



A utilização de dados manifestamente públicos de redes sociais: limites dos termos de uso e responsabilidade civil das plataformas digitais

Larissa Camargo Vallim

Universidade Estadual de Londrina (UEL), Paraná
alexandrefreitas204@gmail.com

Ivana Nobre Bertolazo

Universidade Estadual de Londrina (UEL), Paraná
iv.bertolazo@uel.br

Resumo

O presente trabalho tem como objetivo analisar o uso posterior de dados manifestamente públicos disponibilizados por usuários de redes sociais para finalidades diversas daquelas acordadas nos termos de uso das plataformas.

Utiliza-se o método dedutivo, por meio de pesquisa bibliográfica e documental, com base na análise de legislação, doutrina, jurisprudência e casos concretos, tanto reais quanto hipotéticos, envolvendo a reutilização de dados oriundos de redes sociais.

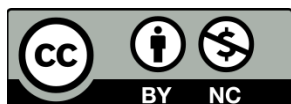
O tema revela-se pertinente devido ao cenário em que 70,4% da população brasileira utiliza redes sociais, favorecendo a circulação e a apropriação de dados pessoais para usos não consentidos. A originalidade da pesquisa reside na delimitação dos limites jurídicos entre a disponibilidade dos dados pelos seus titulares nas redes sociais e o uso posterior para finalidades diversas dos termos de uso sem o expresse consentimento.

Conclui-se que os dados manifestamente públicos não perdem sua natureza de dados pessoais apenas por terem sido disponibilizados voluntariamente pelos titulares. Assim, embora seu acesso possa ser livre, sua utilização permanece limitada pelas finalidades originalmente consentidas, pelos termos de uso das plataformas e pelos princípios da Lei Geral de Proteção de Dados. A reutilização indevida pode ensejar responsabilidade civil tanto do controlador da rede social quanto do terceiro que realiza o tratamento posterior dos dados.

O estudo contribui para diferenciar o livre acesso aos dados manifestamente públicos de sua reutilização para finalidades diversas das originalmente consentidas, além de auxiliar na delimitação dos deveres e responsabilidades dos controladores e operadores de dados.

Palavras-chave

Dados pessoais. Dados públicos. Finalidade. Termos de uso. Consentimento



Esta obra está licenciada com uma licença [Creative Commons Atribuição-Não Comercial 4.0 Internacional](https://creativecommons.org/licenses/by-nc/4.0/).

Revista Jurídica da FA7

ISSN 2447-9055

Vol. 22, n. 3, setembro - dezembro 2026

1. Introdução

As redes sociais são demarcadas pela dinâmica de interação em um novo ambiente virtual, nomeado ciberespaço, em que seus usuários podem trocar opiniões, fotos e vídeos com uma ampla variedade de pessoas sem barreiras geográficas. Esta forma de comunicação a partir de mídias e curtidas é capaz de revelar fatos pessoais e possibilitar o mapeamento do comportamento de seus usuários a partir do algoritmo.

Em um primeiro momento, esta detecção comportamental pode ser favorável para a personalização da experiência dentro do ambiente da rede social, tornando-o único e propiciando a experiência afirmativa de quem estiver acessando o site. Contudo, é necessário conscientizar-se acerca da importância da informação na era atual e do avanço das técnicas de coleta de dados.

A informação deixou de ser um dado simples e passou a figurar como ativo informacional, possuindo valor agregado no mercado. Seu domínio propicia o desenvolvimento de processos organizacionais, construção de negócios, tomada de decisões e criação de produtos e tecnologias moldadas conforme as preferências do público, garantindo o posterior sucesso no mercado. Desta forma, elucida-se o crescente aprimoramento dos profissionais e das técnicas de tecnologia da informação que, além de permitir a venda e a criação de banco de dados, ainda constroem ativos informacionais com valor em si mesmos e na sua posterior forma de exploração.

Não se resume a relevância do tema a inafastável influência das redes sociais no cotidiano dos cidadãos, como também se destaca a posição do Brasil como quinto maior país do mundo em número de usuários de internet, com 185 milhões de pessoas. Dada a extensão do mercado, ilustra-se o potencial de coleta e futura comercialização de dados pessoais, motivo pelo qual deve-se debater a temática de forma a evitar futuros danos à população.

Analogamente, é fato que todas as informações disponibilizadas em redes sociais são fruto de ação voluntária de cada um dos usuários. No entanto, pergunta-se, o fato destas informações estarem facilmente acessíveis ao público significa que estes dados sejam livres para uso? Para responder ao questionamento é imprescindível diferenciar conceitos basilares como o acesso e o uso dos dados e especificar os limites entre a liberdade e a responsabilidade proveniente de apropriação indevida de dados com cunho pessoal. Além disso, urge-se analisar os termos de uso e como as milhões de pessoas que concordam sem ler permitem que informações capazes de traçar o seu perfil podem estar sendo usadas de maneira inapropriada.

Para além dos limites da liberdade, é relevante explorar a captação dessas informações pessoais sem o consentimento dos usuários para inclusive formas de uso que não são imaginadas por seus titulares e que ferem tanto a privacidade quanto a dignidade dos usuários.

Sob esse prisma, a metodologia utilizada foi a leitura da legislação pátria, partindo de princípios fundamentais de dignidade da pessoa humana que permeiam essa relação, abrigando o estudo da legislação infraconstitucional específica, com destaque para a Lei Geral de Proteção de Dados que aborda especificamente a temática, e analisando também a GDPR, lei Europeia sobre proteção de dados que inspirou a brasileira e a doutrina nacional, finalizando com a pesquisa jurisprudencial e a análise da aplicação prática a partir de casos concretos como o da Meta no Brasil, objeto da nota técnica n.º 27 da ANPD.

Observa-se que além do desenvolvimento de produtos e treinamento de algoritmos a partir da formação de perfis comportamentais desenvolvidos a partir da coleta de dados publicamente disponíveis - fora da finalidade de sua disponibilização - a quarta revolução industrial propiciou o uso dessas informações para o treinamento de Inteligência Artificial. Dessa forma, é necessário entender os limites entre a liberdade e a privacidade dos usuários, para que além de terem seu comportamento rastreado, mapeado e transformado em público, estes também não sejam alvo de uma tecnologia maior, o desenvolvimento de inteligências autônomas que têm seu comportamento espelhado do aprendizado de máquina derivado de simples interações desprezíveis de pessoas na internet.

