Revista Direito e Praxis

[Artigos inéditos]

O direito constitucional à proteção de dados e o tratamento dos dados pessoais: análise lexical da Política de Privacidade do *TikTok* a partir do *software Iramuteq*

The constitutional right to data protection and the processing of personal data: a lexical analysis of Tiktok's Privacy Policy using Iramuteq software

Elvis Gomes Marques Filho[1]
[1] Universidade Estadual do Piauí, Picos, Piauí, Brasil. E-mail: elvisfilho@pcs.uespi.br. ORCID: https://orcid.org/0000-0003-2681-6094.

Carlos Mendes Monteiro da Rocha[2]
[2] Universidade Federal do Piauí, Teresina, Piauí, Brasil. E-mail: carlosmendes@uespi.br. ORCID: https://orcid.org/0000-0002-1943-1930.

Ernandes Antônio de Sousa[3]
[3] Instituto Educacional Raimundo Sá, Picos, Piauí, Brasil. E-mail: ernandessousa343@gmail.com. ORCID: https://orcid.org/0000-0001-5532-692X.

Francisco de Assis de Oliveira Santos[4]
[4] Universidade Estadual do Piauí, Picos, Piauí, Brasil. E-mail: franciscodeassisdeosantos@aluno.uespi.br. ORCID: https://orcid.org/0009-0001-4302-3726.

Thyago Felype de Moura Brito[5]
[5] Universidade Estadual do Piauí, Picos, Piauí, Brasil. E-mail: tfdemourabrito@aluno.uespi.br. ORCID: https://orcid.org/0000-0002-3436-3219.

Ludimila Lorrane de Sousa Campelo[6]
[6] Universidade Estadual do Piauí, Picos, Piauí, Brasil. E-mail: ludimila.l.de.sousa.campelo@aluno.uespi.br. ORCID: https://orcid.org/0009-0007-1129-965X.

Guilherme Isidorio da Rocha Abreu[7]
[7] Universidade Estadual do Piauí, Picos, Piauí, Brasil. E-mail: guilhermeisidoriodara@aluno.uespi.br. ORCID: https://orcid.org/0009-0003-7772-9713.

Artigo recebido em 09/12/2023 e aceito em 16/11/2024.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Resumo

O presente trabalho tem como objetivo geral analisar como é feito o tratamento e a utilização de dados pessoais dos usuários das redes sociais, particularmente do Tiktok, bem como se há a observância ao ordenamento jurídico que tutela a proteção de dados pessoais. Quanto à metodologia, esta pesquisa se classifica como bibliográfica, documental e qualitativa. Para a interpretação dos dados obtidos, utilizou-se o método dedutivo e a análise de conteúdo, a partir do software Iramuteq. Mediante análise lexical, pretende-se responder: a política de privacidade dessa rede social é condizente com a legislação brasileira? Os dados pessoais coletados pelo TikTok, especialmente os sensíveis, são efetivamente protegidos, em resguardo ao direito constitucional e convencional à privacidade/intimidade? Para tentar explicar essas problemáticas de pesquisa, formulou-se a hipótese a seguir: a política de privacidade do TikTok não protege efetivamente o direito à privacidade e à intimidade de seus usuários, sejam estes titulares ou não de contas em sua plataforma. Os resultados indicam uma predominância de termos relacionados a informação e usuário, enquanto palavras como privacidade e transparência são menos frequentes, sugerindo uma possível lacuna na adequação às normas da LGPD. A pesquisa conclui que a política do TikTok não promove proteção efetiva à privacidade dos usuários, evidenciando a necessidade de ajustes para que a plataforma respeite os direitos fundamentais previstos na legislação brasileira.

Palavras-chave: Tratamento de Informações Pessoais; Segurança de Dados em Redes Sociais; Compliance Digital; Direito à Intimidade.

Abstract

This research examines the handling and utilization of personal data within social media platforms, specifically TikTok, and evaluates its adherence to legal frameworks safeguarding personal data protection. Employing a qualitative approach that integrates bibliographic and documentary research methods, the study utilizes a deductive approach and content analysis facilitated by Iramuteq software. Lexical analysis of TikTok's privacy policy seeks to answer the following questions: Does the policy align with Brazilian legislation? Are personal data, particularly sensitive data, collected by TikTok effectively protected, upholding the constitutional and conventional right to privacy? The study's hypothesis posits that TikTok's privacy policy fails to effectively protect the right to privacy for all users, irrespective of their

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

account status on the platform. The results indicate a predominance of terms related to information and user, while words like privacy and transparency are less frequent, suggesting a possible gap in compliance with LGPD standards. The research concludes that TikTok's policy does not promote effective protection of user privacy, highlighting the need for adjustments so that the platform respects the fundamental rights provided for in Brazilian legislation.

Keywords: Personal Information Processing; Data Security in Social Networks; Digital Compliance; Right to Intimacy.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Introdução

Com a Lei Geral de Proteção de Dados Pessoais (LGPD), que entrou vigor em agosto de 2020, houve uma sensível mudança nas regras de tratamento de dados pessoais no cenário cibernético e, inclusive, nas redes sociais.

A partir disso, as empresas que coletam e tratam dados pessoais devem estar de acordo com as exigências da LGPD, utilizando bases legais que justifiquem a coleta e o tratamento desses dados. Dessa forma, o funcionamento das mídias sociais também deve observância à LGPD, seja na busca de usuários/clientes ou na divulgação de anúncios publicitários.

