de ter suas informações privadas removidas da Internet, sites ou quaisquer outras plataformas públicas em circunstâncias especiais. O esquecer também é chamado de 'Direito ao apagamento'. O 'esquecer' foi estabelecido pela União Europeia em maio de 2022.

Consalter (2017) usa a interessante formulação de um 'direito', ou melhor, um 'legítimo interesse de esquecer e ser esquecido'. Assim, embora possa ser concebido como um direito, também pode ser visto como um valor ou interesse digno de proteção ou um objetivo político a ser alcançado por algum meio ou outro, seja por meio de lei ou por meio de outros mecanismos regulatórios.

Menciona não apenas a relevância de ser esquecido, mas também de fazer esquecer. Desta forma, existe a visualização do direito ao esquecimento utilizando a perspectiva da primeira pessoa.

Para Consalter (2017), também é importante poder esquecer o seu próprio passado. Isso não tem um significado primordialmente psicológico (uma vez que o esquecimento é geralmente apresentado como uma função natural do cérebro humano, que não precisa de reforço como tal, mas tem implicações sociais e legais: o direito de não ser confrontado com seu passado (que se mesmo esqueceu ou gostaria de esquecer). Um termo guarda-chuva conveniente para ambos os elementos – ser esquecido e esquecer – é esquecimento ou, o conceito é tipicamente denotado em francês como o droit à l'oubli (BUCAR, 2019, p. 30).

Consalter (2017) descreve ainda o conceito como o interesse em ser esquecido e em fazer-se esquecer, fazendo assim uma distinção entre o efeito desejado (ser esquecido) e os meios possíveis (garantir que os outros esqueçam). O

primeiro parece mais associado a um direito negativo (o dever dos outros de se abster de lembrar o passado de alguém), enquanto o último está mais associado a um direito subjetivo, destacando a liberdade ou poder do indivíduo de controlar ativamente seu passado. Este último também é apresentado na forma como formula sua proposta de direito de exclusão, ou seja, que um indivíduo deve ter o direito de excluir informações sobre ela que sejam detidas por outros.

No geral, embora os detalhes das conceituações dos autores variem, parece haver um denominador comum considerável na literatura sobre um direito ao esquecimento, ou seja, que alguém tem um interesse significativo (possivelmente para ser protegido na forma de um direito legal). em não ser confrontada por outros com elementos de seu passado, mais em particular com dados do passado (mais remoto) que não são relevantes para decisões ou visões atuais sobre ela.

A ausência de um regulamento de proteção de dados que restringia o direito fundamental de excluir dados privados inúteis e difamatórios do espaço online, o esquecer atraiu atenção significativa. Assim, neste caso fica claro que é preciso da hora para considerar o esquecer como um Direito fundamental.

Sendo dois direitos fundamentais distintos, o estado coexistente do esquecimento e da liberdade de expressão já foi confirmado pelas autoridades competentes através da ponderação em situações em que colidem. Schreiber (2022) concentra-se como pressupostos históricos nas apreensões de ponderação sendo relativas aos dados de condenações criminais, considerando a decisão do Google e o Regulamento Geral de Proteção de Dados (GDPR) principalmente para análise.

Os princípios contemporâneos na ponderação dos direitos dos dados de condenação criminal foram identificados por Schreiber (2022) que aponta que muito ainda que precisa ser aprimorado cuidadosamente no futuro para contemplar a necessidade de dados e defender o direito de ser esquecido em casos de indivíduos condenados com histórico criminais extensos, de tal forma que seja agradável e justo a todos.

Antes de saltar para equilibrar os conflitos entre os dois direitos, pouca apreensão em relação à sua relação é necessária para melhor compreender suas posições em uma democracia. Schreiber (2022) estabeleceu uma pré-condição para o funcionamento adequado de uma democracia no complexo mundo de hoje, que é proteger dois direitos específicos, a saber, o direito de acesso à informação e o direito à privacidade.

Fortalecido pelo artigo 19 da Declaração Universal dos Direitos Humanos (DUDH) e Pacto Internacional sobre os Direitos Civis e Políticos (PIDCP), novamente, o artigo 10 da Carta dos Direitos Fundamentais da UE (a Carta) e a Convenção Europeia sobre Direitos Humanos (CEDH), o direito à liberdade de expressão ou o direito de buscar ou acessar a informação em todos os documentos públicos recebeu um forte reconhecimento como um direito humano.

Para Schreiber (2021), o direito à informação do governo é visto como um elemento de uma sociedade democrática, pois é respaldado pelo consentimento dos cidadãos que desejam ser informados sobre as atividades do governo e, assim, colocar o controle e o equilíbrio para combater os abusos, fazer valer os direitos e assim por diante.

Além disso, a privacidade é entendida como o cerne da autonomia individual, responsável pelo desenvolvimento da dignidade individual. Artigo 12 da DUDH, 17 do PIDCP, 7 da Carta e art.8 da CEDH, estabelecem um direito de privacidade amplo e forte, proibindo a interferência ilegal na vida, reputação e honra privada e familiar de qualquer pessoa. O direito de proteção de dados pessoais ocupa uma parcela menor no amplo âmbito da lei de privacidade que visa proteger o titular do direito de interferências de terceiros (pessoas físicas ou jurídicas).(RIBEIRO,2016)

Além disso, a adequada salvaguarda dos dados pessoais está ligada à confiança e à confiança do cidadão e é por isso que o Regulamento Geral de Proteção de Dados (RGPD) (Art. 1 (2)) protege os direitos fundamentais das pessoas singulares, por exemplo, o esquecimento (Art. 17) relacionado com a proteção de dados pessoais. Isso indica que ambos os direitos são distintos e responsáveis por proteger interesses distintos. Com a entrada em vigor do Tratado de Lisboa, ambos os direitos atingiram o estatuto de direitos humanos fundamentais no ordenamento jurídico europeu.(WACHOWICZ,2020)

Embora suas posições sejam distintas e diferentes, elas podem colidir ou se sobrepor em alguns pontos específicos onde o acesso à informação pode ser legalmente restrito se os registros públicos incluírem certos dados pessoais como assuntos relacionados ao acesso não autorizado a registros criminais, jornalistas em busca de histórias, indivíduos solicitando acesso a registros públicos ou registros de programas sociais, empresas em busca de dados comerciais, acadêmicos em busca de dados de pesquisa e assim por diante.

Em última análise, Schreiber (2022) aponta que o direito de acesso à

informação e o direito à proteção de dados pessoais se sobrepõem em certa medida. Nesse ponto, o balanceamento torna-se inevitável, sustentando a verdade e suprimindo a culpa, pois não se deve esquecer o que a legislação pretendia proteger.

Voltando ao equilíbrio, Schreiber (2022) considera que a grande questão é se o esquecimento pode ser considerado um dos fundamentos restritivos do direito à liberdade de expressão, uma vez que ambos são direitos fundamentais previstos no art. respectivamente da Carta dos Direitos Fundamentais da União Europeia e têm sido vistas como se sobrepondo.

O fenômeno sugere que não há uma prática padronizada de estabelecer uma norma definitiva, uma vez que ela deve ser equilibrada com os direitos concorrentes. Em outras palavras, os acessos esperam ser bem-sucedidos no acesso a qualquer informação publicamente disponível, mas podem ser autorizados a fazê-lo enquanto protegem a privacidade.

Desde a origem do esquecimento, a questão primordial que se tem visto é o esforço de equilíbrio entre este direito à privacidade e outros direitos públicos, uma vez que o direito primário de proteção de dados pessoais não é um direito incondicional, mas sua função societária também tem a ter em conta de acordo com as normas do princípio da proporcionalidade e do interesse comum da União para cumprir os seus objetivos de proteção dos direitos e liberdades dos outros.

Após o reconhecimento do General Data Protection Regulation (GDPR), denominado Regulamento Geral sobre a Proteção de Dados, o direito ao esquecimento encontrou sua base sólida, na qual o direito público à liberdade de expressão foi prescrito como uma das razões para limitar o ato de esquecer. (GDPR, Art. 17, 3º, alinea a). Assim, o equilíbrio é inevitável.

Para Schreiber (2022), os mecanismos de equilíbrio entre os direitos de privacidade e publicidade, mais relevante, entre o direito ao esquecimento e o direito à liberdade de expressão deram origem a esses princípios de equilíbrio relevantes, que são responsáveis ao determinar se o esquecer seria permitido ou não. Nesse sentido, compreender o desenvolvimento gradual de questões conflitantes entre esses dois direitos é de extrema importância para compreender os pontos de equilíbrio derivados de diferentes visões do direito da União.

