



REVISTA DO CAAP
fundada em 1921

A (DES)PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS NOS TERMOS DE USO DO “GRINDR”: A VULNERABILIDADE DE USUÁRIOS LGBTQIAPN+ EM APLICATIVOS DE RELACIONAMENTOS AMOROSOS E SEXUAIS

Anna Luísa Braz Rodrigues¹

Resumo: O "Grindr" é um aplicativo amoroso e sexual voltado para comunidade “queer”. Principalmente no caso de pessoas LGBTQIAPN+, as informações pessoais sobre sexualidade representam uma camada de vulnerabilidade para usuários dessa plataforma, pois tratam de temas que colocam a pessoa em situações potenciais de preconceitos e exposição pessoal. Dessa forma, o uso crescente da plataforma traz uma importante discussão sobre a responsabilidade dos controladores pela manutenção de espaços virtuais seguros. Busca-se, portanto, investigar a conformidade dos termos de uso do “Grindr” com as exigências da legislação brasileira no que diz respeito ao tratamento de dados pessoais sensíveis. O estudo emprega a análise textual-discursiva, obtendo dados de fontes bibliográficas e adotando uma abordagem jurídico-sociológica pelo método dedutivo, caracterizando-se como pesquisa teórica e jurídico-interpretativa com um caráter propositivo. No presente caso, a empresa possui termos de uso que citam a utilização de publicidade comportamental, o aprendizado de máquina, a criação de perfis de dados e a tomada de decisões automatizada, por exemplo. Assim, conclui-se que os termos de uso do "Grindr" revelam uma falta de atenção ao ordenamento jurídico interno, pois não fazem referências suficientes à LGPD. Além disso, a forma como o tratamento de dados

¹ Mestra e doutoranda em Direito pela UFMG. Integrante do grupo de pesquisa Laboratório de Bioética e Direito. Integrante do grupo de pesquisa Núcleo de Direito Privado e Vulnerabilidades.

pessoais ocorre não é adequadamente definida, gerando incertezas para os usuários e um consentimento inválido nos termos legais.

Palavras-chave: “Grindr”; direito à proteção de dados pessoais; dados pessoais sensíveis; sexualidade; direitos sexuais; LGPD.

(UN)PROTECTION OF SENSITIVE PERSONAL DATA IN "GRINDR'S" TERMS OF USE: THE VULNERABILITY OF LGBTQIAPN+ USERS IN ROMANTIC AND SEXUAL RELATIONSHIP APPLICATIONS

Abstract: "Grindr" is a dating and sexual application targeted towards the queer community. Particularly for LGBTQIAPN+ individuals, personal information regarding sexuality represents a layer of vulnerability for users of this platform, as it deals with subjects that can potentially expose them to prejudice and personal scrutiny. Therefore, the increasing use of the platform sparks an important discussion about the responsibility of controllers in maintaining safe virtual spaces. Consequently, there is a search to investigate the compliance of "Grindr's" terms of use with Brazilian legislation concerning the handling of sensitive personal data. The study employs textual-discursive analysis, gathering data from bibliographical sources and adopting a legal-sociological approach through deductive methodology, characterizing it as theoretical and legally interpretative research with a propositional nature. In this case, the company's terms of use mention the use of behavioral advertising, machine learning, the creation of data profiles, and automated decision-making, among other practices. Thus, it is concluded that "Grindr's" terms of use reveal a lack of attention to domestic legal regulations, as they do not make direct references to the LGPD (Brazil's General Data Protection Law). Additionally, the manner in which personal data is handled is not adequately defined, creating uncertainties for users and resulting in invalid consent under legal terms.

Keywords: "Grindr"; right to personal data protection; sensitive personal data; sexuality; sexual rights; LGPD.

INTRODUÇÃO

As informações pessoais sobre sexualidade representam uma camada de vulnerabilidade para usuários das plataformas de relacionamentos (Luna, 2009, p. 255-266), pois tratam de temas que colocam a pessoa em situações potenciais de discriminação. Principalmente no caso de pessoas LGBTQIAPN+², que enfrentam altos índices de preconceito e violência, a exposição de informações sobre orientação sexual ou identidade de gênero pode ter consequências graves em suas vidas pessoais, profissionais e sociais.

Dessa forma, a popularização do aplicativo “Grindr”, para encontros amorosos e sexuais, traz uma importante discussão sobre o controle efetivo que cada pessoa possui sobre o alcance de seus elementos pessoais e a responsabilidade de controladores pela manutenção de espaços virtuais seguros em termos de tratamento de dados pessoais. Em regra, os termos de uso servem de base para guiar o modo que cada empresa escolhe lidar com essas informações de seus usuários.

Busca-se, portanto, investigar a adequação dos termos de uso do “Grindr” (como plataforma de relacionamentos amorosos e sexuais) quanto aos direitos de personalidade e, especificamente, às exigências para o tratamento de dados pessoais sensíveis dispostas na Lei Geral de Proteção de Dados Pessoais (LGPD), tendo em vista a vulnerabilidade inerente às informações sobre sexualidade do usuário.

A inovação do trabalho se dá pelos avanços significativos, tanto no meio social quanto no direito civil, no que diz respeito à proteção de dados pessoais e à própria discussão sobre identidades LGBTQIAPN+. Dessa forma, é justificável engajar-se em debates abertos e construtivos sobre o tema, tendo em vista o progresso significativo observado no âmbito jurídico quanto aos referidos temas.

Em termos de metodologia, o estudo utiliza a abordagem da análise textual-discursiva. Existe também uma perspectiva crítico-metodológica que enxerga o Direito como uma intrincada rede de linguagens e significados. Os dados coletados são obtidos de fontes bibliográficas, como diplomas normativos, decisões judiciais, livros e artigos científicos, bem

²O termo LGBTQIAPN+ se refere a diversidade sexual e de gênero composta por pessoas que se identificam como lésbicas, gays, bissexuais, transgêneros, “queers”, intersexuais, assexuais, pansexuais e não-binários. O símbolo “+” representa a pluralidade das demais orientações sexuais e de gênero.

como notícias de jornais e outros portais, para fornecer uma visão abrangente e atualizada da realidade investigada. Em relação à perspectiva teórico-metodológica, a vertente jurídico-sociológica com método dedutivo explora o fenômeno jurídico dentro do contexto social. Além disso, a pesquisa é teórica e jurídico-interpretativa, possuindo um caráter propositivo que é característica inerente às pesquisas realizadas nas ciências sociais aplicadas (Gustin, Dias e Nicácio, 2020).

O marco teórico é constituído pela ideia de que o direito à proteção de dados pessoais constitui um direito da personalidade autônomo, conforme o que pressupõe o autor Bruno Ricardo Bioni (2019). A proteção de dados pessoais, inclusive, se qualifica como direito fundamental presente no art. 5º, inciso LXXIX, da Constituição Federal de 1988, em que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais (Brasil, 1988)". Isso se deu após intensos debates teóricos, a princípio encabeçados pelo autor Danilo Doneda (2020), no país.

Para atingir seu objetivo, o trabalho será dividido em três partes. O tópico inicial apresentará um panorama geral acerca das práticas sociais relativas à utilização de aplicativos de relacionamentos amorosos e sexuais, de modo a analisar as principais informações tratadas pelo “Grindr” e os escândalos decorrentes do tratamento delas. Em seguida, serão apresentadas as principais ideias sobre a vulnerabilidade dos usuários e as normativas acerca de dados pessoais sensíveis no ordenamento jurídico brasileiro, diante do que consta na LGPD. Por fim, o tópico final visa a analisar os termos de uso apresentados pelo “Grindr” e sua adequação em relação ao que consta no ordenamento jurídico brasileiro sobre tratamento de dados pessoais sensíveis, bem como propor uma reflexão acerca da tutela de danos no tocante à exposição de informações de sexualidade do utilizador.

