

## Introdução

Em julho de 2023, duas expressões italianas, "*Attenzione pickpocket!*" e "*Attenzione borseggiatrici!*", se tornaram virais nas redes sociais. Estas frases foram popularizadas por uma senhora que alerta turistas sobre furtos em Veneza, na Itália. Traduzindo para o português, elas significam "atenção, batedores de carteira!". Os vídeos são compartilhados pela conta "*Cittadini Non Distratti*", um grupo de voluntários dedicado a prevenir furtos e recuperar carteiras roubadas. Os vídeos ganharam grande repercussão, alcançando mais de 10 milhões de visualizações e atraindo mais de 350 mil seguidores na página.

No mesmo mês, um movimento ainda maior tomou conta das redes: a empresa Meta lançou o aplicativo Threads, que rapidamente atraiu cerca de 30 milhões de usuários em apenas alguns dias. Essa plataforma, parcialmente integrada ao Instagram, permite que os usuários compartilhem textos, fotos e vídeos, além de curtir, compartilhar e comentar os posts de outros usuários. Disponível inicialmente em mais de 100 países, o Threads é a mais recente aposta de Mark Zuckerberg para competir com o X (antigo Twitter) como uma plataforma de conversas públicas.

Mas o que esses assuntos têm em comum? Assim como a senhora italiana alerta os turistas desavisados, o objetivo do artigo é analisar se os termos de uso do Threads estão em conformidade com o disposto na legislação de proteção de dados pessoais do Brasil e da União Europeia e alertar os usuários sobre os possíveis riscos de violação de privacidade relacionados ao aplicativo.

Com vistas ao desenvolvimento da investigação proposta, inicialmente o texto explora conceitos fundamentais da sociedade tecnológica e as leis de privacidade e proteção de dados vigentes no Brasil e na União Europeia. Em seguida, são analisados detalhadamente os termos de uso do aplicativo Threads, abordando aspectos como o consentimento do usuário, a coleta, uso e compartilhamento de dados pessoais, além das políticas de retenção de dados e os direitos dos usuários. O artigo identifica pontos em conformidade com a legislação e outros que podem levantar preocupações legais. Por fim, são propostas recomendações para que a empresa de tecnologia ajuste seus termos de uso de acordo com as regulamentações de privacidade e proteção de dados do Brasil e da União Europeia, buscando garantir maior transparência e proteção aos direitos dos usuários.

O método de pesquisa é o dedutivo e o método de procedimento é o analítico por meio da pesquisa indireta com a consulta a livros e revistas científicas. Importante salientar que não se busca uma análise exaustiva do conteúdo bibliográfico. A proposta do estudo é situar os

leitores acerca de alguns aspectos relevantes em cada tópico que auxiliem na compreensão geral do questionamento proposto.

## **1. Sociedade tecnológica a proteção de dados pessoais no Brasil e na União Europeia**

O desenvolvimento da tecnologia da internet trouxe ao mundo uma significativa transformação na maneira como a comunicação humana se desenvolve e se desenvolverá, porque, se antes as comunicações tinham uma estrutura vertical, com a mídia tradicional atuando de cima para baixo, informando as pessoas com seus jornais, rádios, revistas e canais de televisão, com o desenvolvimento da internet, especialmente das redes sociais, a comunicação humana passou por uma transformação na sua estrutura, tornando-se também horizontal, proposta em que todos informam todos, em que todos expressam seus pensamentos e suas opiniões, seja na forma de comentários, curtidas ou compartilhamentos de conteúdos.

Essa mudança na estrutura da comunicação humana, aliada ao *big data*, aos algoritmos e à inteligência artificial questiona e analisa a relação existente entre a tecnologia da internet e a habilidade cultural da sociedade para conviver com as inovações tecnológicas oriundas dessa tecnologia, assim como, se estariam preparadas as instituições dos países para assegurar aos cidadãos seus direitos e garantias fundamentais em um ambiente dinâmico como o da internet, tendo para isso, que regulamentar com eficácia e sensibilidade as práticas tecnológicas. Da mesma forma, questiona se estariam as grandes empresas de tecnologia, responsáveis por parcelas cada vez maiores da rede, preparadas para o provimento de um serviço não danoso aos seus usuários, tendo que se adaptar constantemente às imposições do mercado e às necessidades dos usuários.

Nesse ínterim, pretende-se demonstrar, que já no fim do segundo milênio da Era Cristã, vários acontecimentos de importância histórica transformaram o cenário social da vida humana. Uma revolução tecnológica concentrada nas tecnologias da informação começou a remodelar a base material da sociedade em ritmo acelerado. Economias por todo o mundo passaram a manter interdependência global, apresentando uma nova forma de relação entre a economia, o estado e a sociedade em um sistema de geometria variável (CASTELLS, 1999, p. 61). Além disso, um novo sistema de comunicação que fala cada vez mais uma língua universal digital tanto está promovendo a integração global da produção e distribuição de palavras, sons e imagens de nossa cultura como personalizando-os ao gosto das identidades e humores dos indivíduos. As

redes interativas de computadores estão crescendo exponencialmente, criando novas formas e canais de comunicação, moldando a vida e, ao mesmo tempo, sendo moldadas por ela (CASTELLS, 1999, p. 62).