Em 2022, com a promulgação da Emenda Constitucional n. 115/2022, o direito à proteção de dados pessoais foi inserido no rol de direitos e garantias fundamentais do art. 5º da Constituição Federal. Ademais, a referida emenda também fixou a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Com isso, é dada uma maior segurança jurídica aos cidadãos na aplicação da LGPD.

Dessa forma, o direito à privacidade e à proteção de dados pessoais estão elencados no rol do art. 5 º da Carta Magna, como direitos fundamentais, que devem ser garantidos com o objetivo de promover a dignidade humana e de proteger os cidadãos.

Quanto à metodologia, esta pesquisa se classifica como bibliográfica, documental e qualitativa. Para a interpretação dos dados obtidos, utilizou-se o método dedutivo e a análise de conteúdo.

Para estruturar a análise deste estudo, adota-se uma matriz teórico-metodológica que combina aspectos da lexicometria e da análise de conteúdo qualitativa, especificamente com o uso do software IRAMUTEQ. A pesquisa bibliográfica se apoiou em obras de autores como Salviati (2017), Castro Neta e Cardoso (2021), entre outros, para fundamentar a análise da Política de Privacidade do *TikTok* e a discussão sobre o direito à proteção de dados.

A escolha por essa matriz fundamenta-se na necessidade de compreender, de maneira detalhada, a relação entre a Política de Privacidade do *TikTok* e os direitos fundamentais à privacidade e proteção de dados dos usuários. A lexicometria oferece a possibilidade de analisar, de forma quantitativa e qualitativa, a frequência e a distribuição de termos no *corpus* textual, permitindo identificar padrões léxicos e semânticos que refletem a abordagem da rede social em relação aos dados pessoais.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Além disso, o uso da análise de conteúdo qualitativa, ancorada no método dedutivo, justifica-se pela capacidade de examinar a aplicabilidade e a transparência dos termos da política de privacidade no contexto da LGPD e da Constituição Federal de 1988 (CF/88).

Esta abordagem teórica possibilita um recorte metodológico específico que prioriza a identificação de categorias de análise, as quais se estruturam por meio de classes lexicais com base na frequência e no contexto de palavras-chave como *informação*, *plataforma* e *usuário*. Esse recorte permite investigar como o *TikTok* comunica as práticas de coleta, armazenamento e compartilhamento de dados, identificando lacunas de transparência e de adequação à LGPD.

Dessa maneira, a matriz teórico-metodológica adotada neste trabalho não apenas se justifica pela pertinência com o objeto de estudo, mas também contribui para uma análise crítica, que almeja verificar se os direitos à privacidade e à proteção de dados são devidamente respeitados pela plataforma em questão.

A pesquisa bibliográfica caracteriza-se por ser elaborada com base em material já publicado, seja impresso ou disponível na Internet. Para obtenção do material impresso, recorreu-se aos livros especializados na temática central e presentes nos acervos das bibliotecas da Universidade Federal do Pará e da Universidade Estadual do Piauí. Quanto ao material virtual, artigos científicos, teses, dissertações e anais de eventos acadêmicos foram obtidos pelo acesso aos sítios eletrônicos Google Acadêmico, Periódicos CAPES, Biblioteca Digital Brasileira de Dissertações e Teses e Catálogo de Teses e Dissertações da CAPES.

Nestes casos, foram utilizadas as seguintes palavras-chave nos buscadores: LGPD, *TikTok* e/ou direito à informação. O critério utilizado para seleção das referências foi a quantidade de citações dos artigos científicos e o Qualis CAPES dos periódicos e dos livros, além da pertinência ao escopo central deste artigo, com o auxílio do software *Publish or Perish*.

Além dos documentos jurídicos pertinentes ao tema, como LGPD, CF/88 e Declaração Universal dos Direitos Humanos (DUDH), utilizou-se o documento institucional de política de privacidade do *TikTok*, este com última atualização em 5 de abril de 2023, bem como informações fornecidas diretamente por esta plataforma, via *e-mail*.

Outrossim, trata-se de pesquisa qualitativa em virtude do enfoque interpretativista. De acordo com essa abordagem, é necessário compreender o mundo e a sociedade a partir da perspectiva daqueles que os experimentam, o que implica reconhecer que o objeto de

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

estudo é percebido como uma construção social. Assim, a pesquisa qualitativa ganhou reconhecimento como crucial para a investigação da experiência vivenciada e dos intricados e prolongados processos de interação social.

Em virtude dos poucos estudos científicos sobre a segurança do *TikTok*, e da falta de clareza desta plataforma sobre o tratamento conferido aos dados pessoais de seus usuários e não usuários, surgem os seguintes questionamentos: a política de privacidade dessa rede social é devidamente aplicada de acordo com a legislação brasileira? Os dados pessoais coletados pelo *TikTok*, especialmente os sensíveis, são efetivamente protegidos, em resguardo ao direito constitucional e convencional à privacidade/intimidade?

Para explicar essas problemáticas de pesquisa, formulou-se a hipótese a seguir: a política de privacidade do *TikTok* não protege efetivamente o direito à privacidade e à intimidade de seus usuários, sejam estes titulares ou não de contas em sua plataforma. A partir disso, efetuou-se uma tentativa de falseamento dessa hipótese, com o estudo e o aprofundamento da temática de proteção de dados pessoais no *TikTok*, de acordo com a legislação brasileira.