1. O “GRINDR” COMO APLICATIVO VIRTUAL DE RELACIONAMENTOS AMOROSOS E SEXUAIS PARA COMUNIDADE “QUEER”

Pelas estatísticas do PoderData, 4 a cada 10 usuários utilizam aplicativos de relacionamentos amorosos e sexuais. Foram mais de 2.500 entrevistas, com grupos de distintas características de sexo, idade, renda, escolaridade e localização. Essas pessoas buscam encontros sérios, casuais ou apenas conversas virtuais, por meio da análise de perfis com informações pessoais, como fotos, cidade, escolaridade, entre outros (Karter, 2023).

O “Grindr”, especificamente, existe desde 2009 e se define como o maior aplicativo de sociabilidade para homossexuais, bissexuais, transgêneros e “queer”. A tecnologia é baseada na localização dos usuários, que podem trocar mensagens de texto, fotografias e vídeos com aqueles que estiverem próximos. A plataforma se propõe a ser “um espaço seguro onde você pode descobrir, navegar e ficar a 0 pés de distância do mundo “queer” ao seu redor” (Grindr, s.d.).

Com sede em West Hollywood, na Califórnia, possui cerca de 11 milhões de utilizadores mensais (O Globo, 2022). A versão paga do aplicativo tem cerca de 700 mil assinantes, sendo que estes podem utilizar recursos que excluem anúncios de terceiros, anulam mensagens já enviadas, oferecem a análise ilimitada de perfis, visualizam quando alguém está escrevendo, enviam fotos temporárias ilimitadas, conversam com perfis sem limitações de localidade, entre outros (Grindr, s.d.).

Essas plataformas são, afinal, uma nova forma de expressar sexualidade, que se enquadra na gama de direitos sexuais, reconhecidos nas últimas décadas como essenciais ao desenvolvimento humano. Importante, então, defini-los brevemente. Eles são um conjunto de direitos fundamentais que visam a garantir a liberdade, a autonomia e a dignidade das pessoas em relação à sua sexualidade (Leite, 2016). Eles abrangem diversos aspectos, como o direito à informação, à educação sexual, à saúde sexual e reprodutiva, à liberdade de expressão e identidade de gênero, ao consentimento, à privacidade e à não discriminação (Gomes, 2021, p. 3-7).

Para mais, ao explorar o significado do termo "queer", reforçado em toda divulgação do aplicativo, Marcelo Maciel Ramos (2021, p. 1694) conclui que tal não apenas expressa a recusa e a disputa teórica abrangente das últimas décadas, mas também é reivindicado e utilizado com diferentes intenções. Na língua inglesa, a palavra abrangeria gays, lésbicas, bissexuais e pessoas trans, de modo que muitos estudos passaram a ser assim identificados devido ao seu enfoque em sexualidades e identidades de gênero não normativas. No entanto, pondera-se que, ao ser usado como um guarda-chuva unificador superficial, há o risco de homogeneizar e apagar diferenças importantes entre os grupos e indivíduos englobados por essa denominação.

No caso de um aplicativo voltado especificamente para encontros LGBTQIAPN+, o sigilo dos perfis e das interações se mostra um aspecto em destaque. Conforme o que os autores

Eder Fernandes Monica e Ramon Silva Costa (2020) analisaram em trinta perfis do aplicativo, na cidade de Juiz de Fora, a abertura de uma conta virtual denota uma complexa expressão de liberdade sexual que reflete preconceitos sociais.

Ao analisar os perfis, foi verificado que os usuários mencionavam explicitamente a necessidade de manter suas interações em segredo, a fim de determinar a importância dada ao sigilo por eles. Entre os trinta usuários examinados, dezenove expressaram o segredo como um fator essencial em suas relações. Esses usuários foram identificados por apelidos como "Macho Discreto", "Discreto", "No Sigilo", "Sigilo", "Na encolha" e solicitavam discrição em seus textos de apresentação (Monica e Costa, 2020, p. 109).

Essas referências iniciais também continham discursos como "macho discreto e fora do meio", "não sou assumido, curto no sigilo", "casado, curto na encolha", "Discreto, não sou e não curto afeminados", "macho afim de machos no sigilo", que destacavam a centralidade da confiança nas interações, bem como, em alguns casos, um distanciamento em relação à homossexualidade ou ao que é feminino. Além disso, dos dezenove perfis, dezessete utilizavam fotos mostrando apenas o torso nu, sem revelar completamente o rosto, enquanto dois não possuíam imagens (Monica e Costa, 2020, p. 109).

Não é surpreendente que os ambientes destinados ao público heterossexual e àqueles voltados para pessoas com diversidades sexuais sejam distintos. Susan McKinnon (2012, p. 120-144) explica que as diversas expressões da sexualidade são estruturadas conforme valores socioculturais específicos relacionados aos corpos, às substâncias corporais e ao gênero, além das concepções sobre outros elementos relevantes para uma existência respeitável.

Um passo fundamental para compreender a vida sexual de uma sociedade, independentemente das tecnologias disponíveis — que são atualmente numerosas —, é entender o que é desaprovado nesse domínio. O conceito de promiscuidade, especialmente dentro do contexto do binarismo entre homens e mulheres, varia de acordo com a lógica cultural específica que organiza a sexualidade em diferentes sociedades (McKinnon, 2012, p. 120-144).

Portanto, chama atenção que um aplicativo com tratamento de dados pessoais, especialmente caros aos seus usuários, seja alvo de vazamentos de informações ao redor do mundo. De fato, isso pode ocorrer por usuários contra usuários ou por responsabilidade da empresa ao tratar os dados pessoais de sua plataforma. Nesse último sentido, o “Grindr” se destaca negativamente.

Em 2018, a organização se envolveu em uma séria polêmica ao divulgar dados pessoais com outras empresas, incluindo status de HIV dos clientes. A princípio, a denúncia foi feita por uma ONG norueguesa chamada SINTEF e divulgada pelo site Axios. Os dados eram enviados juntamente com informações de GPS, telefone e e-mail do usuário para duas empresas contratadas para monitorar o uso do aplicativo e melhorá-lo (BBC, 2018).

O “Grindr” confirmou o compartilhamento, mas afirmou que os dados eram criptografados e negou que informações sensíveis eram compartilhadas com anunciantes. Apesar de supostamente encerrar essas transferências de materiais coletados, não existiram maiores esclarecimentos sobre o alcance da quebra de registros (BBC, 2018).

Outros escândalos de vazamento já atingiram o aplicativo. Em 2020, ele foi notificado pelo governo brasileiro por vender a terceiros os dados de seus usuários. A Secretaria Nacional do Consumidor do Ministério da Justiça pediu esclarecimentos, tendo em vista suspeitas de que conhecimentos sobre idade e orientação sexual seriam sistematicamente utilizados pela empresa para programar seus anúncios (O Popular, 2020).

Uma multa também foi aplicada à empresa, em 2020, pelo governo norueguês. A razão se encontrava no fornecimento de dados pessoais sobre orientação sexual, idade e localidade aos anunciantes da plataforma. A ideia era direcionar produtos voltados para população LGBTQIAPN+ de maneira não explícita (G1, 2021). Em 2024, atualizações apontam que o valor da multa foi de 65 milhões de coroas norueguesas, equivalente a aproximadamente cinco milhões e seiscentos e cinquenta mil euros ou seis milhões e cem mil dólares americanos, foi imposta ao Grindr (Kaldestad, 2024).

As consequências de ser identificado em um aplicativo “queer” são diversas, mas potencialmente drásticas. Um padre que deixa o cargo (IG Queer, 2021), um ator famoso que tem suas características íntimas expostas em sites de fofoca de todo país (Permuy, 2023), um senador que sai do cargo (G1, 2011) e diversos atletas olímpicos de países com leis contra homossexualidade repreendidos (Furtado, 2021) são exemplos do que ocorre quando pessoas são expostas por seus perfis em redes sociais íntimas.