Para Manuel Castells, a primeira característica do novo paradigma é que a informação é sua matéria-prima: são tecnologias para agir sobre a informação, não apenas informação para agir sobre a tecnologia, como foi o caso das revoluções tecnológicas anteriores. O segundo aspecto refere-se à penetrabilidade dos efeitos das novas tecnologias. Como a informação é uma parte integral de toda atividade humana, todos os processos de nossa existência individual e coletiva são diretamente moldados (embora, com certeza, não determinados) pelo novo meio tecnológico. A terceira característica refere-se à lógica de redes em qualquer sistema ou conjunto de relações, usando essas novas tecnologias da informação. A morfologia da rede parece estar bem adaptada à crescente complexidade de interação e aos modelos imprevisíveis do desenvolvimento derivado do poder criativo dessa interação (CASTELLS, 1999, p. 78).

Em quarto lugar, referente ao sistema de redes, mas sendo um aspecto claramente distinto, o paradigma da tecnologia da informação é baseado na flexibilidade. Não apenas os processos são reversíveis, mas organizações e instituições podem ser modificadas, e até mesmo fundamentalmente alteradas, pela reorganização de seus componentes (CASTELLS, 1999, p. 78). A mudança tecnológica, aduzem Moreira e Queiroz, é um processo de ruptura caracterizado pela mudança de patamar produtivo devido ao surgimento de um novo paradigma baseado no desenvolvimento do conhecimento da tecnologia (MOREIRA; QUEIROZ, 2007, p. 1-22).

Nesse diapasão, a sociedade atual, identificada como tecnológica, tem uma economia fortemente guiada pela coleta, armazenamento e proteção de informações e dados pessoais (*data driven economy*). Dessa forma, pesquisadores e analistas do mundo todo analisam e questionam não somente o poder das grandes empresas de tecnologia para com as informações, mas como a atuação dessas corporações está digitalizando os direitos e garantias fundamentais no Brasil e no mundo, utilizando-se o direito na sua condição de estrutura regulatória normativa, institucional, procedimental e organizacional, marcado pelo que se costumou designar de um processo de digitalização, também identificado por transformação digital. Nesse contexto, podemos destacar quatro gerações de leis de proteção de dados pessoais.

Na década de 1970, surgiu a primeira geração da proteção de dados como resultado do processamento eletrônico de informações nas instituições públicas e privadas, bem como da

ideia de centralizar bancos de dados nacionais. Notáveis exemplos incluem a Lei do Estado Alemão de Hesse (1970), a Lei de Proteção de Dados da Suécia (1973) e a Lei Federal de Proteção de Dados da Alemanha (1977). Essas legislações enfatizavam o controle rígido dos procedimentos, porém negligenciavam a salvaguarda da privacidade.

A segunda geração surge como uma resposta à disseminação e proliferação dos bancos de dados existentes, levando à associação da proteção de dados com a privacidade, as liberdades individuais e as liberdades negativas. Nessa fase, a proteção de dados foi incorporada às Constituições de Portugal e Espanha. Além disso, destaca-se a promulgação da Lei Francesa de Proteção de Dados Pessoais (1978). Essa nova abordagem buscava assegurar que os dados fossem tratados de forma a preservar a privacidade e a liberdade pessoal dos indivíduos.

Na década de 1980, surge a terceira geração, caracterizada pela busca de uma tutela mais sofisticada dos dados pessoais, por meio da ideia de autodeterminação informativa. Nessa abordagem, destaca-se o enfraquecimento do controle absoluto das instituições sobre os dados pessoais, em prol do controle exercido pelo próprio indivíduo. Essa perspectiva encoraja uma participação mais ativa do indivíduo em todas as etapas do processo, desde a coleta até a transmissão dos dados, e não se restringe a uma escolha binária de "tudo ou nada". Essa evolução foi influenciada pelas tecnologias de rede e telecomunicações que surgiram nessa época. Legislações relevantes desta época incluem a Lei Alemã de Proteção de Dados (1990), a Emenda da Lei da Áustria (1986) e a previsão constitucional da proteção de dados pessoais na Holanda.

Já a quarta geração, busca fundamentar a proteção dos dados pessoais não apenas na escolha individual, mas também na implementação de instrumentos que elevem o padrão coletivo de proteção. Destacam-se nessa fase a Diretiva n. 2000/58/CE sobre privacidade e comunicações eletrônicas, o Regulamento Geral sobre a Proteção de Dados (RGPD) e a Lei Geral de Proteção de Dados (LGPD). Essas normativas representam um avanço significativo ao estabelecerem diretrizes mais abrangentes e padronizadas para proteger a privacidade e a segurança dos dados em todo o espaço europeu e também no Brasil. Além de enfatizar os direitos individuais, tais medidas visam garantir uma salvaguarda mais efetiva dos dados em um contexto coletivo, considerando o impacto mais amplo das atividades de processamento de dados na sociedade como um todo.

Implementado em maio de 2018, o RGPD estabeleceu diretrizes e regras claras para o tratamento de informações pessoais por empresas e organizações que atuam na União Europeia ou lidam com dados de cidadãos europeus. Essa legislação proporciona aos indivíduos maior controle sobre suas informações pessoais e impõe responsabilidades rigorosas às organizações que coletam, armazenam e processam dados pessoais. O Regulamento estabelece uma base sólida para a proteção dos dados pessoais, promovendo a privacidade e a segurança dos cidadãos europeus em um cenário digital em constante evolução (UNIÃO EUROPEIA, 2016).

Já no Brasil, a LGPD entrou em vigor em agosto de 2020 e estabelece regras claras para o tratamento de dados pessoais por empresas e órgãos públicos. A Lei prevê que os titulares dos dados têm direito à informação sobre o tratamento de seus dados, bem como a correção, exclusão e anonimização dessas informações (BRASIL, 2018). O advento da LGPD no contexto de consolidação de um panóptico digital evidencia o seu papel de reforçar o devido e imprescindível controle que as pessoas precisam exercer sobre seus dados pessoais. Nessa perspectiva, Ana Frazão compreende que a Lei se apresenta como um “freio e um agente transformador das técnicas atualmente utilizadas pelo capitalismo de vigilância, a fim de conter a maciça extração de dados e as diversas aplicações e utilizações que a eles podem ser dadas” (FRAZÃO, 2019, p. 103).