Como essa rede social não explicitou de forma clara e coerente quais são informações coletadas, o modo de coleta e o local de armazenamento dos dados pessoais de seus usuários e não usuários, em sua política de privacidade, partiu-se para a corroboração da hipótese acima levantada. Desse modo, para a análise da Política de Privacidade do *TikTok*, utilizou-se o método dedutivo, bem como a lexicometria (ou estatística textual). Esta análise lexical de conteúdo foi realizada com as ferramentas do *software* IRAMUTEQ (*Interface de R pour les Analyses Multidimensionnelles de Textes et de Questionnaires*).

Essa análise lexical revelou uma ênfase nas palavras *informação*, *plataforma* e *usuário*, enquanto termos centrais para a proteção de dados, como *privacidade* e *transparência*, surgem com menor frequência, o que sugere uma lacuna na comunicação e clareza sobre a proteção de dados. A presente pesquisa contribui, assim, para uma reflexão crítica acerca das práticas de transparência e da adequação do *TikTok* às regulamentações brasileiras de proteção de dados.

Desse modo, constatou-se que a plataforma coleta dados pessoais mesmo sem o consentimento explícito do usuário e sem especificar a finalidade da coleta, o que pode configurar uma violação à LGPD.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

1. A privacidade como direito personalíssimo constitucional e o paradoxo com a sociedade da informação

Com a revolução das tecnologias de informação e expansão dos universos cibernéticos, a preocupação com a privacidade vem sendo colocada em pauta nos mais diversos âmbitos, sejam eles sociais, econômicos, políticos, filosóficos ou jurídicos. Outrossim, se se comparar com outros direitos fundamentais e humanos, como a vida, a segurança, e a liberdade, essa atenção ao direito à privacidade é relativamente recente.

Isso porque o marco jurídico-acadêmico no ocidente para esse direito é o artigo *The Right Of Privacy,* dos autores Samuel Warren e Louis Brandeis, publicado em 1890, que defendeu a teoria do *direito de ser deixado só*. Porém, a privacidade tratada nesse trabalho científico não é a que se conhece hoje, pois detinha um viés muito mais individualista, no sentido egoísta da palavra, ou seja, era a ausência de comunicação entre um sujeito e as demais pessoas, no contexto estadunidense, conhecido como o *zero-relationship* (Doneda, 2005).

Nessa época, a fortificação da imprensa e jornalismo nos Estados Unidos da América (EUA) gerou na burguesia um certo receio, sendo um dos motivos para a criação da obra. O direito à privacidade era invocado por estratos sociais específicos e, por isso, por muitos anos, ficou associado a pessoas socialmente expostas, como famosos, por deter um forte cunho patrimonialista.

Essa concepção perdurou até o final do século XIX e foi sendo aprimorada por muitos autores, destacando-se, em 1981, Richard Posner, que acrescentou que o direito à privacidade não se restringe apenas a *zero-relationship*, mas também aborda o direito de proteger suas próprias informações. Nesse sentido, afirmava-se que a violação do direito à privacidade se dava quando as informações pessoais eram obtidas ou divulgadas sem anuência do detentor, pois era o próprio sujeito que conhecia quais informações poderiam ou não ser socialmente danosas a ele, isto é, o sigilo como forma de salvaguarda à dignidade (Brandão, 2013).

Nesse sentido, é importante ressaltar que Aristóteles, em sua obra Ética a Nicômaco, observou que todas as ações humanas têm como finalidade a busca pela felicidade. Ele entendia que o ser humano devia se deixar agir por condutas racionais que eram adquiridas através do conhecimento, como uma forma de atingir esse bem supremo.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Então, desse modo, buscou-se compreender como essas ações inteligíveis são guiadas e concluiu-se que um ato é considerado racional quando é orientado para o bem-estar humano, impulsionado pela vontade. Com base nisso, sendo os direitos fundamentais peças-chave na proteção de bens que são considerados importantes para o ser humano, a sua satisfação reverbera diretamente na busca dos seus objetivos e, consequentemente, na sua felicidade e realização pessoal.

Dessa forma, percebendo a sociedade que a privacidade impacta diretamente no seu próprio bem-estar, passou-se a enxergá-la como um direito fundamental inato do ser humano, assim como conceitua Weinreb (2012, p. 222): "direitos inatos são direitos que temos em virtude de nossa própria existência e que não precisamos fazer nada para adquiri-los, como é o caso do nosso corpo, mente e liberdades." Baseado nesse fundamento, o direito à privacidade adquiriu um *status* de valor pessoal, uma qualidade intrínseca necessária para uma vida digna, pois o ser humano ao nascer já estaria revestido por esse escudo que protege as suas informações privadas.

Diante da relevância do direito à privacidade, o legislador brasileiro pô-lo em um patamar constitucional, como uma forma de dotá-lo de força e eficácia necessária para que fosse respeitado.

Assim, preconiza o Art. 5º, X da Carta Magna de 1988: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação".

> A vida privada e a intimidade são os outros nomes do direito de estar só, porque salvaguardam a esfera de reserva do ser humano, insuscetível de intromissões externas (aquilo que os italianos chamam de *rezervatezza* e os americanos *privacy*). [...] Amiúde, a ideia de vida privada é mais ampla do que a de intimidade. Vida privada envolve todos os relacionamentos do indivíduo, tais como suas relações comerciais, de trabalho, de estudo, de convívio diário etc. Intimidade diz respeito às relações íntimas e pessoais do indivíduo, seus amigos, familiares, companheiros que participam de sua vida pessoal (Martins, 2022).