Com o avanço da tecnologia e a popularização das plataformas online, tornou-se essencial garantir a segurança e a privacidade dos indivíduos ao explorarem sua sexualidade na internet. É nítido que a liberdade sexual, como um direito fundamental, deve ser protegida e promovida no mundo físico e no ambiente virtual. Assim, é preciso que as empresas

controladoras exerçam sua responsabilidade pela confidencialidade e pela proteção de informações sensíveis.

2. A VULNERABILIDADE AMOROSA E SEXUAL DE PESSOAS LGBTQIAPN+ E O TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS NO ORDENAMENTO JURÍDICO BRASILEIRO

Atualmente, a sociedade está voltada diretamente para informação. Isso é fruto de um percurso histórico em que o valor econômico de certos fatores se alterou, especialmente nas últimas décadas do século passado. Dentre as várias formas de organização social, em cada período, houve um elemento central que impulsionou seu desenvolvimento, sendo a estruturação desse elemento o fator determinante para os marcos históricos correspondentes (Castells, 2011, p. 87-216).

Na sociedade agrícola, a fonte de riqueza era a terra e a prática do escambo, ou seja, a troca de produtos agrícolas impulsionava a economia e ocasionou o surgimento do comércio. Em seguida, a criação das máquinas a vapor e da eletricidade desempenhou um papel central na produção industrial e na geração de riqueza, caracterizando a sociedade industrial (Castells, 2011, p. 87-216).

Posteriormente, após a Segunda Guerra Mundial, os serviços ganharam destaque na estrutura socioeconômica. A chamada sociedade pós-industrial não era definida pelo que se produzia, mas pelos serviços a serem oferecidos. Setores como bancos, seguros, educação, assistência médica e consultoria jurídica se tornaram impulsionadores da economia (Castells, 2011, p. 87-216).

Agora, especialmente nas duas últimas décadas, a sociedade está imersa em uma nova forma de organização em que a informação é o ponto focal para o desenvolvimento econômico, substituindo os recursos que antes estruturavam as sociedades agrícola, industrial e pós-industrial (Castells, 2011, p. 87-216).

É importante considerar esse contexto para compreender a vulnerabilidade digital inerente ao usuário dos aplicativos de relacionamento amorosos e sexuais. O fornecimento de informações pessoais gera um interesse para além das interações óbvias para as quais o “Grindr” se volta. Nesse sentido, a autora Shoshana Zuboff (2019, p. 24-28) esclarece a dinâmica social ocasionada pelo crescente poder de empresas envolvidas com essas novas tecnologias.

Para a autora, há um sistema vigente que busca adquirir fontes cada vez mais preditivas de comportamento, pelas vozes, personalidades e emoções dos seres humanos. Para operar, os controladores desenvolvem processos automatizados para conhecer e moldar comportamento em escala, isto é, transformar conhecimento em poder. Esse novo tipo de administração busca conhecer e direcionar o comportamento humano em prol do interesse de terceiros (Zuboff, 2019, p. 24-28).

Assim, passa a existir uma arquitetura computacional ubíqua composta por dispositivos, coisas e espaços "inteligentes" conectados em rede para exercer seu poder instrumental (Berberí e Fracaro, 2022, p. 9). Voltadas para um capitalismo de vigilância, as empresas estão envolvidas em uma intensificação contínua dos meios de modificação comportamental e um aumento do poder instrumental (Zuboff, 2019, p. 24-28).

Não se reflete sobre uma tecnologia pró-social, inclusiva e propensa à democratização do conhecimento. As empresas (como Google, Facebook, Microsoft e Amazon) criam seus produtos e serviços atrativos que seduzem os usuários para operações extrativas por meio de experiências pessoais coletadas e transformadas em meios para benefício de terceiros (Zuboff, 2019, p. 24-28).

Os clientes, ou usuários, passaram a ser as fontes cruciais do superávit do capitalismo ao serem objetos de uma sofisticada extração de dados da qual é cada vez mais difícil escapar. Isso explica a importância de regulamentar a proteção de dados pessoais, em especial em redes sociais que tratam de conteúdos da intimidade humana (Zuboff, 2019, p. 24-28).

Toda essa hierarquia, se mistura com outra, existente há tempos, quando se fala em interações sexuais por meios virtuais de pessoas LGBTQIAPN+. Isso porque é preciso entender que a relação entre corpos e poder é complexa, e a homossexualidade é historicamente qualificada por julgamentos sociais e culturais profundamente intrincados e negativos.

Por isso mesmo, o renomado Michel Foucault (1988, p. 79-109) se dedicou ao estudo aprofundado da correlação entre esses fatores nas obras intituladas como “História da Sexualidade”, em que o sexo nos últimos três séculos é comentado. De acordo com a teoria do autor, durante o século XIX, o sexo se transformou em um objeto de estudo científico, marcado por uma biologia da reprodução e uma medicina do sexo. O foco era uma visão purificada e neutra do sexo na ciência, que determinava o que era considerado aberrante, perverso, extravagante, patológico ou mórbido.

O dispositivo da sexualidade é um dos principais conceitos teóricos de Foucault. Ele explora a dinâmica entre poder e sexualidade abrangendo práticas de rejeição, exclusão, recusa, bloqueio e ocultação. Pelo discurso jurídico, se promove um ciclo de interdição do sexo, seguindo uma lógica de censura onde coexistem três formas de proibição: o não permitido, o impedido de ser dito e o negado de existir (Foucault, 1988, p. 79-109).

Dessa maneira, é possível concluir que há uma importante vulnerabilidade em destaque quando os dados pessoais de usuários do “Grindr” são indevidamente expostos. Essa comunidade enfrenta diversos tipos de violências, incluindo agressões físicas, violência verbal, discriminação institucional, violência sexual e violência familiar. Essas agressões afetam a saúde emocional, a segurança e o exercício de direitos.

O preconceito contra pessoas do grupo LGBTQIAPN+ é evidente. Estudos da Acontece Arte e Política LGBTQI+ junto a ANTRA – Associação Nacional de Travestis e Transexuais e a ABGLT – Associação Brasileira de Lésbicas, Gays, Bissexuais, Travestis, Transexuais e Intersexos apontam aumento no total de mortes em crimes de ódio contra esses indivíduos.

Em 2020, foram registrados 237 óbitos, enquanto, em 2021, foram 316 e, em 2022, foram 273. Os homicídios não são o único tipo de violência contra essas pessoas, sendo que elas podem ocorrer no ambiente doméstico, em vias públicas, no local de trabalho, entre outros (Observatório de Mortes e Violências LGBTQI+ no Brasil, 2023).

De acordo com Florencia Luna (2009, p. 261-264), por meio da metáfora das capas, a vulnerabilidade é dinâmica e contextual, de modo que certos elementos sociais e circunstanciais se acumulam e exigem estratégias para retirar ou amenizar aspectos negativos da vulnerabilidade, se possível.

Em casos concretos de consumo virtual, a vulnerabilidade pode ser informacional, quando combinada com a falta de conhecimento do consumidor em relação às transações de consumo, e sofre mudanças com as inovações do ambiente virtual. A escassez ou a baixa qualidade das informações fornecidas se alia a uma falta de habilidade ou familiaridade com o ambiente digital (Marques; Mucelin, 2022, p. 22-23).