Nesse contexto, convém destacar o papel desempenhado pela Proposta de Emenda Constitucional nº 17/2019, que foi promulgada em fevereiro de 2022 e acrescentou o inciso LXXIX ao artigo 5º da Constituição, dispondo que “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais” (BRASIL, 1988). Diante do exposto, pode-se afirmar que a proteção de dados pessoais como um direito fundamental fez com que a proteção de dados pessoais estivesse presente em todas as relações jurídicas, trazendo segurança jurídica e diminuindo as assimetrias de poder entre os envolvidos, beneficiando a população brasileira.

Em linhas gerais, compreende-se que a proteção de dados é uma questão de importância global, com o objetivo de preservar os direitos individuais e evitar que abusos sejam cometidos. Essa abordagem visa garantir que as pessoas possam ser quem desejam ser, sem medo de que suas informações pessoais sejam exploradas indevidamente. A busca por leis e regulamentos eficazes sobre o tema é fundamental para assegurar a privacidade e a dignidade de cada indivíduo na era digital.

## 2. Threads: uma análise jurídica sobre os termos de uso do aplicativo

A rápida expansão do Threads tem gerado preocupação entre a comunidade jurídica, que alerta sobre muitos usuários não estarem cientes da extensão das informações coletadas pela plataforma. A Política de Privacidade suplementar do Threads é um complemento à Política do Instagram e da Meta, mas acrescenta algumas coletas adicionais de dados para viabilizar sua interoperabilidade planejada com serviços de terceiros e para outras razões que não estão completamente claras (WOLFORD, 2023).

Graças aos requisitos de privacidade da App Store (Apple) e do Google Play, temos informações específicas sobre os dados que o Threads coleta. De acordo com a App Store, o aplicativo solicita permissão para acessar dados de: saúde e condicionamento físico; compras; informações financeiras; localização; informações de contato; contatos; conteúdo do usuários (mensagens no aplicativo, fotos ou vídeos, conteúdo de jogabilidade, suporte ao cliente, dados de áudio, além de outros conteúdos); histórico de buscas; histórico de navegação; identificados; informações de uso; informações confidenciais/sensíveis (inclui dados raciais ou étnicos, orientação sexual, informações sobre gravidez ou parto, deficiência, crenças religiosas ou filosóficas, filiação a sindicatos, opinião política, informações genéticas ou dados biométricos); diagnóstico (dados de falhas, dados de desempenho, além de outros dados de diagnósticos); e outros dados (APP STORE, 2023). Além desses dados, o Google Play informa que o Threads solicita permissão para acessar dados como: Mensagens (e-mails, SMS ou MMS e outras mensagens no app); Áudio (gravações de voz ou som, arquivos de música e outros arquivos de áudio) e Agenda (eventos da agenda) (GOOGLE PLAY, 2023).

Para além de publicidade, análises, personalização e funcionalidades do aplicativo, há também uma categoria de "outros propósitos" para os quais o Threads coleta muitas das informações listadas acima. O aplicativo não fornece detalhes sobre esses outros propósitos. Contudo, se você estiver utilizando o dispositivo iOS, é possível ativar o recurso de Relatório de Privacidade do Aplicativo e verificar como os aplicativos estão usando as permissões de privacidade que você concedeu a eles (WOLFORD, 2023).

O aplicativo foi lançado em mais de cem países no dia 5 de julho de 2023, contudo, a empresa adiou o seu lançamento na União Europeia (UE) devido às regulamentações relacionadas ao uso de dados pessoais pelas empresas. Embora os reguladores da UE não tenham impedido a empresa de lançar o Threads, fontes sugerem que, em sua forma atual, o aplicativo pode violar uma ou várias das seguintes regulamentações: 1) O *General Data Protection Regulation* (GDPR), que estabelece como os controladores de dados devem coletar,

usar e proteger dados pessoais; 2) O *Digital Markets Act* (DMA) e o *Digital Services Act* (DSA), que formam um único conjunto de regras que se aplicam em toda a UE, com o objetivo de criar um espaço digital mais seguro em que os direitos fundamentais de todos os usuários de serviços digitais sejam protegidos (WOLFORD, 2023). Além disso, é nítida a preocupação com a falta de transparência em relação ao uso de dados pessoais sensíveis.<sup>4</sup>

Na visão de Calli Schroeder, conselheira global de privacidade do *Electronic Privacy Information Center* (Epic), uma organização sem fins lucrativos dedicada à proteção da privacidade digital, várias preocupações sobre a privacidade relacionadas ao Threads estão associadas ao histórico da Meta em práticas preocupantes de privacidade. A conselheira afirmou que não viu evidências de que a Meta está sendo transparente em relação ao uso de dados pessoais sensíveis ou estabelecendo claramente as razões para coletar esses dados, além de simplesmente dizer "porque queremos".<sup>5</sup>

A extensa lista de práticas que preocupa especialistas, como Schroeder, inclui a situação em que a Meta recebeu multas por coletar dados pessoais sensíveis sem obter o consentimento adequado, violando o RGPD, na União Europeia.<sup>6</sup> Conforme Johana Bhuiyan, repórter de tecnologia do *The Guardian US*, quando combinadas, todas essas informações captadas pelo Threads podem criar um mapa extremamente detalhado e complexo das vidas das pessoas, especialmente quando consideradas juntamente com todos os dados já coletados pela Meta por meio do Facebook, Instagram e Meta Pixel (BHUIYAN, 2023).