O escopo deste artigo limita-se a equilibrar as apreensões entre o direito à liberdade de expressão e o direito ao esquecimento e limitou a discussão dentro dos

dados de condenações penais gastas. Para Schreiber (2022), o termo dados de condenação criminal despendida refere-se essencialmente àqueles dados que se referem aos titulares dos dados que já cumpriram suas sentenças ao atingir o prazo estabelecido e os dados foram apagados seguindo o procedimento legal, a saber, sob o English Rehabilitation of Offender's Act 1974, ou registros de ofensas triviais não habituais, ou qualquer ofensa que aconteceu em um momento de loucura que não pertença ao caráter do ofensor que aconteceu uma vez e há muito tempo. Assim, as dívidas são pagas à sociedade por suas gafes.

Além disso, a tarefa de balanceamento é realizada principalmente com base nas diferentes disposições do GDPR. Por último, mas não menos importante, espera-se que o leitor possua o conhecimento mínimo necessário para construir os conceitos básicos do direito à liberdade de expressão e do direito ao esquecimento.

2.2 LIMITES CONTEMPORÂNEOS DO ESQUECIMENTO

Por causa da Internet, a informação é obtida de forma tão voluntária que permanece on-line permanentemente, facilita uma calúnia permanente sobre a reputação de alguém que torna a ocultação dos erros do passado um evento implausível, uma vez que uma quantidade indefinida de dados pode ser obtida inserindo o nome do titular dos dados em um mecanismo de busca.

O fenômeno do esquecimento é hoje uma anomalia já que os dados pessoais estão a apenas um clique de distância na pesquisa do Google. O problema ocorre quando determinada informação traz um impacto adverso na vida de alguém ao trazer fatos à tona. Os fatos podem fazer parte de mídias sociais, notícias, arquivos ou qualquer outro site direcionado por meio de hiperlinks.

O conflito de interesse acontece quando alguém está acessando, recebendo ou divulgando esses fatos no exercício de seu direito legal à liberdade de expressão e outra pessoa de quem a informação diz respeito, no exercício de outro direito legal, tentando ocultá-los para sempre que é a essência do direito ao esquecimento, um aspecto da promulgação da proteção de dados pessoais no sistema jurídico.

Stalling e Brown (2022) delimitam que o esquecer pode fornecer proteções importantes para a privacidade e pode cumprir um papel importante na promoção da agência e da autonomia. Atores estatais e não estatais têm poderes de longo alcance quando se trata de informações pessoais online e identidade de indivíduos.

Permitir que os indivíduos tenham alguma propriedade de suas informações pessoais lhes dá algum controle de suas identidades digitais.

Na era digital, a coleta de dados e a memorização automatizada tornaram-se difundidas e podem continuar afetando a vida de uma pessoa por muito tempo: Um erro do passado, uma negligência involuntária, uma manifestação emocional repentina podem surgir inesperadamente muito depois que alguém e outros já se esqueceram continuando assim a estragar a reputação de uma pessoa.

Com o exercício do “right to be forgotten” (RTBF), denominado em inglês direito a ser esquecido, é antagônico a memória histórica, pois impede a atualização ou exclusão de fatos e acontecimentos que, mesmo verdadeiros, o sujeito gostaria de ocultar. Não obstante, o esquecimento e a memória partilham os mesmos objetivos, nomeadamente a representação correta e verdadeira de factos e pessoas e a proteção da identidade e dignidade pessoal (Bianca, 2019).

A luta entre esquecimento e memória, da qual surge o RTBF, também foi influenciada por mudanças nos conceitos de tempo e dados na era totalmente digital. A informação agora é armazenada por um período indefinido, mas encontrada e disseminada instantaneamente. É como se percebêssemos o tempo em duas formas ao mesmo tempo – como um instante e como uma eternidade (BUCAR, 2019).

As novas preocupações estão surgindo rapidamente; novas demandas decorrentes dessa questão de pegada digital de longa duração exigem a implementação de novos direitos, entre os quais o direito à identidade digital, entendido como o direito do indivíduo de obter a retificação, contextualização, atualização e, em alguns casos, até mesmo desindexação e cancelamento de dados pessoais da Internet, a fim de garantir uma representação confiável de sua própria identidade. Portanto, a ideia por trás do esquecimento é fornecer uma reivindicação legal para que todos tenham uma representação real de sua identidade pessoal, obtendo o apagamento de seus rastros digitais anteriores deixados online (BUCCAR, 2019).

O esquecimento está relacionado a conceitos como dignidade, reputação e privacidade, fazendo parte do direito da personalidade, entendido como a proteção da integridade moral e jurídica de uma pessoa (BUCCAR, 2019) em situações em que certas informações tenham sido perdidas. a maior parte da sua significância, continuando a ter um impacto negativo na privacidade da pessoa envolvida

(CONSALTER, 2016).

É composto por vários direitos, como mudar de opinião sobre dados anteriormente divulgados, ter dados pessoais excluídos quando não mais for necessário mantê-los, não ser lembrado permanentemente do passado e não permitir que prejudique desproporcionalmente o futuro, e obter a desreferenciação de dados, combatendo o poder dos motores de busca na Internet (CONSALTER, 2016).

Por suas características multifacetadas, o termo direito ao esquecimento pode ser percebido como ambíguo e enganoso, sendo normalmente utilizado para tratar de diferentes situações que às vezes se sobrepõem e podem ser confundidas umas com as outras, como o fato de que um evento histórico deve deixar de ser revitalizado devido ao tempo decorrido desde a sua ocorrência – que deveria ser mais apropriadamente definido como direito ao esquecimento – ou a reivindicação de um indivíduo de ter certos dados apagados para que terceiros não possam mais rastreá-los

Com referência a este último significado, uma distinção adicional deve ser feita entre a reivindicação de privacidade dignitária (ou seja, o direito de ser respeitado na própria vida privada e familiar, lar e comunicações. De fato, o direito à proteção de dados incorpora elementos distintos dos componentes do esquecimento como o direito de retirar o consentimento previamente dado para processar dados; o direito de se opor ao processamento de dados; o dever de apagar ou anonimizar os dados uma vez alcançada a finalidade e o direito de apagar os dados quando o seu tratamento não cumprir os requisitos de proteção (CONSALTER, 2016).

Ao longo dos anos, o conflito entre privacidade e liberdade de expressão tem sido fonte de inúmeras batalhas jurídicas, nas quais os tribunais europeus geralmente se esforçam para alcançar um equilíbrio justo e cuidadoso entre esses dois direitos concorrentes. De um ponto de vista europeu o direito ao esquecimento é uma resposta ao eco da manutenção de registros totalitários, uma afirmação contra governos e, com o passar do tempo, entidades não governamentais (CONSALTER, 2016).

No entanto, essas preocupações provavelmente devem ser desmascaradas: embora tenham sido levantadas críticas à atitude imperialista da lei de proteção de dados, reivindicações de soberania digital estão surgindo também em regimes iliberais em todo o mundo, colocando em risco a proteção dos direitos fundamentais

online; para contrabalançar essa atitude, o desenvolvimento de marcos jurídicos transnacionais entre regimes democráticos parece ser uma medida necessária

Assim, a maioria das informações pessoais on-line não tem relação com considerações de interesse público e tem muito mais valor intrínseco para o indivíduo do que para a sociedade em geral. Os atuais desenvolvimentos jurisprudenciais e legislativos a esse respeito têm sido sensíveis a isso, reconhecendo a diferença entre o que é de valor para um indivíduo, o que é de interesse público e o que é de interesse público.

Para Stalling e Brown (2022), havia preocupações de que um direito excessivamente expansivo de ser esquecido levaria à censura da Internet porque os titulares dos dados podem forçar os mecanismos de pesquisa ou sites a apagar dados pessoais, o que pode reescrever a história). Em alguns casos, é permitido que os indivíduos não sejam definidos indefinidamente por seu passado.

Existem benefícios legítimos que acompanham o direito ao esquecimento; no entanto, também existem riscos associados ao direito, em particular no que diz respeito à aplicação de direitos e ao efeito adverso que isso pode ter sobre o direito à liberdade de expressão e o ato de esquecer. Assim, riscos em conferir tal poder decisório a uma entidade privada, principalmente pela necessidade de equilibrar direitos concorrentes, exercício tradicionalmente reservado aos tribunais.

É conceituado por Schreiber (2022) que o direito ao esquecimento é o direito de se opor a uma representação equivocada da pessoa humana perante a sociedade pela desatualização dos fatos que a trajetória daquela mesma pessoa percorreu em vida

Em contraste, no decorrer dos anos, a internet impulsionou para superexposição de informações, o que deu origem LGPD, por exemplo, levando a pensar sobre até que ponto seria razoável restringir a divulgação destas informações na internet sem prejudicar o avanço tecnológico (MORATO; CICCO, 2015).