Ou seja, a noção de intimidade traz consigo uma carga emotiva muito forte, que envolve confiança e ideia subjetivas, o que dificulta a precisão do seu conceito. Enquanto a vida privada seria, em síntese, sua separação da vida pública. Não obstante, há de se fazer uma interpretação teleológica das normas, quer dizer, apesar de toda essa diversidade semântica, a preocupação do legislador e do ordenamento jurídico brasileiro é de que o ser humano tenha o direito pleno de autogerenciamento das suas próprias informações,

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

embasado no consentimento voluntário individual e na determinação de como a esfera privada pode acessá-las.

> Recorre ao intensivo uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informações, como no uso das tecnologias de computação e telecomunicações. Por sua vez, informação consiste em um dado ou conjunto de dados em qualquer suporte capaz de produzir conhecimento, podendo ser uma imagem, som ou documento (Vieira, 2007, p. 156 *apud* Pinheiro; Bonna, 2020, p. 367)

Desse modo, com a constitucionalização da intimidade e da vida privada, o legislador revestiu esses direitos com as características da indisponibilidade ou irrenunciabilidade, por possuírem uma grande relevância social. Com isso, o Estado possui interesse e obrigação de intervir quando estes forem violados. Nesse caso, o titular não pode dispor ou renunciá-los, apesar de que possa deixar de exercê-los.

Canotilho (2012) explica que "poderá, assim, existir uma disposição individual acerca de posições de direitos fundamentais, mas o 'uso negativo' de um direito não significa renúncia a esse mesmo direito". Já é entendimento de que, em certos casos, prevalece o princípio da autonomia da vontade e liberdade do indivíduo, pois cabe a pessoa, e não ao Estado, determinar, diante de suas próprias convicções morais ou culturais, o que melhor atende suas necessidades.

Segundo Almeida e Soares (2022), a LGPD (Lei n.º 13.709/2018) se inspirou em regulamentos internacionais, como o *General Data Protection Regulation* (GDPR) europeu, mas se adaptou ao contexto brasileiro ao reafirmar a proteção de dados como um direito fundamental.

Essa legislação não apenas assegura a privacidade dos dados, mas também promove a transparência e a autonomia informativa, princípios que estão alinhados ao neoconstitucionalismo[1], por colocar o titular dos dados como um sujeito de direitos, com autonomia sobre suas próprias informações. Assim, a LGPD visa prevenir abusos por parte de instituições e empresas, ao impor obrigações que buscam limitar o tratamento e a exposição indevida de dados pessoais.

[1]O neoconstitucionalismo aprofundou a constitucionalização dos direitos fundamentais, dando-lhes maior efetividade e centralidade no sistema jurídico. Nascimento (2012) sugere que o neoconstitucionalismo amplia o campo dos direitos fundamentais ao permitir uma maior flexibilidade interpretativa, orientada por princípios e valores. Este enfoque possibilita que a Constituição seja vista não apenas como um conjunto rígido de normas, mas como um sistema aberto e dinâmico que se adapta aos novos desafios, como a proteção dos dados pessoais em uma era digital marcada pela exploração comercial e pela vigilância constante.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Nesse cenário, a LGPD representa uma resposta legislativa essencial que visa estabelecer diretrizes claras para o tratamento dos dados pessoais no Brasil, especialmente diante do capitalismo digital, no qual dados pessoais se tornaram ativos de valor econômico e estratégico.

Além disso, o capitalismo de vigilância, amplamente discutido por Fornasier e Knebel (2021), oferece um pano de fundo crítico para entender a LGPD como uma medida de resistência jurídica contra a mercantilização de dados pessoais.

Segundo esses autores, o capitalismo de vigilância é caracterizado pela coleta massiva e pela análise comportamental dos dados dos usuários para fins econômicos, muitas vezes sem o conhecimento ou consentimento explícito dos titulares.

Diante disso, a LGPD, ao regular o uso e a circulação desses dados, reafirma a importância do consentimento e da transparência, buscando proteger o direito à autodeterminação informativa.

Este direito garante que os indivíduos possam decidir livremente sobre o tratamento de suas informações pessoais, evitando que os seus direitos à privacidade e à intimidade sejam explorados para fins comerciais sem controle.

Desse modo, a LGPD promove uma defesa estruturada contra a exploração indiscriminada dos dados pessoais, refletindo uma resposta jurídica aos desafios do capitalismo digital e consolidando os direitos à privacidade e à intimidade como direitos fundamentais.

Nascimento e Silva (2023) acrescentam que implementação da LGPD nas redes sociais deve envolver a adoção de políticas de transparência, treinamento e capacitação para o tratamento de dados, especialmente as plataformas que lidam com dados sensíveis. Essa perspectiva reflete a preocupação do neoconstitucionalismo em garantir a proteção dos direitos fundamentais na esfera pública e privada.

Ao estabelecer requisitos para o tratamento de dados, a LGPD reforça o papel do Estado e das instituições como protetores da privacidade e da autonomia informativa dos indivíduos, exigindo que as organizações estatais ou não implementem práticas de segurança e garantam a privacidade dos dados pessoais, sob pena de sanções legais.