O Meta Pixel, um pequeno código que pode ser adicionado a sites, rastreia e analisa a atividade dos visitantes, e vários conjuntos de dados resultantes são compartilhados com a Meta.<sup>7</sup> Por exemplo, conforme Darius Tahir e Simon Fondrie-Teitler, diversas farmácias e redes

---

<sup>4</sup> Sobre o tema, anota a doutrina que, “de modo a promover a dignidade da pessoa humana, a privacidade e a identidade pessoal, a proteção intensificada dos dados sensíveis revela-se fundamental, permitindo que a pessoa humana se realize na sua vida de relação, a salvo de qualquer discriminação ilícita ou abusiva, levando-se em conta suas características peculiares”. (DE LUCCA; MARTINS, 2022, p. 11).

<sup>5</sup> Trecho da entrevista concedida por Calli Schroeder para Johana Bhuiyan, repórter de tecnologia do *The Guardian US*. (BHUIYAN, 2023)

<sup>6</sup> Em janeiro de 2022, a Autoridade de Proteção de Dados (DPC) da Irlanda multou a Meta em €390 milhões. A infração está relacionada ao uso dos dados dos usuários para anúncios personalizados no Facebook e no Instagram, ambas redes sociais pertencentes ao grupo Meta. A União Europeia considerou que essa prática viola o RGPD. As multas foram aplicadas pelo regulador irlandês porque o escritório da empresa norte-americana na Europa está localizado em Dublin. Uma das penalidades, no valor de €210 milhões, foi direcionada ao Facebook, enquanto a outra, no montante de €180 milhões, foi destinada ao Instagram. Em novembro de 2022 e em maio de 2023, a empresa foi multada em €265 milhões e €1.2 mil milhões, respectivamente, também por violar o RGPD.

<sup>7</sup> Trata-se de um trecho de código JavaScript que permite a você rastrear a atividade dos visitantes do seu site. Ele funciona por meio do carregamento de uma pequena biblioteca de funções que poderá ser usada sempre que o visitante de um site fizer uma ação (chamada de evento) que você quer rastrear (chamada de conversão). As conversões rastreadas aparecem no gerenciador de anúncios, onde podem ser usadas para mensurar a eficiência dos anúncios, definir públicos personalizados para o direcionamento de anúncios e para campanhas de anúncios de Catálogo Advantage+, bem como analisar a eficiência dos funis de conversão do seu site.

de supermercados, como Costco, CVS, Sam's Club e Walmart compartilham informações sensíveis com a Meta e outras plataformas sociais por meio do Pixel, incluindo detalhes sobre se os consumidores adicionarem ao carrinho virtual produtos como Plan B,<sup>8</sup> testes de HIV, gravidez e vitaminas pré-natal (TAHIR; FONDRIE-TEITLER, 2023).

De acordo com Bruno Bioni, diretor fundador do Data Privacy Brasil, uma entidade civil sem fins lucrativos dedicada à proteção de dados pessoais, tecnologia e direitos fundamentais, o acesso a dados financeiros e de saúde parece ser excessivo no contexto de redes sociais. Bioni argumenta que é necessário justificar uma finalidade proporcional para esse tipo de uso. A empresa Meta alega que utiliza esses dados para análises, funcionamento do aplicativo, prevenção de fraudes e gerenciamento de contas. Entretanto, o fundador do Data Privacy Brasil considera essas alegações vagas (TEIXEIRA, 2023).

Em 24 de julho de 2023, a Autoridade Nacional de Proteção de Dados brasileira (ANPD) informou que iniciará a fiscalização da nova rede social. Essa medida veio após estudos preliminares conduzidos pela Coordenação-Geral de Tecnologia e Pesquisa (CGTP) sobre o tratamento de dados pessoais realizados na plataforma. O Conselho Diretor da ANPD solicitou a análise inicial devido às preocupações manifestadas por especialistas em proteção de dados, pela imprensa e por instituições internacionais. Com base nos estudos, o Conselho entendeu a necessidade de aprofundar a análise sobre o tratamento de dados pessoais na nova rede social e adotar medidas de monitoramento fiscalizatório (ANPD, 2023).

A vasta coleta de dados pela empresa Meta tem um objetivo específico: a venda de anúncios. Em uma reunião da ANPD com a Meta, foi esclarecido que o Threads *ainda* não realiza a monetização por meio do tratamento de dados pessoais, diferentemente do Instagram, e não exibe anúncios ou publicidade personalizada. A intenção futura é integrar o Threads ao protocolo ActivityPub para torná-lo uma rede social descentralizada (ANPD, 2023).

Em julho de 2023, o Threads ainda não apresenta anúncios, mas especialistas preveem que isso certamente acontecerá no futuro. Enquanto isso, as informações coletadas no Threads podem ser utilizadas como parte do extenso ecossistema de dados que a Meta utiliza para exibir anúncios em suas outras plataformas (BHUIYAN, 2023).