Nessa toada, pretende-se elucidar que a disponibilidade pública dos dados não afasta sua natureza de dado pessoal, razão pela qual seu reaproveitamento para finalidades diversas daquelas consentidas pode configurar violação à LGPD e gerar responsabilidade civil.

2. Dados manifestamente públicos são livres?

2.1. Dados Pessoais em rede social e a possibilidade de se enquadrarem como dados sensíveis

Ao falar sobre tratamento de dados é importante destacar que, conforme a Lei Geral de Proteção de Dados, a delimitação quanto à proteção dos dados não se restringe à mera coleta e uso, mas permeia por vários procedimentos, entre eles os mencionados pelo Art. 5º, X, LGPD:

Art. 5º, X, LGPD toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (BRASIL, 2018)

Dessa forma, entende-se que as várias formas de usufruto de dados possuem proteção legal pela legislação.

Sob esse prisma, destaca-se que embora trata-se de uma informação, os dados pessoais ao serem “toda informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2018), possuem a capacidade de montar o perfil individual de seu titular. Dessa forma, conforme lecionam Danilo Doneda e Laura Schertel, não se trata de mera informação, mas dispõe sobre o próprio indivíduo “a regulação de dados pessoais não incide sobre um objeto externo, mas sobre uma representação da própria pessoa” (Doneda, Schertel, 2021, p.39).

Assim, entendendo a relevância intrínseca a informações de cunho pessoal, e sua capacidade de tratar de aspectos íntimos da vida privada de cada indivíduo, a Constituição Federal estabeleceu a partir da Emenda Constitucional 115/2022 a proteção ao Dado Pessoal como Direito Fundamental nos termos do Art. 5º, LXXIX, CF.

Confirmada a relevância dessa espécie de dado para além de uma simples informação, destaca-se ainda que a LGPD ainda faz distinção de um dado pessoal que trata de assuntos de cunho ainda mais privado e com maior potencial danoso. Conforme ensina Doneda “estes seriam determinados tipos de informação que, caso sejam conhecidas e submetidas a tratamento, podem se prestar a uma potencial utilização discriminatória ou lesiva e que apresentaria maiores riscos potenciais do que outros tipos de informação” (Doneda, 2019, p. 142), motivo pelo qual foram atribuídos a classificação e tratamento específico pela lei.

Os dados sensíveis são definidos pelo art. 5º, II, LGPD como:

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).

Estes dados, no que se destaca os de origem racial ou étnica, convicção religiosa e opinião política são frequentemente abordados em redes sociais, não somente em fóruns de discussão ou aplicativos de opinião como o “X”, mas em postagens com conteúdo informacional ou de exposição de posicionamento e conscientização. Sendo uma rede de interações em nível global, as redes sociais saem do óbvio, que se iniciou pelo compartilhamento de fotos e vídeos, e passam a tratar assuntos de esfera íntima pessoal, envolvendo informações que no âmbito da LGPD saem da esfera de opinião e enquadram-se como dado pessoal sensível.

Ainda que o usuário da rede não exponha diretamente a sua opinião, ainda há risco de identificação de seu posicionamento a partir do rastreamento de suas curtidas, comentários e principais compartilhamentos. Conforme leciona Bruno Bioni, “um dado aparentemente comum pode se tornar um dado sensível quando submetido a tecnologias de Big Data e análise preditiva” (Bioni, 2020, p.118). Além disso, o autor destaca, amparado por estudos da Universidade de Cambridge, que simples “curtidas” em uma rede social permitem criar um “retrato fiel” dos gostos e preferências, viabilizando inferências sobre aspectos íntimos do titular (Bioni, 2020, p. 118).

Não somente o retrato fiel de gostos, mas conforme estudos é possível revelar a própria sexualidade dos usuários, o que também configura dado sensível. Na obra Proteção de dados. pessoais: a função e os limites do consentimento, é verificado isto: “A pesquisa identificou com exatidão a porcentagem dos usuários homossexuais e heterossexuais, os usuários brancos e negros e, por fim, quais teriam uma ligação partidária republicana ou democrata” (Bioni, 2020, p.118). Ou seja, as interações mais despretensiosas em plataformas de interação podem revelar informações que remontam perfil individualizado extremamente específico, que não somente está sendo utilizado para treinar o algoritmo, mas também sendo alvo de captura por usuários externos.

Isto é, os dados sensíveis, que possuem o tratamento cerceado por hipóteses específicas delimitadas pelo art. 11 da LGPD são frequentemente tornados acessíveis publicamente nas redes sociais, possibilitando o seu uso posterior, inclusive sem o consentimento do titular.

Essas questões já foram alvo de discussão pela Autoridade Nacional de Proteção de Dados, na Nota Técnica nº 27/2024, que dispõe especificamente sobre o caso da Meta no Brasil. A Meta foi alvo de relatório técnico após utilizar dos dados pessoais dos usuários de suas redes sociais, sobretudo Facebook e Instagram, para

treinar sua Inteligência Artificial autônoma, mas sem obter o consentimento dos usuários. Por mais que houvesse alterações nos termos de uso, este não chegou ao conhecimento expresso dos usuários, que não sabia que estavam tendo seus dados utilizados para uma finalidade diversa da anteriormente delimitada.

Conforme estabelecido na Nota Técnica:

o tratamento indiscriminado de fotografias, imagens, vídeos e gravações de áudios, especialmente por meio do uso de sistemas de inteligência artificial, pode revelar vinculações políticas, religiosas, sindicais e sexuais dos titulares, caracterizando dados pessoais sensíveis” (art. 5º, II, LGPD). (RELATÓRIO TÉCNICO nº 27, ANPD)

Sob essa justificativa a ANPD suspendeu o treinamento da IA da meta até que fossem feitas alterações compatíveis e obtida a devida autorização dos titulares dos dados conforme exige o art. 11 da LGPD para o tratamento desta espécie de dados.