Para além do papel instrumental de garantir a conformidade com as normas de privacidade e de intimidade, a LGPD tem um significado constitucional mais profundo, ao integrar a proteção de dados ao núcleo dos direitos fundamentais. Essa legislação reflete

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

uma concepção de cidadania informacional, no qual o indivíduo não é apenas um sujeito passivo, mas um titular de direitos, capaz de intervir e controlar o uso de suas informações.

Dessa forma, a LGPD se configura como uma medida de proteção não apenas individual, mas também coletiva, ao estabelecer princípios que orientam uma governança ética dos dados.

Em um contexto de globalização digital e exploração comercial, essa lei brasileira representa uma tentativa de construir uma cidadania que inclua o direito à proteção de dados como um elemento central do neoconstitucionalismo.

Os sítios que estão presentes nos *cyberespaços* são vastos, destacando-se as redes sociais, como *TikTok, X, Facebook, Instagram, WhatsApp*, dentre outros. Para criar um perfil nesses aplicativos é preciso fornecer diversos dados pessoais. Há, inclusive, os que são repassados inconscientemente, como o endereço de *Internet Protocol* (IP), que é captado automaticamente e que revela informações do dispositivo de acesso, que ficam armazenadas nos arquivos dessas empresas. Uma problemática que reside é quando esses dados são vazados, pois, muitas vezes, o próprio detentor não sabe quem e como os divulgou, o que dificulta para o indivíduo achar maneiras de recorrer ao Judiciário, restando frustrada sua dignidade.

Ademais, a seara dos direitos que envolvem a privacidade ganha protagonismo no século XXI, uma vez que o advento de novas tecnologias trouxe consigo ferramentas que possibilitaram um fluxo constante de informações em tempo real. O mundo contemporâneo é marcado pela aproximação entre as pessoas dentro de ambientes cibernéticos, que diminuíram drasticamente as barreiras geográficas existentes.

Outrossim, é fundamental frisar que o princípio da autonomia, diante da sociedade da informação, não deve ser aplicado em sua forma mais *pura*, pois, assim como Bonna e Pinheiro (2020) ressaltam, existe hoje uma dependência e vulnerabilidade pelas plataformas digitais. O sistema capitalista implantou na sociedade máquinas que obrigam o ser humano a mudar o seu estilo de vida através da criação *necessidades* que ele sequer sabia que possuía.

As plataformas digitais estão presentes massivamente na rotina das pessoas, pois existe um aplicativo, com acesso à internet, envolvido para cada aspecto da humanidade, seja no lazer, na economia, na política. Criou-se, assim, uma necessidade de seu uso para comunicação e transmissão de informações. Sendo assim, não há de fato uma *escolha* no

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

compartilhamento e informações para uso desses meios digitais e sim uma *necessidade*. Nesse viés, a autonomia privada foi deturpada e consequentemente a tensão entre essa nova estrutura social e o direito à privacidade aumentou em escalas globais, pois em cada uma desses campos supramencionados existem dados pessoais compartilhados.

2. Direito à proteção de dados: discussões sobre informações pessoais e sensíveis

Dada a importância da privacidade à humanidade e o dever de o direito assegurá-la, a Declaração Universal dos Direitos Humanos de 1948 (DUDH), que tem o objetivo de garantir um mínimo de dignidade às pessoas e sedimentar princípios fundamentais a serem seguidos pelas nações, prevê, em seu artigo 12, que interferências arbitrárias a vida privada são vedadas: "[...] intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito a proteção da lei".

Desse modo, a DUDH consagra em seu texto o direito à privacidade como um direito fundamental à dignidade da pessoa humana, dispondo que toda pessoa deve ter sua intimidade respeitada, e que essa garantia deve ser assegurada por meio de leis.

Nesta seara, o Pacto Internacional sobre Direitos Civis e Políticos, que foi adotado pelas Nações Unidas em 1966, também reconhece, em seu Artigo 17, o direito à proteção contra interferências arbitrárias ou ilegais na vida privada, família, lar ou correspondência. Portanto, embora estes dispositivos tenham sido concebidos antes do auge da coleta de dados, eles destacam a relevância do direito à privacidade como um direito fundamental no âmbito dos direitos humanos em escala global, e estabelecem os alicerces para a proteção da privacidade nos sistemas legais em todo o mundo, mesmo em um cenário atual de crescimento das redes sociais e dos sistemas de coleta de dados.

Outrossim, apesar da importância desses textos legais para o reconhecimento do direito à privacidade, dado os novos contornos tomados pela privacidade na era digital, emerge a necessidade dos ordenamentos jurídicos se adequarem às mudanças ocorridas nesse contexto. Logo, de acordo com Stefano Rodotá (2008), devido à necessária proteção dos dados pessoais, o conceito de privacidade passa a ser mais expansivo, ao englobar o direito de exercer controle sobre suas próprias informações e de definir como utilizá-las na construção de sua esfera pessoal.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Nesse ínterim, os Estados modernos, atentos às diretrizes estabelecidas pelos pactos internacionais e às mudanças da privacidade na era digital, criaram legislações que impõem limitações ao recolhimento de dados. A exemplo disso, a União Europeia editou em 2016, GDPR, que se aplica a todos os estados membros da União Europeia e tem o objetivo de garantir a privacidade e segurança dos dados pessoais no ambiente virtual, tendo como pontos chaves: o consentimento, os direitos individuais, responsabilidade e prestação de contas, notificação de violações de dados e, por fim, controle da transferência de dados para fora dos países membros.