De acordo com Carissa Veliz (2023), professora associada do Instituto de Ética em Inteligência Artificial da Universidade de Oxford, não apenas a Meta não alterou seu modelo

---

<sup>8</sup> Plan B é uma contracepção de emergência que você toma dentro de 72 horas após uma relação sexual desprotegida. A marca afirma que quanto mais cedo você o tomar, melhor ele funciona. No site oficial, destaca-se as seguintes informações: a) Ajuda a prevenir a gravidez antes que ela ocorra; b) Não é necessário apresentar identificação ou receita médica para comprar; c) Não prejudica suas chances de engravidar no futuro. (PLAN B, 2023).

de negócio, mas continua buscando anúncios direcionados, essencialmente publicidade baseada em vigilância. Na visão de Johana Bhuiyan (2023), a empresa está empenhada em coletar o máximo possível de dados e segue na mesma direção desde o início, mesmo diante de todos os escândalos, críticas públicas, advertências regulatórias e multas. Não há uma reavaliação do modelo de negócios para torná-lo mais respeitoso com os usuários.

Uma preocupação, segundo Veliz (2023), é a sensibilidade dos dados coletados pela empresa. Eles podem incluir orientação sexual, raça, etnia, dados biométricos, filiação a sindicatos, status de gravidez, preferências políticas e crenças religiosas. E todos esses dados têm o potencial de serem compartilhados com terceiros. Essas terceiras partes incluem profissionais de marketing e agências de aplicação da lei.

Consoante Emil Vazquez (2023), porta-voz da Meta, a empresa internamente filtra dados sensíveis, como informações de saúde, orientação sexual e visões religiosas, para que não sejam utilizados em publicidade. Contudo, grande parte dessas informações permanece vulnerável a solicitações das autoridades, das quais a Meta recebeu quase 240.000 globalmente no segundo semestre de 2022, sendo 17.421 apenas do Brasil (META, 2023).

No entendimento de Ben Wolford (2023), o aplicativo Threads poderia ter sido desenvolvido de forma mais limitada, como os aplicativos Mastodon<sup>9</sup> ou o Bluesky,<sup>10</sup> coletando menos dados dos usuários. No entanto, a escolha da Meta foi oposta, buscando coletar o máximo possível de dados pessoais, mesmo que isso implicasse inicialmente perder o mercado europeu (WOLFORD, 2023).

Para Wolford, essas decisões de design são resultado do modelo de negócio da empresa, que trata as pessoas como produtos para serem vendidos a anunciantes, o que contrasta com a visão de uma internet que prioriza a privacidade e trata as pessoas como clientes. Apesar dos anos de fiscalização dos reguladores em relação à privacidade e das multas altíssimas aplicadas pela União Europeia à empresa, não há garantia de que a Meta vá mudar seus produtos para proteger a privacidade das pessoas. Portanto, por enquanto, a responsabilidade pela privacidade on-line ainda recai sobre os próprios usuários (WOLFORD, 2023). Dentro desse cenário, o próximo tópico aborda algumas sugestões de melhorias para o aplicativo Threads, com o propósito de assegurar maior transparência e proteção aos usuários.

---

<sup>9</sup> Mastodon é uma rede social federada, distribuída, que faz parte do Fediverso, uma rede descentralizada e interligada de servidores operados de maneira independente. O Mastodon tem recursos de microblogging semelhantes ao Twitter.

<sup>10</sup> Bluesky ou Bluesky Social é um protocolo de uma nova rede social em desenvolvimento, com o destaque de ser uma rede social descentralizada.

### 3. Propostas de adequação: em busca de maior transparência e proteção dos usuários

Como visto, a rápida expansão do aplicativo Threads tem gerado preocupação entre a comunidade jurídica, devido à extensão das informações coletadas pela plataforma. O lançamento do aplicativo na União Europeia (UE) foi adiado devido às regulamentações relacionadas ao uso de dados pessoais pelas empresas. Fontes sugerem que, em sua forma atual, o aplicativo pode violar uma ou várias regulamentações da UE.<sup>11</sup>

No contexto brasileiro, “além de se realizar uma proteção mais ampla dos dados sensíveis, tal proteção também deverá ser observada nos casos em que houver tratamento sensível de dados pessoais” (TEFFÉ, 2022, p. 39), a denotar regime ampliado que qualifica a proteção defendida na tese e que se coaduna com importante enunciado, de nº 690, aprovado por ocasião da IX Jornada de Direito Civil do Conselho da Justiça Federal, em maio de 2022, com os seguintes dizeres: “a proteção ampliada conferida pela LGPD aos dados sensíveis deverá ser também aplicada aos casos em que houver tratamento sensível de dados pessoais, tal como observado no §1º do art. 11 da LGPD”. Disso surge a necessidade de aprimoramento das estruturas de proteção dos usuários da plataforma, o que demanda sistematização específica.

Como salienta Vincenzo Zeno-Zencovich (2009, p. 22), os dados pessoais, “do nascimento à morte”, são tratados “milhares de vezes ao dia”, passando a ser uma “disciplina da vida cotidiana do sujeito e suas cotidianas relações sociais”. Com base nisso, é possível apresentar algumas propostas para incrementar a transparência e a proteção dos usuários no Threads. Uma dessas propostas é fornecer aos usuários divulgação clara e detalhada dos dados que o aplicativo coleta, incluindo informações sobre como esses dados são usados e com quem são compartilhados (TRUDEL, 2009, p. 322). Isso pode ser feito por meio de política de privacidade acessível, bem como por meio de notificações e avisos no aplicativo (UTZ; MICHELS; DEGELING et al, 2023).