É fundamental que o direito fundamental e constitucional à proteção dos dados pessoais seja respeitado, especialmente referente às informações disponibilizadas em redes sociais que, além de imagens, ditam também sobre o foro íntimo de quem as fornece, em consonância com o inferido por Vianna e Gionédis “Interessa, portanto, a proteção do indivíduo no tratamento de seus dados” (Gionédis, Vianna, 2021, p. 21).

2.2. Diferença entre dados públicos e manifestamente públicos

A doutrina faz distinção entre dados públicos e manifestamente públicos relevantes para compreender a dinâmica de disponibilização de informações dentro das redes sociais.

Dados públicos são aqueles cujo acesso decorre de obrigação legal, regulatória ou do próprio funcionamento da vida civil, como nome, CPF, endereço e registros administrativos fornecidos pelo cidadão perante órgãos públicos ou entidades privadas. Conforme leciona a doutrina “**acesso público** - aqueles que a lei exige, por exemplo dados referentes as atividades de órgãos públicos” (Gionédis, Vianna, 2021, p. 46).

Em detrimento a isso, os dados manifestamente públicos não seriam aqueles cujos cidadãos são compilados a fornecer no âmbito da vida cível, mas sim, os que eles voluntariamente decidem por disponibilizar ou tornar público. “Tornado manifestamente públicos pelo próprio titular de dado (aqui é o próprio titular que autoriza o uso de seus dados para uma finalidade)” (Gionédis, Vianna, 2021, p. 46).

Depreende-se que as informações pessoais disponíveis publicamente em redes sociais caracterizam-se como dados manifestamente públicos, tendo em vista que foram tornados públicos por ato voluntário do próprio titular. No entanto, o fato de estarem disponíveis *online* não significa que esses dados são livres.

2.3. O uso de dados públicos e a LGPD

Dados públicos e manifestamente públicos ainda estão submetidos às formas de tratamento em conformidade com a Lei Geral de Proteção de Dados.

Quando o dado pessoal é obtido pelo controlador com uma finalidade específica a indisponibilidade desses dados para uso externo é mais do que clara, conforme observa-se pelo art. 16 da LGPD:

*Art. 16. Os dados pessoais serão **eliminados após o término de seu tratamento**, no âmbito e nos limites técnicos das atividades, **autorizada a conservação somente em finalidades específicas. Entre elas:**
IV - **uso exclusivo do controlador**, vedado seu acesso por terceiro, e **desde que anonimizados os dados.** (Brasil, 2018)*

Há uma vedação clara na norma quanto ao uso posterior, delimitando inclusive a necessidade de descarte desse dado após o seu uso para a finalidade informada.

No entanto, quando o dado é tornado disponível, inclusive na internet, perde-se essa referência, e seu uso - por ser de fácil acesso - passa a ser visto como livre. Dessa forma, torna-se comum métodos de extração de dados em massa em sites para posterior utilização, venda ou formação de banco de dados para as mais diversas finalidades. A inserção de formas de vedar essa coleta, sendo ela realizada por *scraping*, *bots*, *APIs*, entre outros, não se trata de mera proteção do site, e sim do próprio usuário. Esse controle é previsto pela própria doutrina:

Dados pessoais somente poderão ser coletados e utilizados, nos exatos termos legais e de acordo com alguma das bases legais de tratamento de dados, previstas no art. 7º, da Lei Geral de Proteção de Dados Pessoais; e, sempre observados, além da boa-fé, os demais princípios contidos no art. 6º, da mesma lei. (Gionédís, Vianna, 2021, p. 62)

Necessitando, portanto, a base legal para tratamento, e a conformidade com os artigos previstos no art. 6º resta claro que este tratamento não pode ser feito a qualquer modo. No que tange mais especificamente aos dados tornados públicos, Bioni leciona:

*O que define a (i)legalidade do tratamento dos dados é a sua compatibilidade com a **finalidade e o interesse público** pelo qual tais dados são de acesso público. É necessária, portanto, uma análise **contextual para saber por que houve publicização da informação**, o que calibrará os possíveis (re)usos que dela podem ser feitos (Bioni, 202, p.341).*

Os arts. 7º parágrafos 3º e 4º determinam que o tratamento de dados pessoais cujo acesso é público deve considerar a finalidade, a boa-fé e o interesse público que justificaram sua disponibilização. Dessa forma, não se pode confundir facilidade de acesso com disponibilidade de uso. A finalidade é definida pelo art. 6º, I, LGPD como a “realização do tratamento para propósitos legítimos, específicos, explícitos e **informados ao titular, sem possibilidade de tratamento posterior de forma incompatível** com essas finalidades” (Brasil, 2018, grifo nosso). Isto é, ainda que públicos, a determinação posterior de atribuições ao uso dos dados fere a finalidade indicada ao usuário, estando em desacordo à legislação.

Os dados manifestamente públicos são igualmente alvo de dispositivo específico que dita no art. 7º § 4º “É dispensada a exigência do consentimento previsto no caput deste artigo para os dados tornados manifestamente públicos pelo titular, **resguardados** os direitos do titular e os **princípios** previstos nesta Lei” (Brasil, 2018, grifo nosso). Vale ressaltar, que ainda que o dispositivo dispense o consentimento, os princípios ainda sim devem ser considerados. Ou seja, o princípio da finalidade ainda garante a impossibilidade de utilização para finalidades diversas da informada.

Assim, ao se tratar de redes sociais, a finalidade informada ao usuário da qual obteve-se o seu consentimento são aquelas informadas nos termos de uso. Em regra, a disponibilização dos dados é com o objetivo de possibilitar a interação entre os usuários na rede social, publicar e compartilhar mídia de interesse e expor opiniões. Bruno Bioni ao ensinar sobre o assunto dispôs:

[...] terceiros não poderiam usar dados de uma rede social, mesmo que de perfis públicos, para fins de marketing - cujas circunstâncias pelas quais tais dados foram tornados públicos pelo seu próprio titular deram se para uma outra finalidade, que é a de se relacionar com quem integra o seu círculo social. (Bioni, 2020, p.341).