Para além, identifica-se uma vulnerabilidade neuropsicológica devido à repetição e grande quantidade de dados presentes no espaço virtual, o que pode levar à confusão, estimular certas reações e até mesmo alienar os mais vulneráveis, resultando em decisões incorretas. Essa

vulnerabilidade surge a partir de estímulos sensoriais ou emocionais transmitidos pelo meio digital e das respostas dos consumidores, assim como das estratégias da economia comportamental que exploram os gatilhos humanos e utilizam incentivos para reduzir a cautela nas transações online (Marques; Mucelin, 2022, p. 22-23).

Finalmente, é importante considerar como as práticas sociais implicam em uma abordagem adicional da vulnerabilidade digital relacionada à dependência ou submissão na manutenção ou no acesso a um determinado serviço ou produto fornecido por plataformas. Essa dependência é considerada uma condição que pode afetar a plena fruição da vida e a autorrealização na sociedade contemporânea (Marques; Mucelin, 2022, p. 22-23).

Nesse íterim, Bruno Ricardo Bioni (2019, p. 95) defende que o direito à proteção de dados pessoais integra o rol não taxativo de direitos da personalidade no ordenamento jurídico brasileiro. Trata-se de proteção jurídica voltada para o desenvolvimento da pessoa humana, não apenas em relação aos direitos e deveres. O foco é garantir a proteção legal de objetos que contribuam para esse propósito, o que abre margem para o reconhecimento da proteção de dados pessoais.

A proteção de dados pessoais pressupõe um dado atrelado à esfera de uma pessoa, isto é, uma informação caracterizada como pessoal por projetar, estender ou dimensionar o seu titular. Uma vez que as atividades de processamento de dados está presente no cotidiano de todos, surge uma nova forma de compreender a identidade, que justifica uma compreensão própria de direito da personalidade (Bioni, 2019, p. 97-98).

Perante a relevância do tema, o legislador brasileiro elaborou uma legislação própria, além de enquadrar tal direito como fundamental no inciso LXXIX do artigo 5º da Constituição Federal de 1988. A Lei nº 13.709/2018, ou Lei Geral de Proteção de Dados Pessoais (LGPD), qualifica o dado pessoal aquele que revela “informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2018).

No entanto, há uma qualificação a mais quando se fala em dados pessoais presentes em aplicativos de relacionamentos amorosos e sexuais. A lei é clara ao definir como dados pessoais sensíveis aqueles “sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural” (Brasil, 2018).

Ao ser qualificado dessa forma, a legislação exige uma proteção acentuada. A Seção II sobre o tratamento de dados pessoais sensíveis, determina que tal somente poderá ocorrer:

- I - quando o titular ou seu responsável legal *consentir*, de forma específica e destacada, para finalidades específicas;
- II - *sem fornecimento de consentimento do titular*, nas hipóteses em que for indispensável para:
 - a) cumprimento de obrigação legal ou regulatória pelo controlador;
 - b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
 - c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
 - d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
 - e) proteção da vida ou da incolumidade física do titular ou de terceiro;
 - f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
 - g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (Brasil, 2018, grifo nosso).

Os dados pessoais sensíveis são uma categoria especial de dados pessoais porque possuem potencial de expor indivíduos a discriminação. Informações como orientação sexual, religião, política, raça, saúde e filiação sindical levantam preocupações sobre a possibilidade de desvantagens com base nesses aspectos pessoais. Mesmo dados aparentemente insignificantes podem revelar informações sensíveis quando combinados com técnicas de análise de dados (Bioni, 2019, p. 118-119).

É por isso que a proteção de dados pessoais aqui debatida envolve a garantia de igualdade, mas, principalmente, uma medida de combate à discriminação. As leis de proteção de dados, incluindo as leis brasileiras, oferecem uma proteção mais rigorosa para dados sensíveis, com o objetivo de evitar práticas discriminatórias. Essa salvaguarda busca permitir que os indivíduos se relacionem e se realizem na sociedade sem serem prejudicados pela lógica da sociedade de informação (Bioni, 2019, p. 118-119).

Importante destacar a importância da autodeterminação informativa, que consiste na possibilidade do indivíduo de determinar a finalidade para as quais seus dados pessoais serão ou não utilizados. Nesse sentido, a Lei Geral de Proteção de Dados, por exemplo, prevê o direito de revogar consentimento de modo unilateral, reconhecendo o poder do titular de controlar sua

esfera privada. Essa prerrogativa deve ser respeitada sem restrições injustificadas, garantindo o poder de decisão do indivíduo sobre o tratamento de seus dados pessoais (Doneda, 2020, p. 327).

Em última análise, a proteção de dados pessoais desempenha um papel fundamental na promoção da liberdade e no desenvolvimento da personalidade, contribuindo para a igualdade nas relações sociais. Assim sendo, importante compreender o que os termos de uso de um aplicativo de relacionamentos amorosos e sexuais, que transparece uma clara vulnerabilidade aos seus usuários, revela sobre seu tratamento de dados pessoais qualificados como sensíveis (Bioni, 2019, p. 118-119).

3. OS TERMOS DE USO DO “GRINDR” E A LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS: RESPONSABILIDADE DA PLATAFORMA PELO TRATAMENTO DE DADOS PESSOAIS SENSÍVEIS DE USUÁRIOS

Na Play Store³ (s.d.), o “Grindr” apresenta algumas considerações sobre segurança dos dados, conforme exigido pela plataforma que disponibiliza a opção de baixar aplicativos. Inicialmente, o desenvolvedor afirma que não compartilha dados do usuário com outras empresas ou organizações, o que, por si só, contradiz práticas da empresa denunciadas anteriormente.

Quanto aos dados coletados, especifica a coleta de informações sobre local aproximado e local exato, informações pessoais de endereço de e-mail, ID’s de usuários, raça e etnia, orientação sexual, informações financeiras de histórico de compras, informações sobre saúde, mensagens, fotos, vídeos, gravações de voz ou som, atividade no aplicativo, interações no aplicativo, informações e desempenho do aplicativo e identificadores do dispositivo. Ao final, é comunicado ao usuário que os dados são criptografados em trânsito, isto é, os dados são transferidos por uma conexão segura e é possível solicitar a exclusão (Play Store, s.d.).

Entretanto, não existe registro sobre a data em que essas informações foram disponibilizadas na Play Store. Isso é relevante porque, em 01 de julho de 2023, o “Grindr” disponibilizou e passou a operar com uma nova política de privacidade e de cookies. Nela, alguns pontos são especificados, como os dados que são coletados pela plataforma:

³Play Store é a loja oficial de plataformas para dispositivos Android, em que os usuários podem baixar aplicativos, jogos e conteúdos digitais.

A (DES)PROTEÇÃO DE DADOS PESSOAIS SENSÍVEIS NOS TERMOS DE USO DO “GRINDR”: A VULNERABILIDADE DE USUÁRIOS LGBTQIAPN+ EM APLICATIVOS DE RELACIONAMENTOS AMOROSOS E SEXUAIS - *Anna Luísa Braz Rodrigues*

Informações Pessoais que você precisa fornecer. Quando você cria uma conta, exigimos que você forneça Informações Pessoais limitadas, como *e-mail ou número de telefone e data de nascimento*, para confirmar que você é adulto.

Informações Pessoais que você tem a opção de fornecer. Você decide quais Informações Pessoais são fornecidas em seu perfil público (“Perfil do Grindr”). As Informações Pessoais que você inclui em seu Perfil do Grindr são designadas como suas “Informações de Perfil”, as quais são compartilhadas com outros usuários dos Serviços do Grindr (a “Comunidade do Grindr”). Por exemplo, você pode optar por compartilhar *sua localização, seus status de HIV e vacinação, fotos e vídeos*. No entanto, deixar de fornecer certas informações pode afetar a funcionalidade de certos Serviços do Grindr. Se quiser, você também pode fornecer Informações Pessoais para feedback e serviços de suporte ao cliente ou quando concordar em participar de pesquisas. Esses dados variam de pesquisa para pesquisa. (...)