Outra proposta importante é fornecer aos usuários opções de controle de privacidade robustas, permitindo escolhas sobre quais dados compartilhar e sobre como esses dados são usados. Isso pode incluir a capacidade de desativar certas coletas de dados ou limitar o compartilhamento de dados com terceiros. Além disso, é fundamental que o Threads seja transparente sobre os “outros propósitos” para os quais coleta dados, fornecendo aos usuários informações claras e detalhadas sobre como esses dados são usados e por que são necessários,

---

<sup>11</sup> Não é por outra razão que se realça a importância da proteção a categorias mais particulares, inclusive na União Europeia: “These categories of personal data merit specific protection as they allow conclusions about an individual that are linked to his fundamental rights and freedoms, and their processing might entail high risks for the latter” (VOIGT; VON DEM BUSSCHE, 2017, p. 110).

em atendimento ao princípio da finalidade, que deve nortear as atividades de tratamento de dados pessoais.<sup>12</sup>

Para garantir a conformidade com as regulamentações locais, o Threads deve cumprir todas as leis relacionadas à privacidade e proteção de dados. Isso pode incluir a implementação de medidas técnicas e organizacionais para garantir a segurança dos dados dos usuários. Além disso, o aplicativo pode se submeter a auditorias independentes para avaliar suas práticas de privacidade e proteção de dados, demonstrando seu compromisso com a transparência e a responsabilidade (KAMINSKI, 2021, p. 121).

Manter uma comunicação aberta com os usuários também é fundamental, em cumprimento ao fundamento normativo da autodeterminação informativa. Em síntese, o Threads deve informar seus usuários sobre quaisquer mudanças em suas práticas de privacidade ou uso de dados e responder às preocupações dos usuários de maneira transparente e responsável.<sup>13</sup> Além disso, o aplicativo pode investir em programas de educação do usuário para incrementar a compreensão sobre como os dados são coletados, usados e protegidos, bem como fornecer dicas e orientações sobre como gerenciar opções de privacidade no aplicativo. Isso porque, no contexto sob análise, a autodeterminação informativa se refere ao direito dos indivíduos de controlar suas próprias informações pessoais, incluindo como essas informações são coletadas, usadas e compartilhadas (LYNSKEY, 2015, p. 50). Esse conceito está intimamente relacionado ao tema discutido anteriormente, pois as práticas de privacidade do Threads têm um impacto direto na capacidade dos usuários de exercer sua autodeterminação informativa<sup>14</sup>.

Ao adotar essas medidas, o Threads pode ajudar a garantir que os usuários tenham a capacidade de exercer sua autodeterminação informativa, controlando suas próprias informações pessoais e tomando decisões informadas sobre como essas informações são usadas.

---

<sup>12</sup> Sobre tal princípio, descreve Arthur Pinheiro Basan: “O princípio da finalidade é expressamente conceituado como o dever de realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular. Não obstante, o próprio texto legal destaca a impossibilidade de o tratamento posterior ser realizado de maneira incompatível com a finalidade definida *a priori*” (BASAN, 2022, p. 59).

<sup>13</sup> Nesse contexto, torna-se relevante o debate sobre *compliance* digital na dimensão específica que as boas práticas em relação a dados pessoais podem ter para o incremento do controle informacional do usuário, especialmente porque “não há dúvidas de que se está diante de um novo contexto para a regulação social, a demandar novas maneiras de se encarar a própria noção de risco. Para isso, pode-se partir de uma proposta que conjugue o *compliance* digital com rotinas de priorização da proteção de dados pessoais (a exemplo da *privacy by design*), com vistas à melhor moldagem dos critérios de responsabilização” (MARTINS; FALEIROS JÚNIOR, 2021, p. 291).

<sup>14</sup> Isso tudo em razão da proximidade axiológica que tal proteção adquire ao se considerar que, “possivelmente, o fundamento constitucional direto mais próximo de um direito fundamental à proteção de dados seja mesmo o direito ao livre desenvolvimento da personalidade, radicado diretamente no princípio da dignidade da pessoa humana e no direito geral de liberdade, o qual também assume a condição de uma cláusula geral de proteção de todas as dimensões da personalidade humana”. (SARLET, 2020, p. 185).

Isso é fundamental para promover a confiança dos usuários na plataforma e garantir que seus direitos e interesses sejam respeitados e protegidos (VAN ALSENOY, 2019, p. 317-318).

Além das propostas mencionadas anteriormente, existem outras medidas que o Threads pode adotar para incrementar sua transparência e a proteção dos usuários. Por exemplo, o aplicativo pode implementar tecnologias de privacidade avançadas, como criptografia de ponta a ponta e anonimização de dados, para garantir que as informações dos usuários sejam protegidas contra acessos não autorizados. Além disso, o Threads pode adotar uma abordagem proativa em relação à proteção de dados, monitorando regularmente suas práticas de coleta e uso de dados para garantir que estejam em conformidade com as regulamentações locais e as expectativas dos usuários<sup>15</sup>.

Por fim, a empresa Meta, proprietária do Threads, deve demonstrar adequada *accountability* em relação às boas práticas de privacidade do aplicativo, garantindo que os direitos e interesses dos usuários sejam respeitados e protegidos (FALEIROS JÚNIOR, 2020, p. 210). Ao implementar essas propostas, o Threads pode incrementar sua transparência e proteção dos usuários, promovendo confiança e segurança em sua plataforma.