O direito à proteção de dados é uma consequência do direito à privacidade. Porém, com uma maior delimitação referente à proteção de dados pessoais. Com o avanço da sociedade informatizada, essa temática ganhou cada vez mais pertinência nos debates jurídicos e sociais no Brasil.

O direito, portanto, como estrutura organizacional e normativa regulatória de tais esferas e respectivas relações, não poderia deixar de ser convocado a lidar com o fenômeno. Contudo, coloca-se cada vez mais à prova a própria capacidade das ordens jurídicas convencionais de alcançar resultados satisfatórios, particularmente quando se trata de assegurar um mínimo de proteção efetiva aos direitos humanos e fundamentais afetados (Sarlet; Saavedra, 2020).

A CF/88 não previu expressamente o direito à proteção de dados, o que se encontrava, até então, no texto constitucional, era o disposto no artigo 5º, inciso X, que discorre que são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação. Contudo, com os avanços tecnológicos, em 2022, com a Emenda Constitucional nº 115, foi acrescentado o inciso LXXIX, que assegura, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais.

Com isso, o direito à proteção de dados pessoais se expandiu, haja vista que ficou expressamente salvaguardado na Constituição, como também considerou os meios digitais, que cada vez mais armazenam dados pessoais de seus usuários, através dos novos aplicativos de comunicação social.

Desse modo, a proteção constitucional de dados tornou-se de fato um princípio fundamental, assegurado no texto da Carta Magna, que busca cada vez mais garantir a privacidade e a segurança das informações pessoais em uma sociedade cada vez mais

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

conectada e digital. O direito à proteção de dados reconhece que os indivíduos têm o poder de controlar suas próprias informações, estabelecendo quem terá acesso a elas por meio de sua autorização.

O tema ganhou tanta notoriedade que a EC nº 115, de 2022, incluiu no art. 22 da Constituição Federal, que versa sobre as áreas cuja competência para legislar é privativa da União, o inciso XXX - proteção e tratamento de dados pessoais -, cuja competência para criar leis é somente da União, não sendo permitido aos Estados, DF e Municípios legislar sobre o assunto.

Dentro do ordenamento jurídico brasileiro, por sua vez, o direito à proteção de dados foi consolidado com a Lei n.°13.709, de 14 de agosto de 2018, a LGPD, sendo a principal lei brasileira que versa sobre tema.

Contudo, a LGPD no Brasil foi uma conquista de concretização gradual, pois assim como em outros países, até então privacidade e proteção de dados eram temas tratados em leis esparsas, não específicas. A questão ainda era observada de forma difusa e pouco objetiva, o que dificultava determinar se houve coleta, como os dados foram tratados e seu descarte, alinhados aos padrões mínimos recomendados para assegurar a proteção dos dados da população (Canedo, 2021).

O Marco Civil da Internet, oficialmente Lei n° 12 965, de 23 de abril 2014, a exemplo de lei infraconstitucional, é a norma legal que disciplina o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem faz uso da rede, como também da determinação de diretrizes para a atuação do Estado.

Contudo, essa lei não elenca de forma clara o que são dados pessoais e não os torna objetivos, trazendo assim a necessidade de uma maior clareza acerca do tema. De modo que foi com a LGPD que a proteção de dados passou a ser abordada de forma objetiva:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Esses fundamentos se refletem nos princípios que regem o tratamento de dados pessoais, princípios que, por sua vez, são a espinha dorsal da lei, e devem ser seguidos durante a sua aplicação, garantindo a homogeneidade e a eficácia da norma, e auxiliando na compreensão de seus conteúdos.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Para os fins da LGPD, considera-se dado pessoal: informação relacionada a pessoa natural identificada ou identificável; já dado pessoal sensível considera-se sobre dados pessoais 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. Nesse sentido, a LGPD estabelece requisitos específicos para o tratamento de dados pessoais e sensíveis, visando garantir a privacidade e a segurança dessas informações. Assim, é importante que as organizações respeitem essas regras ao lidar com dados pessoais e sensíveis, obtendo o consentimento adequado e implementando medidas de proteção adequadas.

A LGPD traz em seu texto o conceito de dados pessoais e dados pessoais sensíveis. O número de inscrição no Cadastro de Pessoas Físicas (CPF), por exemplo, configura-se como dado pessoal. Contudo, não é considerado dado pessoal sensível. O grande questionamento e crítica com relação a essa não inclusão, deve-se ao fato de que com o CPF é possível identificar o indivíduo, utilizando-se de tal para realizar compras e cadastros.

A LGPD o considera apenas dado pessoal, porém, com o CPF, muitas vezes fornecido no dia a dia do indivíduo em compras e cadastros, é possível se informar acerca da 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; desde que ele tenha sido utilizado como dado identificador no momento do armazenamento dos dados acima.

A principal situação em que isso ocorre no Brasil está na exigência do CPF para a realização de compras (e, muitas vezes, para a obtenção de um desconto ou promoção) em farmácias e drogarias. Ao relacionar o CPF de uma pessoa às compras de medicamentos e outros produtos ou serviços relacionados à sua saúde, esse dado passa a ser enquadrado no conceito de dado pessoal sensível do art. 5º, II, da LGPD.