Assim, é fundamental a busca para os comportamentos que busquem conciliar estas duas realidades (proteção de dados pessoais versus desenvolvimento tecnológico) é relevante tendo em vista que limitar excessivamente a divulgação de dados pessoais e permitir que o avanço tecnológico continue sem impor a ele nenhum limite e regulamentação parecem não ser razoáveis.

O avanço tecnológico, além de trazer vários benefícios para a sociedade, também trouxe preocupações no que se refere à inserção de dados pessoais na

internet quando advir no futuro o desejo de indisponibilizá-los, além das novas formas como estas informações são empregadas, acenderam o debate sobre o direito de proteger a privacidade dos usuários, além dos seus dados pessoais.

Nesse contexto, pode-se compreender o direito ao esquecimento como a pretensão de recobrar o domínio sobre os fatos pessoais depois que eles foram legitimamente divulgados. Consiste, substancialmente, em uma reintegração do poder de dispor, depois de sua perda determinada pela publicação da notícia pessoal (BUCAR, 2019).

Embora a terminologia do direito ao esquecimento possa induzir ao entendimento diverso, o ato de esquecer não impõe uma obrigação de esquecer. Não se trata de exigir que outros sujeitos esqueçam os fatos que nos concernem, mas apenas de impedir a divulgação de informações pessoais quando não haja mais interesse social no conhecimento de determinado fato (BUCAR, 2019).

O que se protege é o livre desenvolvimento da personalidade que seria afetado pela difusão de fatos passados e não pela recordação não exteriorizada. Não existe, portanto, dever de esquecer, mas sim dever de não divulgar fatos passados que possam ocasionar dano ao livre desenvolvimento do projeto vital dos indivíduos (BUCAR, 2019).

Com o advento da internet, este esquecer clássico, de perfil bem definido, sofre profundas transformações, passando a abranger uma vasta gama de possibilidades. No âmbito virtual, qualquer evento é perpetuado com amplo acesso de usuarios, o que era diferente pelas antigas mídias como as revistas e programas televisivos (CONSALTER, 2017). Independentemente se a informação é verossímil ou não, estará na rede.

ntende que é possível fazer uso dos próprios recursos da tecnologia da informação para, de tempos em tempos, suprimir dados, imagens, enfim, arquivos diversos da rede até que estes, com o passar do tempo, desapareçam. A autora entende que, para tanto, a solução mais eficaz está na arquitetura da rede, disseminando ferramentas tecnológicas que subordinam a acessibilidade de determinado dado a um lapso temporal.

No entanto, é possível que alguém tenha feito uma cópia do conteúdo para o computador pessoal e a disponibilizado em outros locais. Um exemplo bastante simples é um amigo que pode ter sido marcado na rede social há muitos anos. Neste caso, independentemente da vontade do principal interessado, ou seja, a

pessoa a que as informações veiculadas se referem, não é possível exercer controle sobre as cópias existentes sob a responsabilidade de terceiros, de maneira que referidas informações podem seguir por distintos caminhos.

Outra questão que enseja preocupação é a falta de consenso que ainda paira sobre ser ou não esquecimento um direito da personalidade. Consalter (2016) entende que o primeiro passo a ser dado quando se trata do ato de esquecer é que os ordenamentos jurídicos o concebam com um direito fundamental; que o indivíduo possa exercê-lo se tiver interesse e se estiverem presentes os pressupostos jurídicos necessários para tanto.

Sob a ótica de Schreiber (2014) sobre o avanço tecnológico e a velocidade como a informação se propaga na internet. Assim, o citado autor leciona que:

> A internet não esquece. Ao contrário dos jornais e revistas de outrora, cujas edições antigas se perdiam no tempo, sujeitas ao desgaste de seu suporte físico, as informações que circulam na rede ali permanecem indefinidamente. Pior: dados pretéritos vêm a tona com a mesma clareza dos dados mais recentes, criando um delicado conflito no campo do direito. De um lado, é certo que o público tem o direito de relembrar fatos antigos. De outro, embora ninguém tenha o direito de apagar os fatos deve-se evitar que uma pessoa seja perseguida, ao longo de toda sua vida, por um acontecimento pretérito (SCHREIBER, 2014, p. 170).

O supracitado autor ainda reconhece o esquecimento e a liberdade de informação como direitos de matriz constitucional e propõe que a ponderação seja aplicada. Para esse é fundamental valer-se de parâmetros que torne possíveis verificar com os princípios predomina no caso concreto. Trata-se assim da técnica de ponderação de princípios para a resolução do caso concreto.

A técnica baseia-se em

De fato, o esquecimento tem sido aplicado no direito brasileiro há muito tempo, fazendo uso, principalmente, da analogia. Como lembra Morato (2015), a apreciação de casos com vistas a compreender o esquecer. Muitos são os casos veiculados na mídia que são constantemente retratados que foram objetos de enfretamento nos tribunais quanto ao direito de esquecimento.

Recentemente, quando do enfrentamento da matéria, o STF, o Ministro Fachin reconheceu que a Constituição Brasileira recepciona um direito ao esquecimento, mas esse deve ser examinado sempre analisando as especificidades do caso concreto. Ainda que o pedido do pleito do Recurso 1.010.606/RJ tenha sido negado, o julgado foi fundamental para a discussão da matéria no ordenamento jurídico interno, visto que, buscava discutir o limite da Rede Globo em transmitir o caso Aída Curi.

3 A EFICÁCIA NO COMBATE DA SUPEREXPOSIÇÃO PARA EMPRESAS E PESSOAS FÍSICAS

A segurança e a privacidade dos dados são parte da tecnologia da informação que lida com a capacidade de uma organização ou indivíduo de determinar os dados em um sistema que pode ser compartilhado com terceiros (STALLINGS, 2015). Além disso, ajuda as organizações a proteger os dados no escritório e nas mãos dos funcionários, reduz as vulnerabilidades que os hackers podem explorar as informações.

3.1 A IDENTIFICAÇÃO E PROTEÇÃO DE DADOS EM EMPRESAS

Stalling e Brown (2022) afirma que, embora a segurança de dados e a privacidade de dados pareçam semelhantes, são bastante diferentes uma da outra. Para esses, a segurança de dados trata da proteção de dados contra criminosos cibernéticos, enquanto a privacidade de dados trata de como organizações de dados ou indivíduos coletam, armazenam e usam legalmente os dados.

Ainda para Stalling (2015), a segurança de dados inclui um conjunto de padrões e diferentes salvaguardas e medidas que uma organização está tomando para evitar que terceiros acessem não autorizados a dados digitais, ou qualquer alteração, exclusão ou divulgação intencional ou não intencional de dados. e concentra na proteção de dados contra-ataques maliciosos e evita a exploração de dados roubados (violação de dados ou ciberataque). Inclui controle de acesso, criptografia, segurança de rede, entre tantos outros.

Leciona Rodatà (2018) que o objetivo da proteção de dados pessoais não é apenas proteger os dados pessoais, mas proteger os direitos e liberdades fundamentais das pessoas que estão relacionados com esses dados. Ao proteger os dados pessoais, é possível garantir que tais núcleos essenciais não sejam violados.

As proteções de privacidade envolvem a garantia de segurança para dados pessoais e todas as atividades associadas envolvidas na coleta, armazenamento, processamento, acesso, transmissão, compartilhamento e descarte de dados. Historicamente, as organizações não tinham controles de segurança de dados fortes e abrangentes implementados em toda a empresa, em todos os dispositivos finais.

Esclarece Guerra (2022) que, na era digital, normalmente aplicamos o conceito de privacidade de dados a informações pessoais críticas, também conhecidas como informações de identificação pessoal e informações pessoais de saúde. Isso pode incluir números do seguro social, registros médicos e de saúde, dados financeiros, incluindo contas bancárias e números de cartão de crédito, e até mesmo informações básicas, mas ainda confidenciais, como nomes completos, endereços e datas de nascimento.

Lima (2016) lembra que as empresas devem proteger a privacidade de seus consumidores é uma meta principal, se preocupam com a privacidade de seus consumidores e apoiam o cumprimento dessa meta com práticas de privacidade transparentes e consistentemente seguidas que demonstram esse cuidado, construirão conexões emocionais com sua marca, que vai melhorar o valor da marca.

As organizações que implementam tais controles irão, como resultado, reduzir o número de incidentes de segurança que resultam em violações de privacidade. Menos violações significam que a empresa não perde a confiança e, consequentemente, perde clientes ou outros tipos de negócios. Isso também significa que a empresa não precisa lidar com multas, penalidades plurianuais ou processos civis após o efeito das violações.

Ainda para Lima (2016), os regulamentos de proteção de dados são necessários para garantir um comércio e uma prestação de serviços justos e amigos do consumidor. Logo, os dispositivos de proteção de dados pessoais causam uma situação em que, por exemplo, os dados pessoais não podem ser vendidos livremente, o que significa que as pessoas têm um maior controle sobre quem os faz e que tipo de ofertas fazem.