Informações Pessoais que recebemos do seu dispositivo quando você utiliza as Propriedades do Grindr. Para manter e melhorar as Propriedades do Grindr, coletamos Informações Pessoais, tais como *atividade do usuário, informações de hardware e software e cookies*, bem como aproveitamos outras tecnologias tais como web beacons, kits de desenvolvimento de software (Software Development Kits, SDKs), armazenamento local e arquivos de log.

Informações Pessoais que recebemos de terceiros. O Grindr coleta informações limitadas de terceiros. Por exemplo, podemos coletar Informações Pessoais de processadores de pagamento, parceiros de informações de uso de aplicativo e rastreamento de sites, parceiros de autenticação (por exemplo, Google e Facebook), parceiros de aprendizado de máquina e nosso provedor de plataforma de gestão de consentimento (Grindr, 2023, grifo nosso).

Como observado anteriormente, muitos dados pessoais coletados pelo aplicativo se qualificam como sensíveis pela legislação e, para além, outros dados pessoais que não se qualificam como sensíveis, se conhecidamente decorrentes da plataforma, indicarão informações íntimas devido ao caráter inerente da plataforma. Ter um perfil no “Grindr” leva a dedução de uma sexualidade ou identidade de gênero diverso.

Desse modo, adota-se o parâmetro legal do tratamento de dados pessoais sensíveis para avaliar como a plataforma trata as informações dos usuários. De início, a empresa indica que a coleta de dados é feita por algumas razões pré-determinadas. Os objetivos de oferecer os serviços associados à conta “Grindr”, responder perguntas, oferecer suporte, realizar pesquisas ou obter feedback voluntário sobre propriedades do aplicativo não apresentam grandes controvérsias.

No entanto, ao citar “proteger nossos interesses como empresa” há uma previsão abrangente e inadequada, já que o consentimento do usuário não é específico e destacado, para finalidades específicas, como pressupõe o artigo 11 da LGPD. Ora, quais interesses serão

protegidos? De que modo os dados pessoais dos consumidores serão utilizados? Isso não é dito, de nenhum modo, tornando a previsão sem efeito legal, já que também não atende às hipóteses de dispensa de consentimento.

Ao falar sobre o aprendizado de máquina e tomada de decisão automatizada, a controladora atribui essas funcionalidades ao desfrute de recursos da plataforma pelo próprio usuário. A própria empresa, além disso, disponibiliza o significado desses conceitos em seu site:

Aprendizado de máquina (em inglês, machine learning) - a capacidade de um dispositivo de executar funções normalmente associadas à inteligência humana, como o raciocínio, o aprendizado e o autoaprimoramento.

Criar um perfil de dados (em inglês, profiling) - avaliar certos aspectos relacionados a uma pessoa, incluindo seus interesses, preferências e comportamentos, a partir de um processo automatizado de processamento de dados pessoais (por exemplo, usar tecnologia para descobrir os interesses e preferências de alguém com base no comportamento que a pessoa tem na internet).

Tomada de decisão automatizada - tomar uma decisão em relação a uma pessoa com meios exclusivamente automáticos (ou seja, tomar decisões por meios tecnológicos, sem qualquer envolvimento humano no processo de tomada de decisão) (Grindr, s.d., grifo nosso).

Sobre o tema, apesar de controverso, não se conclui por descumprimentos a priori da empresa. Relevante, entretanto, ressaltar direito previsto no artigo 20 da LGPD, que assegura a possibilidade de solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem interesses do titular, incluídas as decisões destinadas a definir o perfil pessoal, profissional, de consumo e de crédito ou os aspectos de personalidade. Em caso de não oferecimento dessa oportunidade, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais (Brasil, 2018).

Em seguida, tendo em vista o escândalo referente aos usuários com HIV ocorrido em 2018, o “Grindr” se preocupa em esclarecer que:

Para evitar dúvidas, o Grindr só compartilha o status de HIV, a Data do Último Teste e o status de vacinação com Provedores de Serviços necessários, tais como empresas que hospedam dados em nosso nome (ou seja, Amazon Web Services) ou ajudam no processamento de solicitações de acesso aos dados que você inicia (ou seja, PartnerHero) – não compartilhamos essas informações com nenhuma empresa de publicidade (Grindr, 2023).

Entretanto, ao citar que dados pessoais, no geral, serão utilizados para “permitir o uso de cookies e outras tecnologias por parte de parceiros terceiros de anúncios e marketing para fins de veiculação de anúncios para usuários gratuitos dos serviços”, abre-se margem para um grave descumprimento legal. O aplicativo confirma que informações sobre saúde são coletadas, sem diferenciá-las ativamente em seu tratamento, e, conforme artigo 11, §4º, da LGPD, é vedada a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica (Brasil, 2018).

Assim, o “Grindr” claramente desrespeita essa previsão sobre o tratamento de dados pessoais sensíveis ao apontar expressamente que “compartilha Informações Pessoais com vários parceiros para oferecer as Propriedades do Grindr, como (...) Parceiros de Publicidade/Marketing que ajudam a facilitar experiências de publicidade (por exemplo, AppLovin) e Outros Parceiros (...)” (Grindr, 2023).

O tempo de armazenamento desses dados pessoais também se mostra completamente incerto. A empresa diz apenas que as guardará pelo tempo necessário para cumprir os fins para os quais as informações foram coletadas, mas deixa claro que serão suporte para relatórios, métricas e estatísticas internas. E, mesmo ao apontar um tempo de dois anos após a exclusão da conta para dados de identificação de dispositivo, há uma ressalva sobre a manutenção desse tratamento por períodos mais longos para fins legais ou de segurança (Grindr, 2023).

Embora não haja uma previsão legal clara sobre o tempo de manutenção das informações coletadas por controladores, é incoerente considerar que o consentimento dado pelo titular não possua um prazo razoável definido e que o usuário não tenha possibilidade de ponderar pela exclusão por sequer saber que esses dados ainda são tratados. Há uma omissão da legislação, mas é claro que a prática da empresa é nebulosa e reprovável nesse aspecto.

Em relação à exclusão de dados, contudo, há respeito ao direito de autodeterminação informativa quando a plataforma prevê ampla exclusão de dados, negativa de utilização para fins comerciais e revogação de consentimento a qualquer tempo (Grindr, 2023). A Lei Geral de Proteção de Dados garante controle sobre dados pessoais ao cidadão, indo além do consentimento e assegurando que o fluxo informacional atenda às suas expectativas (Bioni, 2019, p. 39-40).

Para mais, ao acessar o site oficial traduzido para português, o “Grindr” apresenta a aba “Segurança e Privacidade” com o total de 21 artigos de esclarecimento sobre suas práticas.

Nesse ponto, é relevante considerar que a proteção de dados pessoais em aplicativos de relacionamentos sexuais e amorosos alcança a responsabilidade pela adequação e segurança do tratamento de dados da própria empresa e também pelas boas práticas contra o vazamento de dados entre usuários e terceiros (Grindr, s.d.).

Em relação ao espaço de segurança entre os usuários, existe uma política de confirmação de idade e identidade. O aplicativo está restrito aos maiores de 18 anos e, uma vez que houver suspeita sobre o cumprimento dessa regra, o usuário precisará preencher um formulário de comprovação com diversos dados pessoais, entre eles um documento pessoal a ser excluído após análise:

Se você criou sua conta com um endereço de e-mail e senha, inclua o seguinte no envio do formulário: O endereço de e-mail associado à sua conta Grindr, Uma foto nítida sua segurando um pedaço de papel com o endereço de e-mail escrito à mão, Uma foto nítida sua segurando um documento de identidade válido emitido pelo governo mostrando sua data de nascimento e Uma captura de tela da mensagem de suspensão que você recebeu.