A partir dessa citação percebe-se tanto a impossibilidade de uso **ainda que os perfis sejam públicos** quanto a necessidade de adequação do uso posterior à

finalidade vinculada à disponibilização. Ainda que propósitos de marketing sejam frequentemente perceptíveis em redes sociais, ao passo que este não são a finalidade informada ao usuário, não são um propósito viável.

Ainda quanto a essa temática, a Nota Técnica nº 27/2024 da ANPD sobre o caso Meta anteriormente mencionada também aborda a utilização de dados para novas finalidades ainda que estes tenham sido voluntariamente disponibilizados pelos usuários:

[...] mesmo que o titular tenha, por vontade própria, publicado em determinado ambiente online conteúdo de natureza pessoa, a sua utilização por terceiros não pode ser feita em desacordo com as suas legítimas expectativas e com os princípios de proteção de dados pessoais, conforme o disposto no art. 6º da LGPD (nota técnica nº 27/2024)

A utilização dos dados dos usuários da rede social para o treinamento de inteligência artificial, além de fora das hipóteses de utilização de dados sensíveis do art. 11 da LGPD, também descumpra o delimitado pelas hipóteses do art. 7º da mesma lei, por ausência de consentimento e desrespeito aos princípios, sobretudo, da finalidade, adequação e necessidade.

Assim, a publicidade dos dados não se relaciona à liberdade de seu uso, pois continuam sendo protegidos como direito fundamental, e sujeitos às disposições infraconstitucionais da Lei Geral de Proteção de Dados que delineiam sua utilização a critérios específicos, com a preponderância da segurança do titular.

3. Força contratual dos termos de uso

3.1 Seus dados são o produto

Um questionamento que pode surgir em relação aos donos das principais empresas de redes sociais serem bilionários e estarem no *ranking* entre os principais nomes da atualidade enquanto fornecem serviços gratuitos. Redes sociais de grande porte como *Facebook*, *Instagram* e *Tiktok* se destacam no cenário mundial e não cobram nada de seus usuários pelo seu uso regular.

O retorno financeiro se dá pelo modelo de negócios que essas empresas adotam, conhecido como *zero-price advertisement business model*. Esse modelo é explicado por Bruno Bioni:

A contraprestação deriva do fornecimento de seus dados pessoais, o que possibilita o direcionamento de conteúdo publicitário, e cuja receita pagará, indiretamente, pelo bem de consumo (advertisement business model). Há uma troca (trade-of) dos dados pessoais pelo serviço ou produto (Bioni, 2020, p. 295).

Em síntese, os serviços ofertados pelas redes sociais são gratuitos aos usuários, pois a verdadeira contraprestação não é financeira. Os usuários fornecem os dados pessoais com consentimento por meio dos termos de uso, não gerando lucro imediato. Esses dados são posteriormente usados como matéria-prima e transformados em ativos financeiros por meio da publicidade segmentada, ou da formação de base de dados, informação que é o principal ativo de diversas empresas:

Sob um novo modelo de negócio, consumidores não pagam em dinheiro pelos bens de consumo, eles cedem seus dados pessoais em troca de publicidade direcionada. São os anunciantes de conteúdo publicitário que aperfeiçoam o seu arranjo econômico. Dessa forma, tal relação torna-se plurilateral, uma vez que ela envolve, necessariamente, os anunciantes de conteúdo publicitário, para haver retorno financeiro nesse modelo de negócio (Bioni, 2020,p.47).

Esse modelo de negócios distancia-se do tradicional, pautado em relações bilaterais, com destaque para a compra e venda, e que há a contraprestação imediata, narrado por Bioni “No modelo de negócio “tradicional”, consumidores trocam uma quantia pecuniária por um bem de consumo” (Bioni, 2020, p. 47).

O valor econômico das informações fornecidas está associado ao fato deste ser um ativo intangível. Conforme estabelece o CPC 04 (Comitê de Pronunciamentos Contábeis), ativo intangível é um “bem identificável, não monetário, sem substância física”, identificável quando: (a) for separável, podendo ser vendido, licenciado ou transferido; ou (b) resultar de direitos contratuais ou legais. O conjunto de dados por ser separável e poder ser vendido ou transferido, usado como matéria-prima por outras empresas e ser resultado de direitos contratuais pela permissibilidade estabelecida nos termos de uso, encaixa-se perfeitamente na definição como ativo intangível, havendo, portanto, valor agregado em si mesmo.

Assim, a partir desse novo modelo de negócios implementado as relações passam a ser plurais, os dados pessoais passam a ser ativos informacionais valiosos às empresas, e sua disseminação e troca passa a ser frequente. Para além das vantagens, deve-se relembrar o valor fundamental atrelado à proteção dessas

informações e a necessidade de cuidado para que as relações comerciais não estejam desrespeitando direitos legalmente reconhecidos.

3.2. Termos de uso como forma contratual

Ao contratar determinados serviços online estes não estão desprovidos da formulação de negócios jurídicos. Embora não haja um contrato tradicional que permeia as relações, estas - principalmente nas que ditam sobre redes sociais - possuem seus termos de uso, em que, há a permissão para uso dos serviços somente mediante aceite e concordância com as condições da empresa. Os termos de uso, embora tenha como característica a adesão, sem possibilidade de que a outra parte disponha sobre seus treinos, podendo apenas - ao não concordar - declinar os serviços, configura uma forma de contrato.

Ao ser caracterizado pelo acordo de vontades, a modificação, criação ou extinção de direitos e exigir capacidade do agente, objeto lícito, possível e determinado além do livre consentimento, é uma forma válida de contrato, nos termos do art. 104, CC. Frente ao reconhecimento dessas características, Thaís Venturi leciona “os Termos de Uso constituem verdadeiro contrato de adesão, gratuito, bilateral e atípico” (Venturi, 2023).