Para garantir a segurança dos dados pessoais, é importante saber quais dados estão sendo processados, por que estão sendo processados e com que base. Além disso, é importante identificar quais medidas de proteção e segurança estão em uso (RODATÀ, 2018). Tudo isso é possível por meio de uma auditoria minuciosa de proteção de dados, que identifica o fluxo de dados e se os regulamentos de proteção de dados estão sendo seguidos (RODATÀ, 2018).

A responsabilidade civil, encontra-se cada vez mais presente em no cotidiano e apresenta-se, baseada no princípio legislativo de que aquele que causar dano a outrem, seja essa moral ou material deve reestabelecer o bem ao estado em que se

encontrava antes do seu ato danoso e, caso o reestabelecimento não seja possível, deverá compensar o dano causado.

Lembra Diniz (2020) que:

> A responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição lega (DINIZ, 2020, recurso digital).

No âmbito normativo, o Código Civil de 2002 (CC/02), em seu art. 186, versa que, aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. Por sua vez, o art. 187, estabelece que também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes (BRASIL, 2002).

Neste contexto, a responsabilidade civil das empresas tem se tornado cada dia mais presente na sociedade, despertando o interesse jurídico não só dos pacientes, mas de toda a classe médica que busca respaldo e apoio junto ao ordenamento jurídico. Ademais, no contexto do atendimento virtual, é fundamental pensar na proteção desse bem jurídico no espaço virtual.

Nesse sentido, cumpre lembrar que o CC/02 estabelece o dever de reparação. Assim, o art. 927 versa que:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (BRASIL, 2002).

É importante destacar que todas as empresas possuem dados, como arquivos pessoais, dados de clientes, informações de produtos e transações financeiras. As decisões que a administração toma com base nesses dados são os processos de trabalho seguidos pelos funcionários para entregar produtos e serviços de qualidade. Lembra Borba (2019) que, na verdade, os dados são um dos ativos mais importantes de uma organização.

Por esse motivo, a LGPD acrescentou outra camada de importância à segurança de dados, tornando-a não apenas um requisito comercial, mas também um requisito legal. Assim, o legislador optou por uma interpretação ampliativa do sentido de dados pessoais e, dentre outras coisas, o art. 5º, versa que:

> 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; [...] (BRASIL, 2018).

De fato, a Lei de Proteção de Dados contém um conjunto de princípios que as organizações, o governo e as empresas devem seguir para manter os dados de alguém precisos, protegidos, protegidos e legais. Entretanto, essa traz uma cláusula de exclusão as entidades governamentais. Assim, dispõe que:

> O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso[...] (BRASIL, 2018).

Outra evolução normativa, é que essa exige que as organizações implementem medidas técnicas e organizacionais adequadas para garantir e ser capaz de demonstrar que o processamento é realizado em conformidade com o regulamento. Assim, o supracitado artigo ainda versa que:

> segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de

> comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

A partir do exame normativo, é possível verificar que uma parte importante dessas medidas é o treinamento de conscientização sobre segurança: os funcionários precisam estar cientes da importância de seguir os procedimentos e processos de segurança de dados.

3.2 EFICÁCIA DA LGPD NO COMBATE A SUPEREXPOSIÇÃO DE INFORMAÇÕES

Cumpre lembrar que os princípios estabelecidos na Lei de Proteção de Dados ajudam as empresas a garantir que os detalhes de seus funcionários, clientes e usuários sejam devidamente protegidos. Leciona Borba (2019) que como empregador e gerente de negócios, tem-se o dever de garantir que todas as informações estejam corretas.

Ademais, Rodatà (2018) destaca que seguir os procedimentos adequados de proteção de dados também é crucial para ajudar a prevenir crimes cibernéticos, garantindo que os detalhes, especificamente bancários, endereços e informações de contato sejam protegidos para evitar fraudes. Na prática, uma violação em sua proteção de dados pode custar caro. E os clientes e funcionários afetados, em alguns casos, podem buscar compensação contra a empresa.

Para Rodatà (2018), quando os clientes fornecem suas informações pessoais a empresas, esses confiam- dados pessoais que podem ser usados contra si se caírem em mãos erradas. É por isso que a privacidade de dados existe para proteger esses clientes, mas também as empresas e seus funcionários, de violações de segurança.

No que se refere ao consentimento, estabelece a norma, em seu art. 8º, que:

> O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas

> contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei (BRASIL, 2018).

Diante da análise do dispositivo, verifica-se que cumprir os regulamentos de privacidade de dados é importante não apenas porque informações confidenciais podem ser mal utilizadas no caso de ocorrer uma violação de dados, mas também porque existem leis que impõem essa conformidade.

Entretanto, um dos principais motivos pelos quais as empresas cumprem os regulamentos de privacidade de dados é evitar multas. Dentre os dispositivos que estabelecem esse tipo de sanção, destaca-se o art. 52 que versa da seguinte forma:

> Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II (BRASIL, 2018).

Para cumprir os regulamentos de privacidade de dados, se precisa atender a certos requisitos legais. Um desses requisitos é a implementação de fortes proteções de segurança para garantir a proteção da privacidade dos dados. Com essas medidas, o número de ameaças à segurança diminuirá significativamente e sua empresa não sofrerá perda de receita

Como mencionado antes, uma violação de dados pode levar ao roubo de informações valiosas do cliente, o que pode impactar negativamente os proprietários

dos dados. Leciona Borba (2019) que a maioria das organizações possui um código de ética em vigor. Mesmo aqueles que não o possuem seguem pelo menos certas práticas éticas. Sem isso, eles não seriam capazes de permanecer no mercado. Uma dessas políticas afirma que as informações confidenciais devem ser tratadas com responsabilidade e usadas apenas para fins comerciais.

Buscando criar uma gestão organizacional dos dados, Stallings (2015) leciona que Sempre que dados pessoais são coletados, esses precisam ser devidamente identificados e inventariados. Logo, a empresa também precisa fornecer um método de rastreamento para todos os dados que tornará mais fácil localizar e proteger. Tudo isso precisa estar de acordo com os padrões legais e recomendados.

Desta forma, as organizações que cumprem os regulamentos de privacidade de dados devem garantir integridade, confidencialidade e disponibilidade de dados com salvaguardas físicas, técnicas e administrativas. Essas proteções precisam ser eficazes na detecção e interrupção do acesso não autorizado aos dados.

Nesse sentido e buscando outras proteções, o art. 10 da LGPD, versa que:

> O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; eII - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei (BRASIL, 2018).

Para Stallings (2015) também é vital monitorar, avaliar e atualizar constantemente a segurança das informações para garantir que novas ameaças possam ser enfrentadas e tratadas de maneira adequada e eficiente. O autor esclarece que ainda que todas as políticas de conformidade, o sistema não pode ser totalmente protegido contra violações de dados e ataques cibernéticos. É por isso que toda organização precisa ter um plano de resposta eficaz para violações de dados, bem como funcionários treinados nesses planos de resposta a violações.

Como já disposto, todos os processos e planos de conformidade precisam ter a documentação adequada. É importante manter essa documentação disponível com um bom sistema de gerenciamento de conteúdo. Stallings (2015) defende que em grandes corporações também deve ter um funcionário responsável pelo

gerenciamento desses documentos.

Buscando compreender as estratégias de segurança de proteção de dados de uma organização, Stallings (2015) afirma que essa também precisa ter um processo definido para relatar não conformidade e um plano de escalonamento. Além disso, se precisa provar que é continuamente aderente por meio de auditoria, monitoramento e uso de controles.

3.3 MAIOR IMPACTO NA VIDAS DE INDIVÍDUOS NO VAZAMENTO DE DADOS

Junto com a segurança de dados, a privacidade de dados cria uma área de proteção de dados com dados utilizáveis protegidos como saída. No entanto, a privacidade de dados não se trata apenas do tratamento adequado dos dados, mas também da expectativa pública de privacidade, centrada no indivíduo como uma figura-chave.

Embora a LGPD não tenha sido a primeira lei de privacidade, foi a lei de proteção de dados mais abrangente e inovadora que refletiu a nova era digital na maneira como os dados são criados e gerenciados nos processos de negócios cotidianos modernos. Leciona Guerra (2022) que:

> Privacidade significa respeitar os indivíduos. Se uma pessoa deseja manter algo privado, é desrespeitoso ignorar os desejos dessa pessoa sem uma razão convincente para fazê-lo. Obviamente, o desejo de privacidade pode entrar em conflito com valores importantes, portanto, a privacidade nem sempre pode vencer na balança. Às vezes, os desejos das pessoas por privacidade são simplesmente deixados de lado por causa da visão de que o dano em fazer isso é trivial (GUERRA, 2022, p. 14).