### **Considerações finais**

A análise dos termos de uso do aplicativo Threads revelou que, embora muitos aspectos estejam em conformidade com as leis de privacidade e proteção de dados do Brasil e da União Europeia, ainda existem pontos que podem levantar preocupações legais. É importante que a empresa Meta ajuste seus termos de uso de acordo com as regulamentações de privacidade e proteção de dados dessas regiões, buscando garantir maior transparência e proteção aos direitos dos usuários. O lançamento do aplicativo na União Europeia (UE) foi adiado devido às regulamentações relacionadas ao uso de dados pessoais pelas empresas. Fontes sugerem que, em sua forma atual, o aplicativo pode violar uma ou várias regulamentações da UE. No contexto brasileiro, a proteção dos dados sensíveis é ampla e deve ser observada nos casos em que houver

---

<sup>15</sup> Comenta a doutrina: “As características peculiares da hipótese de responsabilidade civil em questão – que se expressam principalmente na regulação detalhada das obrigações comportamentais do controlador e do operador de dados, com um novo foco no perfil de gerenciamento de riscos, especialmente relacionado ao uso da inovação tecnológica – possibilita garantir a efetividade do recurso de compensação, adaptando-o às especificidades da atividade de processamento de dados pessoais e aos requisitos de proteção que ele apresenta. Desse modo, criou-se um modelo, por assim dizer, mais maduro de responsabilização civil, no qual se vai além da responsabilidade dos agentes, tendo-se em vista, especialmente, a evitação de danos. Admitida sua natureza multifuncional, não foram postos obstáculos ao lançamento dessa figura complexa de responsabilidade especial descrita pelos art. 42 e seguintes da LGPD, no mesmo feitiço do regulamento europeu” (MORAES; QUEIROZ, 2019, p. 133-134).

tratamento sensível de dados pessoais. Isso surge a necessidade de aprimoramento das estruturas de proteção dos usuários da plataforma, o que demanda sistematização específica.

Assim como a senhora italiana alerta os turistas desavisados sobre os perigos dos batedores de carteira ("*Attenzione pickpocket!*"), é importante que os usuários do aplicativo Threads estejam cientes dos possíveis riscos de violação de privacidade relacionados ao uso do aplicativo. É fundamental que os usuários leiam atentamente os termos de uso e as políticas de privacidade antes de compartilhar suas informações pessoais com qualquer plataforma on-line.

Além disso, é importante que os usuários estejam cientes de seus direitos em relação à coleta, uso e compartilhamento de seus dados pessoais. As leis de proteção de dados do Brasil e da União Europeia garantem aos usuários o direito de acessar, retificar e excluir seus dados pessoais, bem como o direito de se opor ao processamento de seus dados em determinadas circunstâncias.

A internet trouxe uma significativa transformação na maneira como a comunicação humana se desenvolve, permitindo que todos informem todos e expressando seus pensamentos e opiniões. No entanto, é importante que essa liberdade não seja usada para violar a privacidade e os direitos dos usuários. É fundamental que as empresas de tecnologia respeitem as leis de privacidade e proteção de dados e garantam a transparência e a proteção dos direitos dos usuários. Para incrementar a transparência e a proteção dos usuários no Threads, algumas propostas podem ser apresentadas. Uma dessas propostas é fornecer aos usuários divulgação clara e detalhada dos dados que o aplicativo coleta, incluindo informações sobre como esses dados são usados e com quem são compartilhados. Outra proposta importante é fornecer aos usuários opções de controle de privacidade robustas, permitindo escolhas sobre quais dados compartilhar e sobre como esses dados são usados. Além disso, é fundamental que o Threads seja transparente sobre os “outros propósitos” para os quais coleta dados, fornecendo aos usuários informações claras e detalhadas sobre como esses dados são usados e por que são necessários. Para garantir a conformidade com as regulamentações locais, o Threads deve cumprir todas as leis relacionadas à privacidade e proteção de dados.

Por fim, é importante salientar que a responsabilidade pela proteção da privacidade e dos dados pessoais não recai apenas sobre as empresas de tecnologia, mas também sobre os próprios usuários. É fundamental que os usuários estejam cientes dos possíveis riscos relacionados ao compartilhamento de suas informações pessoais on-line e tomem medidas para proteger sua privacidade. Afinal, assim como a senhora italiana alerta os turistas desavisados sobre os perigos dos batedores de carteira, é importante que todos estejamos atentos aos possíveis riscos relacionados ao uso das plataformas on-line.

## Bibliografia

ANPD. Autoridade Nacional de Proteção de Dados. *ANPD fiscaliza a rede social Threads*. Publicado em: 24 jul. 2023. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-fiscaliza-a-rede-social-threads>. Acesso em: 25 jul. 2023.

APP STORE. *Threads, an Instagram app*. Publicado em: 05 jul. 2023. Disponível em: <https://apps.apple.com/br/app/threads-an-instagram-app/id6446901002>. Acesso em: 25 jul. 2023.

BASAN, Arthur Pinheiro. Artigo 6º. In: MARTINS, Guilherme Magalhães; LONGHI, João Victor Rozatti; FALEIROS JÚNIOR, José Luiz de Moura (coord.). *Comentários à Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018)*. Indaiatuba: Foco, 2022, p. 53-66.

BHUIYAN, Johana. *As Threads app thrives, experts warn of Meta's string of privacy violations*. Publicado em: 11 jul. 2023. Disponível em: <https://www.theguardian.com/technology/2023/jul/11/threads-app-privacy-user-data-meta-policy>. Acesso em: 25 jul. 2023.

BRASIL. *Constituição da República Federativa do Brasil de 1988*. Disponível em: [http://www.planalto.gov.br/ccivil\\_03/constituicao/constituicao.htm](http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm). Acesso em: 30 abr. 2023.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Disponível em: [https://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/113709.htm](https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm). Acesso em: 31 jul. 2023.

CASTELLS, Manuel. *A Era da Informação: Economia, Sociedade e Cultura*. v. 1. A Sociedade em Rede. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 1999.

DE LUCCA, Newton; MARTINS, Guilherme Magalhães. A tutela dos dados pessoais sensíveis na Lei Geral de Proteção de Dados. In: SCHREIBER, Anderson; MARTINS, Guilherme Magalhães; CARPENA, Heloísa (coord.). *Direitos fundamentais e sociedade tecnológica*. Indaiatuba: Foco, 2022, p. 1-13.