Sob esse prisma, reconhecendo os termos de uso como forma contratual deve-se considerar a correta interpretação contratual e a incidência do princípio do *pacta sunt servanda*. Nesse aspecto, considerando que “não só a lei deve ser interpretada, mas também os negócios jurídicos em geral” (Gonçalves, 2017, p. 62), e que pelo princípio do *pacta sunt servanda*, o contrato faz lei entre as partes, “O contrato é obrigatório entre as partes, como se lei fosse” (Glanz, Cavalcanti, Paesani, 2011, p. 341), é válido analisar os termos de uso das principais plataformas e as condições que a maioria dos usuários aceita sem ter verdadeira ciência da permissibilidade de uso por eles assentida.

3.2.1 Termos de uso das principais redes sociais

Ainda que a coleta massificada de informações em redes sociais seja uma prática cada vez mais comum, especialmente diante do avanço das tecnologias de Big Data e de Inteligência Artificial, os dados disponibilizados pelos usuários continuam sendo dados pessoais protegidos constitucionalmente pelo direito à privacidade, à intimidade e à autodeterminação informativa, bem como infraconstitucionalmente pela Lei Geral de Proteção de Dados.

Nesse sentido, conforme visto, a mera acessibilidade de uma informação em ambiente digital não implica autorização irrestrita para sua captação, reprodução, comercialização ou utilização por terceiros estranhos à relação originalmente estabelecida entre plataforma e usuário. Ao contrário, além da legislação e da doutrina supra mencionados, os próprios termos de uso das principais redes sociais demonstram que há uma limitação expressa ao uso de mecanismos automatizados de coleta de dados, sobretudo quando empregados para finalidades econômicas, construção de bancos de dados ou treinamento de algoritmos.

O Facebook, por exemplo, estabelece expressamente que o usuário não pode “acessar ou coletar dados dos nossos Produtos usando meios automatizados (sem nossa permissão prévia)” nem “tentar acessar dados que não tenha permissão para acessar”. A plataforma também proíbe que terceiros burlam “quaisquer medidas tecnológicas que a Meta usa para controlar ou limitar o acesso aos nossos Produtos ou dados”. Além disso, veda a coleta de nomes de usuário, senhas e tokens de acesso.

De forma semelhante, o Instagram dispõe que os usuários não podem “fazer, ou tentar fazer, nada para burlar, contornar ou substituir quaisquer medidas tecnológicas que controlem ou limitem o acesso ao Serviço ou aos dados”.

O TikTok, por sua vez, proíbe expressamente “usar scripts automatizados para colher informações dos Serviços” e também “burlar quaisquer medidas que utilizemos para impedir ou limitar o acesso aos Serviços”.

Já a plataforma X veda “atividades coordenadas e inautênticas que influenciem artificialmente as conversas”, demonstrando preocupação não apenas com a coleta massiva de informações, mas também com o uso artificial e manipulado da plataforma por meio de múltiplas contas, bots e perfis falsos.

Os próprios termos da Meta reforçam essa vedação ao estabelecer que os usuários não devem se envolver em “comportamento não autêntico coordenado”, tampouco utilizar múltiplos ativos do Facebook e Instagram para criar operações artificiais com contas falsas. A empresa também considera como “tráfego inautêntico” a atuação de indivíduos que buscam ganhos próprios mediante tais práticas.

Verifica-se, portanto, que as principais plataformas digitais reconhecem que os dados compartilhados em seus ambientes não estão livres para coleta indiscriminada por terceiros. Embora o conteúdo possa ser visualizado publicamente, o uso automatizado dessas informações, sobretudo para a construção de bancos de

dados, direcionamento de publicidade, treinamento de Inteligência Artificial ou exploração econômica, encontra limites tanto nos termos contratuais quanto na legislação de proteção de dados.

A controvérsia envolvendo o LinkedIn e a empresa hiQ Labs evidencia essa limitação. A hiQ alimentava seu banco de dados por meio da extração automatizada de informações constantes de perfis públicos do LinkedIn. Para tanto, utilizava programas de computador capazes de coletar massivamente dados dos usuários da plataforma.

O LinkedIn ajuizou demanda sustentando que a prática configurava violação de seus termos de uso, uma vez que a hiQ realizava scraping automatizado, utilizava os dados coletados para finalidades próprias e, ainda, criava identidades falsas para acessar a plataforma. Em última instância, o tribunal concluiu que a hiQ violou o Contrato de Usuário do LinkedIn tanto pela extração e utilização dos dados quanto pela criação de perfis falsos.

O caso demonstra que, mesmo quando os dados estão publicamente disponíveis, sua coleta automatizada e seu reaproveitamento econômico não são irrestritos. A disponibilidade pública não desnatura a condição de dado pessoal, tampouco elimina a necessidade de observância da finalidade, da boa-fé, do consentimento e das legítimas expectativas do titular.

Assim, os termos de uso das plataformas funcionam como importante instrumento contratual de limitação da coleta massificada de dados, reforçando a proteção conferida pela LGPD. A violação dessas cláusulas pode ensejar não apenas inadimplemento contratual, mas também responsabilidade civil, especialmente quando houver utilização indevida de dados pessoais para finalidades diversas daquelas originalmente consentidas pelo usuário.

4. A responsabilidade civil na LGPD e nas relações contratuais

Tendo em vista que os termos de uso, assinado por todos que fazem uso das redes sociais, tratam-se de uma espécie de contrato de adesão, havendo, portanto, a incidência de seus princípios, como o mencionado *pacta sunt servanda*, deve-se analisá-los sob a ótica da responsabilidade civil.

A responsabilidade civil se aplica em duas facetas: da responsabilidade do controlador pela segurança e uso adequado dos dados, e quanto a usuários externos

que descumprem os termos de uso e colocam em risco o titular pelo uso inadequado de dados pessoais obtidos por coleta não permitida para finalidades não autorizadas.

4.1. Responsabilidade do controlador

Ao disponibilizar uma plataforma digital e estimular o compartilhamento de informações pessoais, a rede social assume deveres jurídicos que vão além da simples prestação do serviço. Os termos de uso e as políticas de privacidade criam legítima expectativa de segurança, sigilo e limitação do tratamento dos dados pessoais dos usuários. Por essa razão, o controlador da plataforma não pode se eximir de responsabilidade sob o argumento de que os dados eram públicos ou de que terceiros foram os responsáveis imediatos pela coleta indevida.