De fato, esse conceito de privacidade, a vida privada toma novos contornos com as modificações das relações sociais. Nesse sentido, Arendt (2017) leciona que privacidade moderna, diferentemente da que existia na antiguidade, não é apenas oposto à esfera política, mas se contrapõem à esfera social, possuindo como primordial função a de abrigar o que é íntimo. Buscando tutelar esse novo valor, o art. 2º da LGPD estabelece como diretrizes:

> 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 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; eVII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Assim, a supracitada norma recepciona preceitos estabelecidos em texto e reconhece que a privacidade deve ser tutelada por todos os sujeitos que compõe a sociedade. Inclusive, o art. 3º versa que a norma se aplica a pessoa natural ou por pessoa jurídica de direito público ou privado. Tal ampliação é considerado um grande avanço normativo e faz da LGPD e um marco na tutela desse bem jurídico.

De fato, pode se verificar também quando correlacionado a doutrina da Guerra (2022) que compreende que do direito à privacidade decorre à proteção da reputação depende da proteção não apenas contra falsidades, mas também contra certas verdades. Para esse autor, saber detalhes particulares sobre a vida das pessoas não leva necessariamente a um julgamento mais preciso sobre as pessoas.

Ainda para Guerra (2022), a privacidade de dados se concentra nos direitos dos indivíduos, no objetivo da coleta e processamento de dados, nas preferências de privacidade e na forma como as organizações governam os dados pessoais dos titulares dos dados. Nessa perspectiva, a LGPD se se concentra em como coletar, processar, compartilhar, arquivar e excluir os dados.

Castells e Cardoso (2006) acreditam que romper esses limites pode criar situações sociais embaraçosas e prejudicar nossos relacionamentos. A privacidade também é útil para reduzir o atrito social que se encontram na vida e fundamental para que o indivíduo desenvolva sua personalidade.

Cumpre ressaltar que, o ordenamento jurídico interno está em consonância com as normas de direito internacional, visto que, a DUDH/48, em seu art. 12, versa que ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. De fato, a partir da técnica de interpretação sistêmica do ordenamento jurídico interno e internacional, no direito à privacidade está implícito no direito à vida e à liberdade garantidos aos cidadãos.

No âmbito conceitual, Branco e Mendes (2012) lecionam que o domicílio

delimita um espaço físico em que o indivíduo desfruta da privacidade, em suas variadas expressões. Para esses, nesse espaço o indivíduo não deve sofrer intromissão por terceiros, e deverá gozar da tranquilidade da vida íntima. Ou seja, é um local em que deve ter repouso e tranquilidade.

Ademais, os supracitados autores ainda afirmam que assim o conceito de domicílio abrange ‘todo lugar privativo, ocupado por alguém, com direito próprio e de maneira exclusiva, mesmo sem caráter definitivo ou habitual’. Para esses, o conceito constitucional de domicílio é, assim, mais amplo que aquele do direito civil. De fato, o ordenamento jurídico interno vem ampliando a interpretação desse instituto.

Por sua vez o Pacto de San José da Costa Rica, em seu art. 11, 2, quando da tutela da proteção da honra e da dignidade, versa que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.(RIBEIRO,2016)

Buscando delimitar o conceito de domicílio, o Código Civil de 2002, em seu art. 70 versa que esse é o lugar onde em que a pessoa natural estabelece a sua residência com ânimo definitivo. Todavia, diante das complexidades das relações da vida, esse reconhece que as pessoas podem possuir mais de um domicílio. Logo, art. 71 dispõe que se a tiver diversas residências, onde, alternadamente, viva, considerar-se-á domicílio seu qualquer dessas.

Buscando tutelar a prática profissional, em seu art. 72 há uma extensão desse instituto. Assim, o dispositivo versa que é também domicílio da pessoa natural, quanto às relações concernentes à profissão, o lugar onde está é exercida. De fato, essa garantia vem sendo observada quando do julgamento de lides contendo a matéria em e, partir, da técnica de interpretação extensiva, até por vezes tendo seu sentido ampliado.

Na medida em que a relação com os meios de comunicação se intensifica e a produção em massa torna-se evidente, surge a preocupação geral de garantir uma mídia livre, independente, plural e diversificada, preocupação esta que passa a se fixar como o ideal a ser alcançado para que o direito à liberdade de buscar, difundir e receber informações possa ser realizado em sua plenitude (SILVEIRA, 2016).

Sendo o Brasil um país signatário da Declaração Universal dos Direitos Humanos de 1948 (DUHD) e do Pacto de San Jose da Costa Rica de 1969, esse possui o deve de garantir esse direito fundamental. Nesse sentido o documento

americano dispõe que:

> 4. O acesso à informação em poder do Estado é um direito fundamental de cada indivíduo. Os Estados têm a obrigação de garantir o pleno exercício deste direito. Este princípio permite apenas limitações excepcionais que devem ser previamente estabelecidas por lei no caso de um perigo real e iminente que ameace a segurança nacional em sociedades democráticas (CADH, 1969).

Ademais, lembra Reimão (2011) que o acesso do público à informação e proteger as liberdades fundamentais, de acordo com a legislação nacional e acordos internacionais. Para Reimão (2011) é esse instrumento deve ser compreendido como parte de um aparelho de coerção e repressão que, muito mais do que afetar a circulação de alguns bens culturais, restringia a produção e circulação da cultura. Ademais, ainda é uma forma de exercício de controle estatal.

Ao passo em que a mídia constitui um importante meio de transmissão de informações com o intuito de educar e democratizar surge questionamentos direcionados ao potencial que as mídias sociais têm em criar condições manipulativas e gerar tendências nas preferências e opiniões da população sobre determinado tema. (SILVEIRA, 2016).

Esses fatos demonstram a influência das desses recursos nas relações modernas, a dimensão imprevisível que tais ferramentas podem assumir e a vulnerabilidade à qual todos, irrestritamente, estão sujeitos. Ainda assim, Reimão (2011) justifica que nada pode suspender garantias individuais e criam condições para à divulgação da informação, à manifestação de opiniões e às produções culturais e artísticas.

De fato, se outrora uma informação sensacionalista praticada na presença de um grupo de pessoas gerava um inegável prejuízo para o ofendido, hodiernamente, a mesma ofensa, se veiculada em uma rede social, pode atingir nefastas proporções (OLIVEIRA, 2003). É notória, assim, a carga negativa que se atribui ao estilo sensacionalista. As características desse tipo de produção informativa baseada no exagero podem justificar a situação.

Por outro, contrasta-se com o desvio da finalidade dessas redes, porque os usuários passaram a escrever informações que com certa frequência violam direitos e garantias fundamentais, praticados por usuários que por muitas vezes se

escondem por trás de apelidos, pseudônimos e perfis falsos, cometendo crimes ocultados pelo anonimato (LEITE, 2017).

Ainda assim, lembra Fiss (2005) que:

> (...) uma sociedade democrática está continuamente em processo de mudança, terá restrições de direitos e liberdades e seus procedimentos serão frequentemente questionados. Isso é garantido pelo direito à liberdade de expressão, que, portanto, é vista como um pré-requisito da democracia. Consequentemente, a democracia pode ser vista como um sistema político trágico (FISS, 2005, recurso digital, grifo nosso).

Entretanto, lembra Leitão (2011) que isso não garante que a liberdade de expressão é ou poderá ser absoluta e deve ser respeitada em todos os espaços um código de conduta específico. Ainda assim, essa esclarece que a censura – mais que um ato de poder oficial – se sofisticou e se consolidou como um instrumento institucional, sustentado por rígidos mecanismos de controle e administração da informação

Ainda para Leitão (2011), o público em geral está se tornando mais ciente de todos os seus direitos crescentes de dizer àqueles que coletam seus dados pessoais que esperam ter seus dados pessoais protegidos e têm direito de acessar e controlar seus dados pessoais. Assim, leciona Castells e Cardoso (2006) que privacidade de dados está relacionada a como uma informação - ou dados - deve ser tratada com base em sua importância relativa.

Já para Rodatà (2018), para uma empresa, a privacidade de dados vai além das proteções de informação de seus funcionários e clientes. Também inclui as informações que ajudam a empresa a operar, sejam dados proprietários de pesquisa e desenvolvimento ou informações financeiras que mostram como ela está gastando e investindo seu dinheiro. Ademais, lembra o autor que:

> Quando os dados que deveriam ser mantidos em sigilo chegam às mãos erradas, coisas ruins podem acontecer. Uma violação de dados em uma agência governamental pode, por exemplo, colocar informações ultrassecretas nas mãos de um estado inimigo. Uma violação em uma empresa pode colocar dados proprietários nas mãos de um concorrente (RODATÀ, 2018, recurso digital).