Se você criou sua conta por meio de terceiros (como por exemplo, pela Apple, Google ou Facebook), inclua o seguinte no envio do formulário: Uma foto clara de você segurando um pedaço de papel com o ID do seu dispositivo escrito à mão (você pode encontrar o ID do seu dispositivo listado na tela que você vê atualmente ao abrir o aplicativo Grindr), Uma foto nítida sua segurando um documento de identidade válido emitido pelo governo mostrando sua data de nascimento e Uma captura de tela da mensagem de suspensão que você recebeu.

Nós agradecemos sua cooperação. Observe que seu documento de identidade emitido pelo governo é excluído imediatamente do nosso sistema após verificarmos sua idade (Grindr, s.d., grifo nosso).

Ademais, há diversas orientações que visam a instruir o usuário contra golpes e a favor de contato seguro com os demais. Dicas sobre proteção da própria identidade, configurações das funcionalidades de localização, modos de denunciar e bloquear perfis e até prática segura de sexo são elaboradas. O “Grindr”, a princípio, cumpre com o dever de informação aos usuários (Grindr, s.d.).

No entanto, essas informações se apresentam de forma esparsa e pouco clara no site da empresa, cujo links são direcionados internamente no aplicativo. Apesar de não serem encontrados precedentes sobre uma possível responsabilização por atos lesivos de terceiros que se valem das funcionalidades da plataforma, cabe propor que as empresas se atentem aos aspectos de proteção de dados pessoais sensíveis pelos mecanismos tecnológicos disponíveis.

Um conceito útil a essa discussão é o “privacy by design”, que objetiva integrar a privacidade como um aspecto considerado desde o início de qualquer modelo de negócio, incorporando-a à arquitetura técnica dos produtos e serviços. Embora tenha se popularizado com a implementação da GDPR, em 2018, o conceito e a sua aplicação remontam aos anos 80 (Camargo, 2023, p. 107-110).

A metodologia proposta por Ann Cavoukian vai além e pressupõe que a proteção da privacidade não depende apenas de requisitos técnicos. Para tal, ela estabelece sete princípios primordiais: proatividade, privacidade como configuração padrão, privacidade incorporada no design, funcionalidade integral, segurança de ponta a ponta, visibilidade e transparência e respeito à privacidade do usuário (Camargo, 2023, p. 107-110).

Em suma, esses princípios buscam prevenir incidentes de privacidade, garantir que a privacidade seja considerada desde o início do desenvolvimento, eliminar o dilema entre segurança e funcionalidade, assegurar a segurança em todas as etapas, promover a transparência e respeitar os direitos dos usuários em relação à privacidade (Camargo, 2023, p. 107-110).

Essa perspectiva responde a obrigação legal imposta pelo artigo 46 da LGPD, que fala sobre adotar medidas de segurança, técnicas e administrativas desde a fase de concepção do produto ou do serviço até a sua execução (Brasil, 2018). O “Grindr”, por exemplo, poderia investir em maiores bloqueios de cópia e registro dos conteúdos trocados entre usuários, como senhas para acesso ao aplicativo, telas pretas automáticas na tentativa de “prints” e proibição de registro interno do telefone de fotos e vídeos íntimos.

No geral, os termos de uso contêm especificações sobre a norma europeia de proteção de dados pessoais, a saber, o Regulamento Geral de Proteção de Dados (RGPD), aplicáveis exclusivamente aos usuários residentes na União Europeia (UE) e no Espaço Econômico Europeu (EEE). Uma consideração genérica relativa ao ordenamento jurídico brasileiro foi incluída no site apenas em 2023 e se resume a uma única frase: “se você residir no Brasil ou tiver dúvidas relacionadas à Lei Geral de Proteção de Dados Pessoais (LGPD) 13.709/2018, pode entrar em contato com o DPO do Grindr no Brasil por meio do nosso site aqui”.

O aplicativo estudado faz questão de citar que “nenhum método de transmissão pela internet, ou método de armazenamento eletrônico, é totalmente seguro, e a Grindr não pode garantir a segurança de suas Informações Pessoais”, e é categórica: “não podemos garantir confidencialidade, anonimato, nem segurança pessoal em absoluto” (Grindr, 2023).

A título de maiores esclarecimentos, então, é importante citar o posicionamento jurisprudencial brasileiro sobre o desrespeito aos pressupostos e as falhas no tratamento de dados pessoais sensíveis, na vigência da LGPD, salientando, de antemão, que esse não está consolidado e se mostra em aberto sobre questões presentemente tratadas.

Em especial, se destaca, no que cabe, a Ação Direta de Inconstitucionalidade 6387, julgada em 07 de maio de 2020, pelo Supremo Tribunal Federal, sobre o compartilhamento de dados de usuários de serviço telefônico com o Instituto Brasileiro de Geografia e Estatística com fins de averiguar condições sanitárias decorrentes da pandemia de COVID-19 (Supremo Tribunal Federal, 2020, p. 1-3).

Há, primeiramente, um claro reconhecimento do direito à proteção de dados pessoais como direito fundamental constitucionalmente colocado e justificado, decorrente de evoluções históricas do direito à privacidade e autodeterminação informativa, inclusive com citações ao marco teórico adotado no presente trabalho (Supremo Tribunal Federal, 2020, p. 1-3).

Apesar de reconhecer a possibilidade legal de interesse legítimo de compartilhamento por razões sanitárias, o acórdão entende que, ao não definir apropriadamente como e para que serão utilizados os dados coletados, há um desrespeito quanto ao devido processo legal por não oferecer condições de avaliação quanto à adequação e necessidade da medida pública (Supremo Tribunal Federal, 2020, p. 1-3).

Para além, quanto ao tempo de manutenção dos dados pessoais, considerou-se excessiva a conservação de dados pessoais coletados, pelo ente público, por trinta dias após a decretação do fim da situação de emergência de saúde pública, por ser manifestamente excedente ao estritamente necessário para o atendimento da sua finalidade declarada (Supremo Tribunal Federal, 2020, p. 1-3).

No âmbito do Superior Tribunal de Justiça (2023, p. 1-2), ainda, o julgado do Agravo de Recurso Especial de nº 2.130.619 - SP (2022/0152262-2) se mostrou relevante por firmar a tese de que “o vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável”.

No caso em questão, a tese foi firmada em relação ao pedido de indenização por danos morais de uma mulher contra uma empresa de energia elétrica que compartilhou indevidamente informações como nome completo, número de identidade, gênero, data de nascimento, idade,

telefone fixo, telefone celular e endereço, além daquelas relativas ao contrato de fornecimento de energia elétrica (Superior Tribunal de Justiça, 2023, p. 10).

É questionável, entretanto, quais são os caminhos que o tribunal tomará em relação ao vazamento sistemático de dados pessoais e, em específico, qual será a interpretação sobre a presunção de danos no caso de lesão ao direito pela divulgação indevida de dados pessoais sensíveis, que possuem proteção especial e foram considerados como elencados em rol taxativo na LGPD. A dúvida se dá, em especial, pelo entendimento subentendido dado pelo próprio acórdão, ao destacar que sua tese de dano não presumível não se aplica aos dados pessoais sensíveis:

O vazamento de dados pessoais, a despeito de se tratar de falha indesejável no tratamento de dados de pessoa natural por pessoa jurídica, não tem o condão, por si só, de gerar dano moral indenizável. Ou seja, o dano moral não é presumido, sendo necessário que o titular dos dados comprove eventual dano decorrente da exposição dessas informações. *Diferente seria se, de fato, estivéssemos diante de vazamento de dados sensíveis, que dizem respeito à intimidade da pessoa natural* (Superior Tribunal de Justiça, 2023, p. 10-11, grifo nosso).