Nos termos do art. 422 do Código Civil, os contratantes devem observar os princípios da probidade e da boa-fé tanto na conclusão quanto na execução do contrato. A boa-fé objetiva impõe deveres anexos de lealdade, cooperação, informação e proteção, os quais vinculam a plataforma digital desde a fase pré-contratual até o período posterior ao encerramento da relação jurídica.

O Superior Tribunal de Justiça já reconheceu que a boa-fé objetiva restringe o exercício abusivo de direitos e impõe às partes o dever de colaboração mútua para a consecução dos fins comuns perseguidos pelo contrato, de modo que os legítimos interesses da contraparte sejam preservados. REsp 1.779.763/SP, Quarta turma afirma:

[...] a boa-fé objetiva restringe o exercício abusivo de direitos, impondo que as partes colaborem mutuamente para a consecução dos fins comuns perseguidos com o contrato - que não é um mero instrumento formal de registro das intenções -, e também encontra a sua vinculação e limitação na função econômica e social do contrato, visando a fazer com que os legítimos interesses da outra parte, relativos à relação econômica nos moldes pretendidos pelos contratantes, sejam salvaguardados” (STJ apud AgInt no REsp 1779763/SP, Quarta Turma, DJe 13/08/2020, sem destaque no original).

Nesse contexto, a plataforma que afirma proteger os dados dos usuários, mas posteriormente tolera, facilita ou não impede a coleta massiva e o uso incompatível dessas informações por terceiros, incorre em comportamento contraditório. Tal hipótese se aproxima da vedação ao venire contra factum proprium, segundo a qual ninguém pode adotar comportamento incompatível com a confiança legitimamente criada na outra parte. Conforme leciona Carlos Roberto Gonçalves, “A “teoria dos atos próprios”, ou a proibição de venire contra factum proprium, “protege uma parte contra

aquela que pretende exercer uma posição jurídica em contradição com o comportamento assumido anteriormente” (Gonçalves, 2017,p. 57).

Sob a mesma ótica, Régis Pereira na Obra sobre responsabilidade civil pré-contratual afirma "o que se quer evitar com a proibição do venire contra factum proprium é que a parte da relação jurídica contratual adote mais de um padrão de conduta, segundo as vantagens que cada situação possa lhe oferecer” (Pereira, 2001. p. 85).

Essa contradição caracteriza violação positiva do contrato, pois a plataforma deixa de cumprir deveres anexos de proteção e segurança inerentes à relação contratual. Segundo Carlos Roberto Gonçalves, há inadimplemento quando o contratante descumpre deveres laterais derivados da boa-fé objetiva. Nessa linha, o Enunciado 24 da I Jornada de Direito Civil estabelece que a violação dos deveres anexos constitui espécie de inadimplemento, independentemente de culpa.

Além disso, a vedação ao comportamento contraditório encontra fundamento nos arts. 187 e 422 do Código Civil, conforme reconhece o Enunciado 362 da IV Jornada de Direito Civil, “A vedação do comportamento contraditório (venire contra factum proprium) funda-se na proteção da confiança, tal como se extrai dos artigos 187 e 422 do Código Civil.

No âmbito da proteção de dados, esses deveres contratuais são reforçados pela própria LGPD. O art. 46 determina que os agentes de tratamento adotem medidas técnicas e administrativas aptas a proteger os dados pessoais contra acessos não autorizados e situações ilícitas, enquanto o art. 47 estende esse dever de segurança a todos que intervenham em qualquer fase do tratamento, inclusive após seu encerramento.

Quanto ao regime jurídico aplicável, a responsabilidade da plataforma pode ser compreendida sob dois fundamentos complementares: extracontratual e contratual.

Sob a ótica extracontratual, trata-se de responsabilidade aquiliana, fundada na prática de ato ilícito, nos termos dos arts. 186 e 187 do Código Civil, segundo os quais comete ilícito aquele que viola direito e causa dano a outrem, inclusive pelo exercício abusivo de uma posição jurídica. A obrigação de reparar decorre do art. 927 do Código Civil, sendo possível sustentar a incidência do parágrafo único do referido dispositivo, diante do risco inerente à atividade de tratamento massivo de dados pessoais.

Além disso, nas hipóteses em que a plataforma mantém relação de consumo com o usuário, aplica-se o art. 45 da LGPD, que remete ao Código de Defesa do Consumidor. Nesses casos, a responsabilidade tende a ser objetiva, nos termos do art. 14 do CDC, bastando a comprovação do defeito do serviço, do dano e do nexo causal, independentemente de culpa. O serviço será considerado defeituoso quando não fornecer a segurança legitimamente esperada pelo usuário, especialmente quanto à guarda, ao controle e à proteção dos dados pessoais.

Por outro lado, também há responsabilidade contratual, pois, a plataforma assume, por meio dos termos de uso e da política de privacidade, deveres específicos de segurança, transparência e proteção de dados. O descumprimento desses deveres anexos caracteriza inadimplemento contratual, nos termos dos arts. 389 e 422 do Código Civil. Nessa hipótese, a responsabilidade decorre da violação da confiança legitimamente criada no usuário, especialmente quando a plataforma promete proteção dos dados, mas permite sua coleta indevida, vazamento ou utilização incompatível com as finalidades informadas.

No âmbito específico da LGPD, a obrigação de indenizar decorre diretamente do art. 42, segundo o qual o controlador ou operador que, em razão da atividade de tratamento, causar dano patrimonial ou moral em violação à legislação de proteção de dados pessoais, deve repará-lo. Há, ainda, solidariedade entre os agentes envolvidos no tratamento, nos termos do §1º do mesmo dispositivo.

4.2. Responsabilidade do usuário externo

Também há responsabilidade própria do terceiro usuário externo que realiza coleta massiva, scraping ou reaproveitamento de dados extraídos da plataforma. Isso porque, ao criar conta, efetuar login ou utilizar funcionalidades da rede social, esse agente adere aos termos de uso e assume contratualmente a obrigação de respeitar as limitações impostas pela plataforma quanto ao acesso, cópia e reutilização dos dados.