Além disso, as habilidades e oportunidades para recuperar diferentes tipos de dados pessoais estão evoluindo extremamente rápido. Logo, o processamento não autorizado, descuidado ou imprudente de dados pessoais pode causar grandes danos a pessoas e empresas.

Por exemplo, especificamente, quando do contexto pandêmico, inúmeras organizações tiveram que desenvolver suas atuações através teleatendimento. Quando da reflexão da proteção dos dados dos usuários do paciente, parece que as normas devem ser ainda mais observadas, visto que, podem ocasionar um dano maior a honra dos usuários.

Nesse sentido, a Resolução nº 2.217 de 27 de setembro de 2018 e Lei nº 13.787, de 27 de dezembro de 2018, dispõem sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, em seu art. 2º essa versa que o processo de digitalização de prontuário de paciente será realizado de forma a assegurar a integridade, a autenticidade e a confidencialidade do documento digital.

Ademais, os parágrafos dos referidos artigos ainda versam que:

> § 1º Os métodos de digitalização devem reproduzir todas as informações contidas nos documentos originais. § 2º No processo de digitalização será utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito. § 3º O processo de digitalização deve obedecer a requisitos dispostos em regulamento (BRASIL, 2018).

Lembra Rodatà (2018) que o não cumprimento dos regulamentos de proteção de dados pessoais pode levar a situações ainda mais duras, em que é possível extrair todo o dinheiro da conta bancária de uma pessoa ou mesmo causar uma situação de risco de vida, manipulando informações de saúde.

Não tem como negar que nos dias atuais existe a formação de um contrato quando um médico atende um paciente. Esse contrato mantém uma obrigação subjetiva, pois apesar de tudo, o médico não pode prometer a cura ao paciente, e sim usar todo o seu conhecimento para fazer o tratamento mais adequado para que o paciente fique bem.

Assim dispões Gonçalves (2022):

> Comprometem-se os médicos a tratar o cliente com zelo, utilizando-se dos recursos adequados, não se obrigando, contudo, a curar o doente. Serão, pois, civilmente responsabilizados somente quando ficar provada qualquer modalidade de culpa: imprudência, negligência ou imperícia. (GONÇALVES, 2022, p. 15).

Ademais, o art. 31 estabelece que:

> A oferta e apresentação de produtos devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores. (BRASIL, 1999).

Se estendendo esse dever de informar não só para os pacientes, como também para os seus familiares ou responsáveis, os quais devem ser orientados de todos os cuidados que devem ter com o doente. Segundo Melo (2008) o dever mais importante do médico deveria ser o de continuar aprimorando e atualizando para um melhor atendimento aos seus pacientes, procurando sempre novas técnicas, medicamentos que sejam mais eficazes para tratamentos.

Para Rodatà (2018), a privacidade reflete, portanto, duas noções subjacentes. Em primeiro lugar, a privacidade em geral e a privacidade informativa em particular são sempre questões de grau. Raramente alguém está em uma condição de completa inacessibilidade física ou informativa para outras pessoas, nem desejaria permanecer assim. Em segundo lugar, embora a privacidade das informações possa ser valiosa e merecedora de proteção, muitos defensores da privacidade ponderados argumentam que ela não tem, por si só, significado moral ou valor inerente.

Confidencialidade e privacidade são princípios relacionados, ambos protegendo o paciente da divulgação de registros médicos. Embora a confidencialidade seja geralmente considerada uma regra ética para profissionais médicos e a privacidade como uma questão legal, muitos países também codificaram a confidencialidade médica dentro das leis nacionais ou dos princípios da lei comum, o que significa que as informações médicas não podem ser

divulgadas sem o consentimento do paciente. Os prestadores de cuidados de saúde são, portanto, geralmente obrigados por lei ao dever de confidencialidade e privacidade.

Para Rodotà (2017), duas tendências um tanto distintas levaram ao aumento do acesso ao registro de saúde primária e subsequentes preocupações sobre privacidade. Um tem a ver com os registros de saúde primários, independentemente de como são criados e mantidos; a outra envolve registros de saúde armazenados eletronicamente.

Leciona Villas-Bôas (2015) que as abordagens éticas, legais e outras existentes para proteger a confidencialidade e a privacidade dos dados pessoais de saúde oferecem algumas salvaguardas, mas permanecem lacunas e limitações importantes. Para o autor, à medida que os registros continuam a suplantar os encontros face a face em nossa sociedade, não houve nenhuma tendência compensatória de dar ao indivíduo o tipo de controle sobre a coleta, uso e divulgação de informações.

Rodotà (2008) ainda lembra que quantidade e o tipo de informações sobre cuidados de saúde agora coletadas também aumentaram nos últimos anos. A participação na prestação de cuidados de saúde de muitos indivíduos e grupos de provedores diferentes exerce forte pressão para documentar cada vez mais detalhadamente. O número crescente de tecnologias disponíveis para diagnóstico e terapia significa que os detalhes que um provedor poderia em um determinado momento convocar devem agora ser registrados e, assim, estar disponíveis para inspeção por outros.

Ainda para autor supracitado, quanto mais detalhadas forem as informações sobre um indivíduo ou classe de indivíduos, mais apropriado, espera-se, será o tratamento que receberão. Além disso, a documentação do atendimento e dos fatores de risco é essencial para promover a continuidade do atendimento ao longo do tempo e entre os provedores. É também uma primeira defesa contra-acusações de imperícia.

Além disso, a crise do COVID-19 tornou as questões de privacidade de dados ainda mais salientes. Conforme as organizações coletam informações pessoais sobre a saúde dos funcionários e viagens como parte de sua resposta para conter a propagação do vírus, essas precisam tomar medidas adequadas para proteger a privacidade dos funcionários e manter a conformidade com os regulamentos de

privacidade de dados aplicáveis. (WIMMER, M. 2021)

4 ENFRENTAMENTO NO DIREITO AO ESQUECIMENTO POR TRIBUNAIS

Nos últimos anos, o direito ao esquecimento tem sido objeto de crescente atenção e preocupação. À medida que as pessoas percebem o quão implacável a memória férrea da Internet pode ser, e quão repentinamente os dados do passado podem ressurgir em contextos inesperados, muitos têm uma sensação distinta de desconforto.

4.1 DO DIREITO COMPARADO

A preocupação com a proteção dados é uma tendência no direito comparado. Nether (2018) expõe que o Regulamento Geral de Proteção de Dados da União Europeia ('GDPR') executa fielmente as implicações da metáfora do petróleo, apesar do ajuste inadequado da metáfora. O GDPR presume que os dados pessoais são importantes, tanto que todos os aspectos da interação com os dados requerem um planejamento cuidadoso.

Especificamente, no caso do referido conjunto normativo, Nether (2018) esclarece que as práticas da indústria da informação e até mesmo a literatura acadêmica sobre técnicas de identificação de ponta. Para o autor, por essa e outras razões, o GDPR tem um alcance extraordinariamente amplo em todas as dimensões. Duas definições de limite são 'dados pessoais' e as atividades de informação consideradas 'processamento'.

Estudando os pressupostos históricos e a política legislativa, Guerra (2022) afirma que na Europa há muito reconhece o direito da privacidade explicitamente como um direito humano. Ainda para o autor, os compromissos europeus vão além do lar, o foco de tantas leis americanas, para incluir proteções para a vida familiar, comunicações, reputação e, com o aumento da era da informação, para a privacidade no contexto do processamento de dados.

Guerra (2022) esclarece que embora os advogados norte-americanos possam se referir amplamente a 'privacidade' ou 'privacidade de informações', a lei europeia discute a privacidade de informações como 'proteção de dados'. De fato, Nether (2018) reconhece que na Europa, a proteção de dados é cada vez mais vista como separada do direito à privacidade. A proteção de dados se concentra em se os dados são usados de forma justa e com o devido processo enquanto a privacidade

preserva o ideal ateniense de vida privada.

Também aponta que em 1990, a Comissão Europeia temia que as leis nacionais divergentes de proteção de dados prejudicassem o mercado interno na UE. Nesse ano, publicou uma proposta de diretiva relativa à proteção de dados. Após cinco anos de negociações, a Diretiva de Proteção de Dados final foi adotada em 1995. A Diretiva estabeleceu um regime omnes baseado nos FIPs, que se aplicava à maior parte dos setores público e privado (com exceção deste último). A Diretiva exigia que os Estados-Membros aprovassem legislação de implementação.

Nether (2018) acredita que os problemas surgiram rapidamente com a diretiva. A Diretiva não harmonizou totalmente as leis nacionais de privacidade e, mesmo na Europa, os países se comportaram de forma oportunista para cortejar as grandes tecnologias com sinais de aplicação fraca e esquemas fiscais vantajosos.