DPC IRELAND. *Data Protection Commission announces conclusion of two inquiries into Meta Ireland*. Publicado em: 04 jan. 2023. Disponível em: <https://www.dataprotection.ie/en/news-media/data-protection-commission-announces-conclusion-two-inquiries-meta-ireland>. Acesso em: 25 jul. 2023.

FALEIROS JÚNIOR, José Luiz de Moura. *Accountability e devida diligência como vetores da governança corporativa nos mercados ricos em dados*. *Revista Semestral de Direito Empresarial*, Rio de Janeiro, n. 26, p. 183-211, jan./jun. 2020.

FRAZÃO, Ana. Objetivos e alcance da Lei Geral de Proteção de Dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena D. (Coord). *Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro*. 1 ed. São Paulo: Thomson Reuters Brasil, 2019.

GOOGLE PLAY. *Threads, an Instagram app*. Publicado em: 05 jul. 2023. Disponível em: <https://play.google.com/store/apps/datasafety?id=com.instagram.barcelona&gl=it>. Acesso em: 25 jul. 2023.

INSTAGRAM. *Política de Privacidade Suplementar do Threads*. Publicado em: 05 jul. 2023. Disponível em: <https://help.instagram.com/515230437301944>. Acesso em: 25 jul. 2023.

KAMINSKI, Margot E. Understanding Transparency in Algorithmic Accountability. In: BARFIELD, Woodrow (ed.). *The Cambridge Handbook of the Law of Algorithms*. Cambridge: Cambridge University Press, 2021, p. 121-140.

LYNSKEY, Orla. *The foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015.

MARTINS, Guilherme Magalhães; FALEIROS JÚNIOR, José Luiz de Moura. Compliance digital e responsabilidade civil na Lei Geral de Proteção de Dados. In: MARTINS, Guilherme Magalhães; ROSENVALD, Nelson (coord.). *Responsabilidade civil e novas tecnologias*. Indaiatuba: Foco, 2021, p. 263-297.

META. *Government Requests for User Data*. Disponível em: <https://transparency.fb.com/data/government-data-requests/>. Acesso em: 25 jul. 2023.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGPD. *Cadernos Adenauer*, Rio de Janeiro, n. 3, p. 113-135, out. 2019.

MOREIRA, D. A.; QUEIROZ, A. C. S. Inovação: conceitos fundamentais. In: MOREIRA, Daniel Augusto; QUEIROZ, Ana Carolina S. (Coord.). *Inovação Organizacional e Tecnológica*. São Paulo: Thomson Learning, 2007.

PLAN B. *What is Plan B?* Disponível em: <https://www.planbonestep.com/>. Acesso em: 25 jul. 2023.

SARLET, Ingo Wolfgang. Proteção de dados pessoais como direito fundamental na Constituição Federal brasileira de 1988: contributo para a construção de uma dogmática constitucionalmente adequada. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 14, n. 42, p. 179-218, jan./jun. 2020.

TAHIR, Darius. FONDRIE-TEITLER, Simon. *Need to Get Plan B or an HIV Test Online? Facebook May Know About It*. Publicado em: 30 jun. 2023. Disponível em: <https://themarkup.org/pixel-hunt/2023/06/30/need-to-get-plan-b-or-an-hiv-test-online-facebook-may-know-about-it>. Acesso em: 25 jul. 2023.

TEFFÉ, Chiara Spadaccini de. *Dados pessoais sensíveis: qualificação, tratamento e boas práticas*. Indaiatuba: Foco, 2022.

TEIXEIRA, Pedro. *Instagram lança Threads, app de textos que vai concorrer com o Twitter*. Publicado em: 05 jul. 2023. Disponível em: <https://www1.folha.uol.com.br/tec/2023/07/instagram-lanca-threads-app-de-textos-que-vai-concorrer-com-o-twitter.shtml>. Acesso em: 24 jul. 2023.

TRUDEL, Pierre. Privacy protection on the Internet: risk management and networked normativity. In: GUTWIRTH, Serge; POULLET, Yves; DE HERT, Paul et al (ed.). *Reinventing data protection?* Cham: Springer, 2009, p. 317-334.

UNIÃO EUROPEIA. *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016*. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679>. Acesso em: 22 jun. 2023.

UTZ, Christine; MICHELS, Matthias; DEGELING, Martin et al. Comparing large-scale privacy and security notifications. *Proceedings on Privacy Enhancing Technologies*, v. 1, p. 173-193, Lausanne: Université de Lausanne, 2023. Disponível em: <https://doi.org/10.56553/popets-2023-0076> Acesso em: 25 jul. 2023.

VAN ALSENOY, Brendan. *Data protection law in the EU: roles, responsibilities and liability*. Cambridge: Intersentia, 2019.

VELIZ, Carissa. Entrevista. Entrevistadora: Johana Bhuiyan. *As Threads app thrives, experts warn of Meta's string of privacy violations*. Publicado em: 11 jul. 2023. Disponível em: <https://www.theguardian.com/technology/2023/jul/11/threads-app-privacy-user-data-meta-policy>. Acesso em: 25 jul. 2023.

VOIGT, Paul; VON DEM BUSSCHE, Axel. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Cham: Springer, 2017.

ZENO-ZENCOVICH, Vincenzo. La 'Comunione' di dati personali. Un contributo al Sistema dei Diritti della Personalità. *Il Diritto dell'Informazione e dell'Informatica*, Roma, ano XXV, n. 1, p. 5-22, jan./fev. 2009.