Cabe citar que novas iniciativas legislativas são veiculadas, tendo em vista a dinâmica complexa com que os relacionamentos virtuais se dão. Um exemplo é o Projeto de Lei nº 2.811/2023, que “estabelece medidas de segurança na prestação dos serviços oferecidos pelos aplicativos de relacionamento e atribui responsabilidades às empresas que prestam esses serviços” (Brasil, 2023).

Nos breves artigos propostos, são previstas medidas de segurança e responsabilidades para as aplicações de internet de relacionamento, incluindo verificação de identidade dos usuários, detecção e bloqueio de perfis falsos ou abusivos, canais de denúncia e medidas educativas sobre segurança. O descumprimento da lei poderia resultar em sanções, como advertência, multa, suspensão temporária ou proibição das atividades da empresa. Além disso, os órgãos responsáveis pela fiscalização ficariam encarregados de combater os crimes digitais e proteger as vítimas (Brasil, 2023).

Observando novamente uma lógica maior, Gayle Rubin (2006, p. 14-21) aponta que os sistemas sexuais modernos exercem uma influência significativa na formação pessoal, impondo características restritivas sobre o ideal de sujeito sexual. Indivíduos que se identificam de forma diversa e interagem em redes sociais como o “Grindr” estão sujeitos a esses

juízos, uma vez que o aplicativo é especificamente projetado para facilitar o encontro dessas pessoas que são censuradas na “vida real”.

Aqueles no topo da pirâmide valorativa são geralmente certificados com saúde mental, têm mobilidade social e física e recebem apoio institucional. Por outro lado, indivíduos identificados pela sigla LGBTQIAPN+ e outros grupos marginalizados são frequentemente estigmatizados como problemáticos mentalmente, criminosos ou economicamente desfavorecidos (Rubin, 2006, p. 14-21).

A sexualidade que é considerada aceitável, padrão e intrinsecamente correta é aquela heterossexual, dentro do matrimônio, monogâmica, voltada para a reprodução, sem transações comerciais, envolvendo apenas dois parceiros, baseada em relações estáveis e entre pessoas da mesma geração. Qualquer forma de pornografia, objetos fetichistas, brinquedos sexuais ou papéis de gênero que não sejam estritamente masculinos ou femininos são proibidas (Rubin, 2006, p. 14-21).

Em contraste, a sexualidade vista como inaceitável, não padrão e não natural é aquela homossexual, fora do casamento, promíscua, não focada na procriação, comercial, solitária, envolvendo múltiplos parceiros, casual, com diferenças geracionais. O uso de pornografia, objetos fetichistas, brinquedos sexuais ou papéis menos convencionais de gêneros também é repudiado (Rubin, 2006, p. 14-21).

É por isso que estar no “Grindr” adquire significados mais profundos sobre sexualidade, pois, apesar dos avanços tecnológicos e mudanças nas concepções sexuais, o preconceito ainda persiste como uma realidade. Especificamente na sociedade brasileira, embora inclusiva em muitos aspectos, ainda prevalecem valores culturais que subestimam o afeto homossexual e reprimem os desejos sexuais de pessoas com identidades sexuais diversas.

Portanto, entende-se que o “Grindr” está presente e tem uma importância maior na proteção dos dados pessoais comparado a outras empresas. Essas informações são facilmente classificadas como sensíveis pela legislação, mas é essencial aprofundar esse conceito a partir da realidade e dentro de um contexto prático.

CONSIDERAÇÕES FINAIS

O “Grindr” oferece uma plataforma para que indivíduos da comunidade LGBTQIAPN+ possam conhecer e interagir com outros membros, buscando conexões

emocionais e encontros íntimos. No entanto, existem preocupações em relação à proteção de dados pessoais fornecidos ao aplicativo, que constitui direito garantido constitucionalmente no artigo 5º, LXXIX, e em legislação própria por meio da Lei Geral de Proteção de Dados Pessoais.

A empresa controladora enfrentou históricos de vazamentos de dados sem esclarecimentos suficientes, o que levanta questões sobre a segurança e a privacidade dos usuários. Essa situação é particularmente relevante, pois o aplicativo lida com dados pessoais sensíveis, relacionados à orientação sexual e identidade de gênero, que podem colocar os usuários em situações de discriminação.

Ser parte do grupo LGBTQIAPN+ implica em uma camada de vulnerabilidade importante, tornando essencial refletir sobre a salvaguarda desse banco de informações nesse contexto. Conforme o marco teórico adotado, o direito à proteção de dados pessoais é um direito de personalidade autônomo e fundamental.

Apesar de contemplar parcialmente a autodeterminação informativa, ao mencionar explicitamente a retificação e a exclusão de dados e a revogação de consentimento, o “Grindr” falha ao não fazer uma diferenciação adequada entre dados pessoais e dados pessoais sensíveis.

Essa falta de distinção é preocupante, especialmente quando se trata das informações relacionadas à saúde. A política de privacidade permite, indevidamente, que esses dados pessoais sensíveis sejam utilizados para vantagens econômicas e compartilhados com terceiros, o que desrespeita os parágrafos do artigo 11 da LGPD.

No mais, embora haja instruções informativas no aplicativo, inclusive com supervisão em relação à idade dos usuários, é evidente que as diretrizes podem ser aprimoradas por meio da implementação de métodos de “privacy by design”, por exemplo.

Conclui-se, então, que os termos de uso do “Grindr” revelam uma falta de atenção ao ordenamento jurídico interno, pois não fazem referências diretas à LGPD. Além disso, a forma como o tratamento de dados pessoais ocorre não é adequadamente definida, gerando incertezas para os usuários e um consentimento inválido nos termos legais.

Ademais, não são descartáveis os posicionamentos jurisprudenciais que surgem e surgirão sobre a aplicação da LGPD, tampouco propostas legislativas que visam a lidar com os problemas pontuais sobre o direito à proteção de dados pessoais.

Cada vez que um usuário escolhe se expressar sexualmente de forma diferente do padrão esperado pela sociedade, ele enfrenta um risco social significativo. Fato é que os

potenciais danos enfrentados pelos usuários do “Grindr” quando expostos de alguma forma tendem a ser maiores do que os enfrentados por aqueles cujo padrão sexual é aceito pela sociedade.

Logo, se a plataforma constrói uma imagem comercial de suposta segurança para seus consumidores e assume o compromisso legal de protegê-las, os julgamentos de suas falhas deve levar em conta os fatores individuais que caracterizam seu público.

REFERÊNCIAS BIBLIOGRÁFICAS

Aplicativo Grindr é multado em US\$ 11,7 milhões por compartilhar dados de seus usuários. **G1**, 26 de janeiro de 2021. Disponível em:

<https://g1.globo.com/economia/tecnologia/noticia/2021/01/26/aplicativo-grindr-e-multado-em-us-117-milhoes-por-compartilhar-dados-de-seus-usuarios.ghtml>. Acesso em junho de 2023.

App de relacionamento gay Grindr compartilhou status de HIV de usuários com outras empresas. **BBC**, 04 de abril de 2018. Disponível em:

<https://g1.globo.com/economia/tecnologia/noticia/app-de-relacionamento-gay-grindr-compartilhou-status-de-hiv-de-usuarios-com-outras-empresas.ghtml>. Acesso em junho de 2023.

BERBERI, Marco Antonio Lima; FRACARO, Beatriz. Pessoas com deficiência, acessibilidade e inclusão: entre possibilidades e desafios para inclusão. **Pensar**, Fortaleza, v. 27, n. 4, p. 1-14, 2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. 1ª ed. Rio de Janeiro: Forense, 2019.

BRASIL. Câmara dos Deputados. **Projeto de Lei nº 2.811/2023**. Autora: Deputada Luizianne Lins. Brasília, DF, 2023.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Senado Federal, 1988. Disponível em:

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em junho de 2023.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em:

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em junho de 2023.