Assim, o CPF, que é frequentemente utilizado pelo cidadão para identificar-se em determinadas situações em que expõe dados pessoais sensíveis, torna-se também dado sensível, necessitando de igual proteção como dado pessoal sensível.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

3. Política de Privacidade do *TikTok*: armazenamento e tratamento de dados pessoais

Os dados pessoais são inseridos, por serem necessariamente imperiosos, para a efetivação ou validação de uma conta em toda e qualquer rede social. Desse modo, as condições e as circunstâncias em que os usuários, nesse cadastro, submetem-se, merecem indiscutível atenção.

A massa coletiva, como de praxe, não se habitua à recomendação da análise das políticas de privacidade vigentes em todas as redes, o que não é diferente quando se trata do *Tiktok*.

Riscos à privacidade de dados, aos próprios direitos fundamentais e de segurança é o que se presencia quando se leva em consideração os requisitos básicos da criação de uma conta em redes sociais desta conjuntura, em específico, o *Tiktok*. Isso porque a própria plataforma se torna pouco confiável ao corroborar para incertezas desde o compartilhamento de dados, à política de postagem, algoritmo, armazenamento e o tratamento de dados pessoais.

A começar da coleta de dados que é intrínseca à plataforma do *Tiktok*. Quando se cria uma conta na plataforma, ainda nos pontos destacados da Política de Privacidade da rede, é afirmado que o indivíduo terá seus dados coletados pela plataforma, bem como utilizados para publicidade direcionada. O intrigante é que a motivação, finalidade ou tampouco o propósito de tal assertiva não é informado pela rede, o que leva à mazela jurídico-institucional referente à plataforma em questão, que põe à dúvida o que fora outrora citado.

Outrossim, pode destacar o *status* de personalização da plataforma, que proporciona aos usuários o que, de fato, este possui preferência em visualizar. O que é direcionado tanto ao *feed*, quanto às demais áreas da plataforma, expandindo-se com base nos interesses individuais de cada usuário. O ato de compartilhamento de dados pessoais pode parecer inofensivo ou incólume ao indivíduo que possui a conta na plataforma. No entanto, a empresa passa a transitar com tais dados absorvidos dentro e fora da plataforma, ou seja, não se restringe apenas ao que está sendo vislumbrado naquele momento específico.

Ainda no que diz respeito à coleta efetuada pelo *Tiktok*, é realizada a análise das tendências individuais de quem faz uso da rede, em todas as áreas, seja referente a comportamentos sociointerativos, preferências políticas, gênero, sexualidade e até nicho social, a partir do contexto em que o indivíduo em questão está inserido.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

O acesso do *Tiktok* às áreas alheias à plataforma é perigosamente comum e, de praxe, aceito pelo indivíduo que valida a inscrição na rede. Nesse ínterim, é validada a coleta de informações sobre os nivelamentos da tecla de usuário, a localização em que a pessoa se encontra ou que teve acesso. Sob tal perspectiva, também é coletado o próprio histórico do navegador, o que, inegavelmente, configura-se como violação à privacidade do indivíduo. Ademais, são coletados dados relacionados à impressão facial e de voz, bem como o controle de todas as opções já citadas anteriormente.

Sob tal perspectiva, o destaque que engloba a violação à privacidade nada mais é do que a condição aceita pelo indivíduo ao cadastrar a referida conta na plataforma, o que ocasiona a invasão de dados referida, caracterizando como a modulação da plataforma, no entanto, lacuna notoriamente inserida.

Ao analisar a política de privacidade, a própria plataforma, em primeiro plano alerta que terá acesso a dados restritamente a saber e elabora tópicos, exemplificando as informações de perfil, conteúdo do usuário, mensagens recebidas e enviadas, informações de compra, contatos e respectivos telefones, bem como documentação referente à faixa etária.

Até então, sob uma ótica comum, são entendíveis os dados requeridos pela plataforma, que são condizentes com os caracteres personalíssimos de cada indivíduo, que é justamente o que diferencia um usuário de outrem, no entanto, este é apenas o início dos tópicos existentes na Política de Privacidade do *Tiktok*, existindo inúmeros outros tópicos que retratam outras captações da plataforma no que tange às informações pessoais de cada indivíduo.

O próprio Direito enfatiza o Princípio do Consentimento Informado, que preza justamente pelo conhecimento prévio de quem recebe determinado serviço ou congênere e faz jus ao que se submete a determinado quadro de necessidade. Fator que não se correlaciona com o que, de fato, é visto no cotidiano de quem utiliza o *Tiktok* pois, repentinamente, quaisquer usuários poderão se deparar com acessos indesejados, no sentido de que, como é informado na Política de Privacidade, existirão informações coletadas automaticamente, ou seja, sem o prévio consentimento do usuário.

Por meio da proteção de dados pessoais, garantias a princípio relacionadas à privacidade passam a ser vistas em uma ótica mais abrangente, pela qual outros interesses devem ser considerados, abrangendo as diversas formas de controle tornadas possíveis com

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

a manipulação de dados pessoais. Para uma completa apreciação do problema, estes interesses devem ser considerados pelo que representam, e não somente pelo seu traço visível – a violação da privacidade (Doneda, 2011).