Mesmo entre os países comprometidos com a privacidade, a fiscalização foi frouxa, com os franceses multando o Facebook em meros 150.000 euros em 2017. Essa lacuna de fiscalização deixou a Europa com a reputação de região com regras, mas sem policiamento real, enquanto os Estados Unidos eram vistos como não estando vinculados às regras, mas tinham a Federal Trade Commission na ronda de fiscalização.

Ainda para Nether (2018), o GDPR é a tentativa da UE de abordar essas e outras deficiências. Fez isso em um processo completamente diferente dos esforços legislativos dos Estados Unidos. Os legisladores europeus iniciaram um processo que envolveu uma grande variedade de consultas a especialistas e profunda sofisticação sobre como as práticas de informação podem ser manipuladas para fugir das metas regulatórias.

4.2 DAS DEMANDAS DO DIREITO AO ESQUECIMENTO NO ORDENAMENTO INTERNO

O direito ao esquecimento foi colocado firmemente na agenda política brasileira e é frequentemente discutido na literatura. Embora a referência a um direito ao esquecimento já possa ser encontrada na década de 1990, como parte dos admiráveis produtos do pensamento e da legislação.

A literatura mais atual discute porque tal direito precisa ser estabelecido e

quais meios possíveis poderiam ser inventados para efetivá-lo. No entanto, não há consenso sobre o que exatamente significa o direito ao esquecimento e seu status – como direito, interesse ou valor; precisa de reforço ou para ser criado do zero – não é claro.

Além disso, embora a ideia geral seja intuitiva e pareça amplamente apreciada, a forma jurídica e as implicações práticas de um direito ao esquecimento ainda não foram analisadas. Esta contribuição visa avaliar criticamente o que um direito ao esquecimento pode ou deve implicar na prática.

Consalter (2016), quando do exame de lides internas, se concentra particularmente no direito ao esquecimento como um direito legal (em vez de, por exemplo, um valor abstrato), pois como advogado estou interessado em como o status jurídico de tal direito pode ser imaginado. Também me limitarei ao contexto europeu, onde o direito ao esquecimento tem o impulso político mais visível, bem como bons pontos de partida para o esquecimento de dados na Diretiva de Proteção de Dados.

Ainda assim, atualmente não há lei ou regulamento que trate expressamente do esquecimento no Brasil. No entanto, um projeto de lei foi discutido na legislatura brasileira que teria modificado o Marco Civil da Internet brasileiro, incluindo um esquecimento muito amplo. O projeto teria concedido aos tribunais a competência para ordenar a remoção de conteúdo, e não apenas uma mera desalistagem nos sites de busca.

O Superior Tribunal de Justiça (STJ), o mais alto tribunal do Brasil para questões não constitucionais, decidiu recentemente um caso histórico que trata da responsabilidade e responsabilidade dos provedores de mecanismos de busca. A decisão veio em resposta ao recurso do Google Brasil contra um julgamento que ordenou a subsidiária local do Google a remover determinado conteúdo do banco de dados de seu mecanismo de busca.

Na Reclamação 18.685 ES/2014 de, 2014, o STJ decidiu que não era obrigação dos provedores de mecanismos de pesquisa remover os resultados da pesquisa, mas que o proprietário do conteúdo era responsável pelo conteúdo adequado (SCOCUNGLIA,2014). Além disso, o tribunal estabeleceu que que os provedores de mecanismos de busca, pela natureza de seu serviço, não pré-selecionam o conteúdo obtido por critérios de busca pelo usuário. O tribunal também determinou que os provedores de mecanismos de pesquisa não podem ser

obrigados a filtrar seus resultados de pesquisa por termos, frases, imagens ou texto específicos, independentemente da indicação de um URL específico.

É importante destacar que o STJ não se pronunciou expressamente sobre a aplicabilidade ou não do esquecimento no caso, mas apenas analisou o regime de responsabilidade para determinar se o Google Brasil tinha a obrigação de remover o acesso ao conteúdo.

Assim como no caso Aída Curi, o STJ no Recurso Especial (Resp) n 1.334.097 decidiu sobre a existência e aplicabilidade do esquecimento no ordenamento jurídico brasileiro (CANÁRIO, 2013). Em ambas a ré foi a Rede Globo, a maior rede de televisão comercial do Brasil, como única ré. O STJ teve que decidir em ambos os casos se a denúncia de crimes ocorridos há muitas décadas poderia servir de fundamento para a aplicação do esquecimento.

O STJ decidiu nos autos REsp. 1.335.153 que o réu violou os direitos do autor à honra e à dignidade ao apresentá-lo como coautor de um crime pelo qual ele havia sido considerado inocente. É importante ressaltar o entendimento da ministra Nancy Andrighi expõs que direito à liberdade de imprensa será considerado legítimo se o conteúdo transmitido for verdadeiro, de interesse público e não violar os direitos da personalidade do indivíduo noticiado

A ministra teve todos os argumentos favoráveis a remoção do conteúdos jornalisticos desatualizados que a corroboram com o direito ao esquecimento sobre o direito de impressa, somente ao final, seu voto teve influencia pela última decisão do transitado em julgado do STF, o tema de 786.

No caso do Resp. 1.593.873o STJ decidiu que a importância histórica de um crime ou evento pode superar o esquecimento e os direitos à honra e à dignidade. O tribunal decidiu que o nome da vítima estava tão inextricavelmente ligado ao crime em si, que a representação dos eventos seria impossível sem usar o nome da vítima. Assim, determinou que o direito à liberdade de imprensa deveria prevalecer. Além disso, o tribunal também determinou que a própria passagem do tempo havia – de certa forma – feito as pessoas esquecerem o crime e, portanto, minimizado o nível de dor que a família de uma vítima de um crime poderia sentir ao ver o nome e as imagens de a vítima retratada e divulgada na mídia.

Mais recentemente, o Superior Tribunal de Justiça decidiu em um caso envolvendo o Google Brasil. O tribunal decidiu que forçar os provedores de mecanismos de busca a remover o acesso ao conteúdo de seus mecanismos de

busca imporia um fardo intolerável a eles. O tribunal determinou que essa responsabilidade, por sua vez, transformaria essas empresas em uma forma de censores digitais. Ainda no REsp. 1.593.873 O tribunal também decidiu que, uma vez que os conteúdos permaneceriam na Internet, a responsabilidade por esses conteúdos recai sobre o fornecedor de conteúdos, e não sobre o fornecedor do motor de busca.

É importante ressaltar que há um processo ainda pendente no Supremo Tribunal de Justiça, a mais alta corte do Brasil em questões constitucionais, que pode se mostrar essencial para a aplicação do esquecimento no ordenamento jurídico brasileiro, bem como fundamental para o equilíbrio entre o esquecimento e outros direitos e liberdades constitucionais fundamentais.

Por sua vez, no resolução 759/2021, o STF seguiu um argumento que possibilita a compreensão que a que infere-se deia por trás do direito ao esquecimento (é fornecer aos indivíduos uma representação correta e atualizada de sua identidade pessoal, obtendo o apagamento (ou pelo menos o chamado desreferenciamento) de seus rastros digitais anteriores deixados online.

De fato, a Internet não foi projetada para esquecer, mas para armazenar nossas pegadas digitais quase permanentemente, mesmo nos casos em que possam prejudicar nossa dignidade e reputação. Um papel fundamental a este respeito é desempenhado pelos motores de busca, empenhados em facilitar a recuperação de informações que não seriam tão facilmente descobertas de outra forma.

Por quando do julgamento da Ação Direta de Inconstitucionalidade (ADI) 4815 Plenário do Supremo Tribunal Federal declarou inexigível a autorização prévia para a publicação de biografias. Nesses autos, o STF definiu a natureza do RTBF como parte do direito da personalidade, relacionado a conceitos como dignidade, reputação, privacidade e proteção da integridade moral e jurídica da pessoa.

Com efeito, o termo direito ao esquecimento pode ser entendido como ambíguo e enganador, englobando várias componentes e referindo-se a diferentes situações que por vezes se sobrepõem e podem ser confundidas umas com as outras. Além disso, parece ser significativamente determinado por elementos externos, como a passagem do tempo, o interesse público pela informação e o papel desempenhado pelo titular dos dados na sociedade.

5 CONSIDERAÇÕES FINAIS

O esquecimento traz à tona as tensões entre o direito à privacidade e o direito à liberdade de expressão e, dado o ritmo acelerado em que o espaço digital está mudando, é provável que essas tensões persistam. Desde que as substituições do interesse público sejam priorizadas e as salvaguardas adequadas sejam implementadas, pode haver algum grau de consonância

No que tange a revisão de literatura, percebeu-se que ser humano é considerado um ser autônomo com um instinto que precisa ter controle e confidencialidade sobre determinados aspectos de sua vida, considerando que estamos em uma era em que nossos dados estão na internet ou em fóruns públicos. Portanto, é mais importante que todos a protejam. Para isso, muitos países já se apresentaram para fazer leis sobre proteção de dados essa questão se tornou o centro das atenções do mundo.