Nessa hipótese, a responsabilidade é predominantemente contratual em relação à plataforma, fundada nos arts. 389 e 422 do Código Civil, uma vez que o terceiro descumpre obrigação assumida ao aceitar os termos de uso. Além disso, pode haver responsabilidade extracontratual perante os titulares dos dados, com fundamento nos arts. 186, 187 e 927 do Código Civil, especialmente quando a coleta ou utilização dos dados ocorre para finalidades distintas daquelas legitimamente esperadas pelo usuário.

Segundo Carlos Roberto Gonçalves, o abuso de direito configura-se quando o titular exerce sua prerrogativa de maneira desviada da finalidade social para a qual o direito subjetivo foi conferido. (Gonçalves, 2024).

A conduta também pode caracterizar abuso de direito, nos termos do art. 187 do Código Civil, pois o agente se vale da aparente publicidade dos dados para justificar uma utilização incompatível com a confiança depositada pelo titular e com as restrições expressamente impostas pela plataforma. O abuso de direito pode ser definido como “o ato que constitui o exercício egoístico, anormal de direito, sem motivos legítimos, com excessos intencionais ou involuntários, dolosos ou culposos, nocivos a outrem, contrários ao destino econômico e social do direito em geral, e por isso, reprovado pela consciência pública” (Gonçalves, 2019, p. 70).

Em tais casos, há violação ao dever de lealdade, à boa-fé objetiva e à vedação ao comportamento contraditório, já que o usuário aceita contratualmente determinadas limitações e, posteriormente, atua em desconformidade com elas.

O caso entre LinkedIn e hiQ Labs é emblemático nesse ponto. Embora a hiQ sustentasse que coletava apenas dados públicos, a Justiça norte-americana reconheceu que a empresa havia aderido aos termos de uso do LinkedIn e os violado ao realizar scraping automatizado, utilizar dados coletados comercialmente e empregar terceiros para criar perfis falsos. O tribunal entendeu que os termos proibiam expressamente scraping, criação de contas falsas e uso não autorizado dos dados da plataforma.

Além disso, a decisão ressaltou que o fato de determinadas informações serem visíveis publicamente não autoriza sua coleta por meios expressamente proibidos contratualmente. Em outras palavras, a publicidade do dado não elimina a necessidade de observância dos limites de uso impostos pela plataforma e pela finalidade para a qual o titular disponibilizou a informação.

A própria decisão reconheceu que a hiQ poderia responder pelos atos praticados por seus prepostos e contratados (“turkers”), os quais criaram perfis falsos para acessar e validar dados dentro da plataforma. Isso reforça a possibilidade de responsabilização solidária entre a empresa que se beneficia economicamente da coleta ilícita e os agentes que operacionalizam a prática. A decisão reconheceu que a hiQ poderia responder pelos atos praticados por seus prepostos e contratados (“turkers”), os quais criaram perfis falsos para acessar e validar dados dentro da plataforma. Isso

reforça a possibilidade de responsabilização solidária entre a empresa que se beneficia economicamente da coleta ilícita e os agentes que operam.

5. Conclusão

Depreende-se, que os dados acessíveis nas redes sociais não se confundem com dados livres. Ainda que os usuários tenham optado voluntariamente por torná-los disponíveis, enquadrando-se no conceito de dados manifestamente públicos, o seu tratamento só é viabilizado quando estiver de acordo com a base legal, respeitando sempre o consentimento e a finalidade informada ao titular no momento de sua publicação.

O uso dos dados fora da finalidade original, ainda que para fins como marketing ou para fins mais específicos como treinamento de Inteligência Artificial ferem a legislação infraconstitucional, e conseqüentemente colocam em risco o direito fundamental à proteção do dado pessoal, que revela aspectos de foro íntimo do indivíduo. Além disso, as informações disponibilizadas em redes sociais, por possuírem caráter de opinião ou expressão de raça, etnia, política, religião ou sexualidade, seja de modo direto ou indireto, são identificados como dados pessoais sensíveis, possuindo a forma de tratamento ainda mais restrita e sujeita às hipóteses do art. 11 da LGPD.

Desta forma, reconhecendo a obtenção dos dados pelas empresas como forma de contraprestação em decorrência do atual modelo de negócios das empresas de redes sociais, e compreendendo os termos de uso como um contrato de adesão que se atém a questões de proteção e segurança dos dados pessoais, ainda não há de se falar em liberdade no uso dos dados. As informações captadas ainda estão sujeitas à LGPD, e seu tratamento incorreto implica em responsabilidade civil tanto ao controlador responsável pela plataforma que possui o dever de vigilância e de tratamento adequado dos dados, quanto do terceiro externo à relação que se apropria inadequadamente dos dados para proveito próprio, ambos sujeitos à responsabilização contratual ou extracontratual.

Conclui-se, portanto, que os dados disponibilizados voluntariamente em redes sociais não possuem tratamento livre, estando a segurança do titular assegurada tanto constitucionalmente quanto infraconstitucionalmente, preocupando-se sempre com a privacidade e a dignidade dos usuários.

Referências

BRASIL. **Autoridade Nacional de Proteção de Dados**. Nota Técnica n.º 27/2024/CGF/ANPD. Brasília, DF: ANPD, 2024.

BRASIL. Conselho da Justiça Federal. **Enunciado n.º 24 da I Jornada de Direito Civil**. Brasília, DF: CJP, 2002.

BRASIL. Conselho da Justiça Federal. **Enunciado n.º 170 da III Jornada de Direito Civil**. Brasília, DF: CJP, 2004.

BRASIL. Conselho da Justiça Federal. **Enunciado n.º 362 da IV Jornada de Direito Civil**. Brasília, DF: CJP, 2006.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988.

BRASIL. Constituição (1988). **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais. Diário Oficial da União: seção 1, Brasília, DF, 11 fev. 2022.

BRASIL. **Lei n.º 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União: seção 1, Brasília, DF, 12 set. 1990.

BRASIL. **Lei n.º 10.406, de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, 11 jan. 2002.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018.