CAMARGO, Júlia Lio Rocha. Utilização da base legal do consentimento sob a perspectiva da metodologia do privacy by design. In: PEREIRA, Fabio Queiroz Pereira; LARA, Mariana Alves (Org.). **Os direitos de personalidade na sociedade em rede**. 1ª ed. Belo Horizonte: Editora Dialética, p. 93-120, 2023.

CASTELLS, Manuel. **A sociedade em rede - a era da informação**: economia, sociedade e cultura. 6ª ed. São Paulo: Paz e Terra, 2011.

Central de ajuda. **Grindr**, [s.d.]. Disponível em: <https://help.grindr.com/hc/pt>. Acesso em junho de 2023.

DONEDA, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais**: elementos da formação da Lei Geral de Proteção de Dados. 2ª ed. São Paulo: Thomson Reuters Brasil, 2020.

Dossiê denuncia 273 mortes e violências de pessoas LGBT em 2022. **Observatório de Mortes e Violências LGBTI+ no Brasil**, 08 de maio de 2023. Disponível em: <https://observatoriomorteseviolenciaslgbtibrasil.org/dossie/mortes-lgbt-2022/>. Acesso em junho de 2023.

FOUCAULT, Michel. **História da sexualidade I**: a vontade de saber. 13ª ed. Rio de Janeiro: Edições Graal, 1988.

FURTADO, Otavio. Atletas Olímpicos gays estão sendo expostos com vazamento dos perfis no Grindr. **Gay travel and fun**, 02 de agosto de 2021. Disponível em: gaytravelandfun.embarquenaviagem.com/atletas-olimpicos-gays-grindr/. Acesso em junho de 2023.

Grindr, app de encontros mais popular na comunidade gay, vai estrear na Bolsa valendo US\$ 2,1 bi. **O Globo**, 09 de maio de 2022. Disponível em: <https://oglobo.globo.com/economia/negocios/noticia/2022/05/grindr-app-de-encontros-mais-popular-na-comunidade-gay-vai-estrear-na-bolsa-valendo-us-21-bi-25504941.ghtml>. Acesso em junho de 2023.

Grindr. **Play Store**, [s.d.]. Disponível em: https://play.google.com/store/apps/details?id=com.grindrapp.android&hl=pt_BR&gl=US&pli=1. Acesso em junho de 2023.

GUSTIN, Miracy Barbosa de Sousa; DIAS, Maria Tereza Fonseca; NICÁCIO, Camila Silva. **(Re)pensando a pesquisa jurídica**: teoria e prática. 5ª ed. São Paulo: Almedina, 2020.

KARTER, Jonathan. PoderData: 22% usam ou já usaram aplicativos de paquera. **Poder 360**, 07 de maio de 2023. Disponível em: <https://www.poder360.com.br/poderdata/poderdata-22-usam-ou-ja-usaram-aplicativos-de-paquera/>. Acesso em junho de 2023.

KALDESTAD, Øyvind H. Grindr is made to pay after a complaint from the Norwegian Consumer Council. **Forbrukerrådet**, 01 de julho de 2024. Disponível em: <https://www.forbrukerradet.no/side/the-district-courts-judgment-in-the-grindr-case/>. Acesso em junho de 2023.

LEITE, Letícia. O que são direitos sexuais e reprodutivos? In: RAMOS, Marcelo Maciel; NICOLI, Pedro Augusto Gravatá; BRENER, Paula Rocha Gouvêa. **Gênero, Sexualidade e Direito**: uma introdução. 1ª ed. Belo Horizonte: Initia Via, p. 206-219, 2016.

LUNA, Florencia. La Declaración de la Unesco y la vulnerabilidad: la importância de la metáfora de las capas. In: CASADO, María (Coord.). **Sobre la dignidad y los principios**: análisis de la Declaración Universal sobre Bioética y Derechos Humanos UNESCO. 1ª ed. Madrid: Civitas, p. 255-266, 2009.

MARQUES, C. L.; MUCELIN, G. Vulnerabilidade na era digital: um estudo sobre os fatores de vulnerabilidade da pessoa natural nas plataformas, a partir da dogmática do Direito do Consumidor. **Civilística**, [s.l.], v. 11, n. 3, p. 1-30, 2022.

MCKINNON, Susan. **Genética neoliberal**: mitos y moralejas de la psicología evolucionista. 1ª ed. Ciudad de México: Fondo de Cultura Económica, 2012.

Ministério da Justiça notifica Tinder e Grindr por vender dados pessoais de usuários. **O Popular**, 15 de janeiro de 2020. Disponível em: <https://opopular.com.br/ministerio-da-justica-notifica-tinder-e-grindr-por-vender-dados-pessoais-de-usuarios-1.1973534>. Acesso em junho de 2023.

MONICA, Eder Fernandes; COSTA, Ramon Silva. Privacidade, liberdade sexual e sigilo: sentidos de liberdade no aplicativo "Grindr". **Interfaces Científicas**, Aracaju, v. 8, n. 2, p. 99-116, 2020. Disponível em: <https://periodicos.set.edu.br/educacao/article/view/7904/3786>. Acesso em junho de 2023.

Padre deixa cargo após ser descoberto no Grindr e em bares gays. **IG Queer**, 21 de julho de 2021. Disponível em: <https://queer.ig.com.br/2021-07-21/padre-gay-deixa-funcoes-grindr.html>. Acesso em junho de 2023.

PERMUY, Pedro. "Sigilo no Grindr": Marco Pigossi tem intimidade exposta: "Caçava doidão". **Folha Vitória**, 28 de março de 2023. Disponível em: <https://www.folhavoria.com.br/entretenimento/noticia/03/2023/sigilo-no-grindr-marco-pigossi-tem-intimidade-exposta-cacava-doidao>. Acesso em junho de 2023.

Política de privacidade e de cookies da Grindr. **Grindr**, 01 de julho de 2023. Disponível em: <https://www.grindr.com/privacy-policy/?lang=pt-BR>. Acesso em junho de 2023.

RAMOS, Marcelo Maciel. **Teorias Feministas e Teorias Queer do Direito**: gênero e sexualidade como categorias úteis para a crítica jurídica. *Rev. Direito Práx.*, [s.l.], v. 12, n. 03, p. 1679-1710, 2021.

RUBIN, Gayle. **Thinking sex**: notes for a radical theory of the politics of sexuality. In: PARKER, Richard; AGGLETON, Peter. *Culture, society and sexuality*. 1ª ed. London: Routledge, p. 143-179, 2006.

Senador questionado por foto nu publicada em site gay pede demissão. **G1**, 30 de agosto de 2011. Disponível em: <https://www.olhardireto.com.br/noticias/exibir.asp?id=201423¬icia=senador-questionado-por-foto-nu-publicada-em-site-gay-pede-demissao>. Acesso em junho de 2023.

SUPERIOR TRIBUNAL DE JUSTIÇA. **Agravo de Recurso Especial de nº 2.130.619 - SP (2022/0152262-2)**. 2ª Turma. Julgamento em 07 de março de 2023. Publicação em 10 de março de 2023.

SUPREMO TRIBUNAL FEDERAL. **Ação Direta de Inconstitucionalidade 6387 MC**. Relatora Rosa Weber. Tribunal Pleno. Julgamento em 07 de maio de 2020. Publicação em 12 de novembro de 2020.

ZUBOFF, Shoshana. **The age of surveillance capitalism the fight for a human future at the new frontier of power**. New York: PublicAffairs, 2019.

GOMES, Juliana Cesario Alvim. Direitos sexuais e reprodutivos ou direitos sexuais e direitos reprodutivos? Dilemas e contradições nos marcos normativos nacionais e internacionais. **Revista Direito GV**, São Paulo, v. 17, n. 3, p. 1-33, 2021.