Com o avanço da tecnologia de comunicação, o conceito tradicional de fazer, acessar e gerenciar registros mudou do formato baseado em papel para o formato eletrônico, que pode estar disponível em um ambiente de rede pública. É por isso que o equilíbrio marcante entre os dois direitos é mais difícil, exigente e desafiador.

No Brasil, a discussão sobre proteção de dados e a privacidade entrou em contexto conflito e percebeu-se uma tendência de onde a Suprema Corte reconhecer o direito à privacidade como um direito fundamental, como os caso que foram apresentados.

A última decisão do STF se deduziria o fim da discussão do direito ao esquecimento no Brasil. No entanto, para Satatinni e Gobato(2021), a discussão ainda se estende após o transitado em julgado e o que poderia possibilitar uma revisão futura da decisão.

Vale ressaltar que o Marco Civil da Internet e a implementação nacional da lei especifica para a proteção de dados na internet, a LGPD, houve o reconhecimento da necessidade de controle e proteção da privacidade do individuo diante do interesse público com o dever de publicar e informação transgredindo o princípio da privacidade e responsabilizar quem disponibiliza informações pessoais não consentidas. Infere-se que a leis que originadas de prevenção

A LGPD, como previamente tratado, não menciona o direito ao esquecimento de forma explicita, porém a lei promove o direito do indivíduo ter controle de seu

dados e informacões na internet. Dentre os principios abordados, se informações são ilegitimas e incorretas, é possível que o indivíduo tenha a remoção de dado na na web.

REFERÊNCIAS

ALMEIDA, L. G. e GOMES , A. S. M. S. **Direito ao esquecimento, LGPD e liberdade de expressão: como ponderá-los?**. Revista Consultor Jurídico. Disponível em: https://www.conjur.com.br/2021-fev-28/opiniao-direito-esquecimento-lgpd-liberdade-expressao. Acesso em: 21 de Dezembro 2022

ARAÚJO, N. R. N. **Liberdade de expressão e o discurso do ódio**. Curitiba: Juruá Editora, 2018.

BORBA, J. E. T. **Direito societário.** 12. ed. Rio de Janeiro: Renovar, 2019.

BRANCO, P. G. G.; MENDES, G. F. **Curso de direito constitucional**. 12º ed. São Paulo: Saraiva, 2017.

BRASIL. [Constituição (1988)]. Constituição Federal da República Brasileira de 1988. *In*: **VADE** Mecum. São Paulo: Saraiva: 2022.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA. **Enunciado 531.** Disponível em: https://www.cjf.jus.br/ enunciados/ enunciado/142. Acesso em: 10 out. 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. *In*: **VADE** Mecum. São Paulo: Saraiva: 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**.** *In*: **VADE** Mecum. São Paulo: Saraiva, 2022.

BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. *In*: **VADE** Mecum. São Paulo: Saraiva, 2022.

BUCAR, D. Controle temporal de dados: o esquecimento. **Revista Civilistica.com**. Rio de Janeiro, a. 2, n. 3, jul.-set. 2019, p. 9-10. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/113/83. Acesso em: 17 out. 2022.

CANÁRIO, Pedro. **STJ aplica 'direito ao esquecimento' pela primeira vez** Revista Consultor Jurídico. Disponível em: https://www.conjur.com.br/2013-jun-05/stj-aplica-direito-esquecimento-primeira-vez-condena-imprensa. Acesso em: 17 out. 2022

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

CASTELLS, M.; CARDOSO, G. (Org.). **A sociedade em rede:** do conhecimento a acção política. Lisboa: Imprensa Nacional: Casa da Moeda, 2006.

CONSALTER, Z. M. **Direito ao esquecimento**. Curitiba: Juruá Editora, 2016.

CONVENÇÃO AMERICANA DE DIREITOS HUMANOS. **Pacto de San Jose da Costa Rica.** *In*: **VADE** Mecum. São Paulo: Saraiva: 2022.

DINIZ, M. H. **Curso de direito civil brasileiro.** 20. ed. São Paulo: Saraiva, 2020.

FISS, O. M. **A Ironia da liberdade de expressão:** Estado, regulação e diversidade na esfera pública. Rio de Janeiro: Renovar, 2005.

GONÇALVES, C. R. **Direito Civil brasileiro:** responsabilidade civil. 5 ed. São Paulo: Saraiva, 2019.

GUERRA, S. C. S. **O direito à privacidade na internet:** uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2022.

HANS, B. C. **No exame**: reflexões sobre a era digital. São Paulo: Antropos, 2019.

LEITÃO, B. J. M. Bi**bliotecas públicas, bibliotecários e censura na Era Vargas e regime militar:** uma reflexão. Rio de Janeiro: Intertexto; Interciência, 2011.

LEITE, F. P. A. O exercício da liberdade de expressão nas redes sociais: e o marco civil da internet. **Revista de Direito Brasileira**, São Paulo, SP, n. 6, v. 13, n. 6, p. 150 - 166 , jan./abr. 2016.

LIMA, G. D. **Manual de direito digital:** fundamentos, legislação e jurisprudência. Curitiba: Appris, 2016.

MÈLO, Augusto. **Proteção de dados pessoais na era da informação**. Curitiba: Juruá Editora, 2019.

MORAES, Melina Ferracini de. **Esquecimento na internet**: das decisões judiciais no Brasil. Curitiba: Juruá Editora, 2018.

MORATO. Antônio Carlos; CICCO, M.C. Direito ao esquecimento: luzes e sombras. *In*: SILVEIRA, Renato de Mello Jorge. (Org.). **Estudos em homenagem a Ivette Senise Ferreira**. São Paulo: LiberArs, 2015.

NETHER, Nicholas Augustus de Barcellos. **Proteção de dados dos usuários de aplicativos**. Curitiba: Juruá Editora, 2018.

OLIVIEIRA, L. **A importância histórico-social das redes.** Rio de Janeiro: Terceiro Setor, 2003.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS EM PARIS. Declaração universal dos direitos humanos de 1948. *In*: **VADE** Mecum. São Paulo: Saraiva: 2022.

REIMÃO, S. **Repressão e resistência:** censura a livros na ditadura militar. São

Paulo: Fapesp, 2011.

RIBEIRO,T.S. Direito ao esquecimento como decorrência dos direitos da personalidade e da dignidade da pessoa humana. **Jus**. Disponível em: https://jus.com.br/artigos/52214/direito-ao-esquecimento-como-decorrencia-dos-direitos-da-personalidade-e-da-dignidade-da-pessoa-humana. Acesso em: 8 Dezembro 2022

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

RODOTÀ, Stefano. **A antropologia do homo dignus**. Revista civilistica. 2017. Disponível em: https://www.jur.puc-rio.br/wp-content/uploads/2021/08/STEFANO-RODOTA-A-antropologia-do-homo-dignus.pdf

SABATTINI, G. e GOBATO, C. **Direito ao esquecimento na 'era da superinformação'.** Consultor Jurídico. Disponível em: https://www.conjur.com.br/2021-mar-08/opiniao-direito-esquecimento-superinformacao. Acesso em: 10 de outubro 2022

SCHREIBER, Anderson**. Direito civil e constituição.** São Paulo: Atlas, 2019.

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2021.

SCOCUGLIA, Livia. **Google não é obrigado a filtrar conteúdo de busca, decide ministro do STJ.** Consultor Jurídico. Disponível em: https://www.conjur.com.br/2014-set-08/superior-tribunal-justica-decide-direito-esquecimento. Acesso em: 8 de Dezembro 2022

SILVEIRA, C. M. **Regulação da mídia e liberdade de expressão:** análise da experiência alemã. Rio de Janeiro: EdPUC, 2016.

STALLING, W. BROWN, L. **Segurança de computadores**. 2. ed. São Paulo: Pearson Education do Brasil, 2022.

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

VILLAS-BÔAS, M. E. O direito-dever de sigilo na proteção ao paciente. **Revista Biomédica,** São Paulo, n 23, a. 3, p. 13-23, 2015. Disponível em: https://www.scielo.com br. Acesso em: 10 out 2022.

WACHOWICZ,Marcos. **Proteção de dados pessoais em perspectiva: LGPD E RGPD na ótica do direito comparado**.GEDAI, Curitiba, 2020

WIMMER, Miriam**. Proteção de dados pessoais em tempos de pandemia: novos paradigmas para o compartilhamento e o uso secundário de dados no poder público.** Panorama Setorial da Internet, 2021