BRASIL. Ministério da Justiça. Secretaria de Direito Econômico. Departamento de Proteção e Defesa do Consumidor. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Elaboração de Danilo Doneda. Brasília: SDE/DPDC, 2010. 122 p. Disponível em: <https://www.gov.br/mj/pt-br/assuntos/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>

BRASIL. Superior Tribunal de Justiça. **Agravo Interno no Recurso Especial n.º 1.779.763/SP**. Relator: Ministro Marco Buzzi. Quarta Turma. Julgado em 10 ago. 2020. Diário da Justiça Eletrônico, Brasília, DF, 13 ago. 2020.

BRASIL. Tribunal de Justiça de Santa Catarina. **Entenda por que a informação é o ativo mais importante de uma organização**. Disponível em: https://www.tjsc.jus.br/web/servidor/dicas-de-ti/-/asset_publisher/0rjEBzj2Oes/content/entenda-porque-a-informacao-e-o-ativo-mais-importante-de-uma-organizacao. Acesso em: 8 abr. 2026.

BIONI, Bruno Ricardo Bioni. **Proteção de dados pessoais: a função e os limites do consentimento**. 3. ed. Rio de Janeiro: Forense, 2021.

BIONI, Bruno Ricardo Bioni. Proteção de dados pessoais e o modelo de negócio das plataformas digitais. In: FRAZÃO, Ana; MULHOLLAND, Caitlin (org.). **Inteligência artificial e direito: ética, regulação e responsabilidade**. São Paulo: Thomson Reuters Brasil, 2022.

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

DONEDA, Danilo Doneda.; MENDES, Laura Schertel Mendes. Fundamental right to personal data protection in Brazil. In: CELLA, José Renato Gaziero; DONEDA, Danilo (org.). **Data protection in Brazil: fundamental right and legal framework**. São Paulo: Thomson Reuters Brasil, 2021.

GIONÉDIS, Louise Rainer Pereira; VIANNA, Maria Amélia Mastrorosa (org.). **Lei Geral de Proteção de Dados (LGPD) e o compliance**. Curitiba: Juruá Editora, 2021.

GLANZ, Semy; CAVALCANTI, Ana Elizabeth Lapa Wanderley; PAESANI, Liliana Minardi. **Contratos eletrônicos e relações de consumo**. São Paulo: Revista dos Tribunais, 2011.

GONÇALVES, Carlos Roberto Gonçalves. **Direito civil brasileiro**: contratos e atos unilaterais. v. 3. 21. ed. São Paulo: SaraivaJur, 2024.

GONÇALVES, Carlos Roberto Gonçalves. **Direito civil brasileiro**: responsabilidade civil. v. 4. 19. ed. São Paulo: SaraivaJur, 2024.

LinkedIn Corporation v. hiQ Labs, Inc.. United States District Court for the Northern District of California. **LinkedIn Corporation v. hiQ Labs, Inc.**, No. 17-cv-03301-EMC. Julgado em 2022.

MARTINS-COSTA, Judith Martins-Costa. **A boa-fé no direito privado**: sistema e tópica no processo obrigacional. 2. ed. São Paulo: Revista dos Tribunais, 2018.

META PLATFORMS. **Instagram Terms of use**. Disponível em: <https://www.facebook.com/help/instagram/581066165581870>. Acesso em: 12 jan. 2026.

PEREIRA, Régis Fichtner. **A responsabilidade civil pré-contratual**. Rio de Janeiro: Renovar, 2001.

SZTAJN, Rachel; BAROSS FILHO, Milton. **Cláusulas contratuais gerais**. São Paulo: Revista dos Tribunais, 2012.

TIKTOK. **Terms of Service**. Disponível em: <https://www.tiktok.com/legal/page/row/terms-of-service/en>. Acesso em: 12 jan. 2026.

VENTURI, Thaís G. Pascoaloto. Os termos de uso: você já leu? In: **Migalhas**, Migalhas de Responsabilidade Civil, 14 dez. 2023. Disponível em: <https://www.migalhas.com.br/coluna/migalhas-de-responsabilidade-civil/398919/os-termos-de-uso-voce-ja-leu>. Acesso em: 8 abr. 2026.

VENTURI, Thaís Goveia Pascoaloto. **Termos de uso e contratos eletrônicos nas plataformas digitais**. São Paulo: Thomson Reuters Brasil, 2022.

X Corp.. X Terms of Service. Disponível em: <https://x.com/en/tos>. Acesso em: 12 jan. 2026.

The use of manifestly public social media data: Limits of terms of use and civil liability of digital platforms

Abstract

This study aims to analyze the subsequent use of manifestly public data made available by social media users for purposes other than those agreed upon in the platforms' terms of use.

The deductive method is employed through bibliographic and documentary research, based on the analysis of legislation, legal doctrine, case law, and concrete cases, both real and hypothetical, involving the reuse of data obtained from social media platforms.

The topic proves relevant due to the context in which 70.4% of the Brazilian population uses social media, thereby favoring the circulation and appropriation of personal data for non-consented uses. The originality of the research lies in defining the legal boundaries between the availability of data made public by their holders on social media and their subsequent use for purposes different from those established in the terms of use, without express consent.

It is concluded that manifestly public data do not lose their nature as personal data merely because they were voluntarily disclosed by their holders. Thus, although access to such data may be free, their use remains limited by the purposes originally consented to, by the platforms' terms of use, and by the principles established in the General Data Protection Law.

Improper reuse may give rise to civil liability both for the controller of the social network and for the third party that subsequently processes the data.

The study contributes to distinguishing free access to manifestly public data from their reuse for purposes other than those originally consented to, while also helping to define the duties and responsibilities of data controllers and data processors.

Keywords

Silent partnership. Hidden partner. Employment relationship fraud. Recognition. Social dumping.

Como citar

VALLIM, Larissa Camargo; BERTOLAZO, Ivana Nobre. A utilização de dados manifestamente públicos de redes sociais: limites dos termos de uso e responsabilidade civil das plataformas digitais. **Revista Jurídica da FA7**, Fortaleza, v. 22, n. 3, p. 74-94, set./dez. 2025.