Sob tal óbice, serão coletadas informações do uso, discernentes às interações, anúncios e, como um todo, acerca do que é visto; também, as chamadas informações inferidas, ou seja, o que a plataforma entende por atributos do usuário, incluindo interesses, gênero e faixa etária, para que haja, segundo o *Tiktok*, a personalização do conteúdo. E isto é apenas o que abre a gama de permissões que o indivíduo concede à rede, que vão desde o uso das informações, até ao armazenamento, os direitos e as escolhas dos usuários.

De forma específica, quando se analisa a parte da Política de Privacidade do *Tiktok* no que tange à forma das informações serem coletadas, existe uma lacuna exorbitante na explicação do propósito de tais coletas e a respectiva finalidade. Em alguns pontos, a exemplo, é informado que tal coleta seria para "facilitar a pesquisa que atenda a determinados critérios". A generalização não permite a compreensão em alguns pontos acerca dos propósitos de tais coletas; acerca de qual segurança ou qual proteção a plataforma está citando.

Para contextualizar fatos que já aconteceram e estão concatenados à realidade consolidada, pode-se citar o fato de que a empresa *Cambridge Analytica*, desde 2014, por intermédio do *Facebook*, fez jus ao apontamento do uso indevido de informações privadas de usuários, bem como exposição destes, o que tomou notoriedade e ganhou proporção por toda a região.

Em estudo conduzido por Lin (2021), foram comparadas as configurações e os mecanismos de segurança e privacidade do *Tiktok* e do *Douyin*, articulado pela mesma empresa, ou em outros termos, aplicativo-gerador do *Tiktok*. Em tal estudo, fora analisada a incógnita acerca da possível censura prévia no que tange ao conteúdo, bem como ao controle da plataforma sobre os interagentes das tais, o que trouxe à tona, ademais, a análise do tráfego no que tange ao uso efetivo da plataforma, que reverberaria o levantamento de informações imperiosas dos indivíduos, desde os dados pessoais até as correlações com outros dispositivos. Isso enfatiza que tais questionamentos não são isolados e sim alvos de estudo e investigação, bem como molas propulsoras no tocante à percepção das lacunas da política de privacidade da plataforma.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

4. Resultados e discussões: análise lexical da Política de Privacidade do *TikTok* a partir do *software Iramuteq*

Dentre os documentos relacionados à política de privacidade do *TikTok*, o que foi analisado nesta pesquisa é o único que se encontra atualmente disponível em português brasileiro. Os demais, que são intitulados *diretrizes de aplicação das normas do TikTok*, *privacidade e segurança* e *violação de propriedade intelectual* (tradução livre), estão disponíveis apenas no inglês estadunidense, o que dificulta a compreensão dos usuários que não leem nesse idioma.

Além disso, solicitou-se informações de privacidade sobre os dados pessoais de um dos coautores, que é usuário desta plataforma, com questionamentos sobre: quais são as informações pessoais utilizadas e armazenadas; como os dados pessoais são armazenados e onde estes são mantidos em segurança; por quanto tempo esses dados são guardados; sobre o compartilhamento das informações pessoais com terceiros, pessoas físicas e jurídicas; e sobre os mecanismos de segurança adotados para evitar o vazamento desses dados pessoais.

Em resposta, recebida por correio eletrônico, em 28 de setembro de 2023, o *TikTok* limitou-se apenas a indicar links direcionados ao seu site, para as seções *Segurança e retenção de dados*, *Os seus direitos e escolhas* e as instruções para obtenção de cópia dos dados pessoais diretamente pelo aplicativo. Os links direcionaram apenas ao sítio eletrônico intitulado *Política de Privacidade*, cujo *corpus* textual foi analisado nesta pesquisa, utilizando as ferramentas do *software Iramuteq*.

Corpus é o conjunto de textos compilados pelo pesquisador, e que compõem o objeto de análise. No *corpus* analisado, encontraram-se 569 hápax, que representam 54,40% das formas, com 12,66% de ocorrências. Hápax trata-se de um verbete que é detectado uma única vez, em um determinado idioma – que, no caso em comento, é o português brasileiro (Salviati, 2017).

Os cinco substantivos mais frequentes na análise foram, em ordem decrescente: informação (97 vezes), plataforma (61 vezes), conteúdo (44 vezes), usuário (39 vezes) e dado (31 vezes).

As figuras abaixo apresentadas são resultantes das análises efetuadas pelo *software Iramuteq*, por intermédio do Método de *Reinert*, que propõe uma classificação hierárquica descendente. O objetivo deste método é formular categorias de segmentos de texto (ST)

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

que, simultaneamente, compartilhem um vocabulário semelhante entre si e diferenciem-se do vocabulário dos ST de outras categorias (Salviati, 2017).

Por conseguinte, as análises infracolacionadas se baseiam na proximidade léxica e na premissa de que as palavras usadas em contextos semelhantes estão ligadas ao mesmo universo lexical e que, por isso, fazem parte de sistemas de representação mentais específicos. Desse modo, os segmentos de texto foram categorizados de acordo com seu vocabulário respectivo, e o conjunto de termos foi dividido com base na frequência das raízes das palavras. Com isso, o *Iramuteq* criou categorias compostas por palavras significativamente associadas a contextos similares, dentro do *corpus* textual analisado (Salviati, 2017).

Nas estatísticas textuais, exibe-se um gráfico que representa a distribuição de frequência das palavras no *corpus*, conforme apresentado na Figura 1.

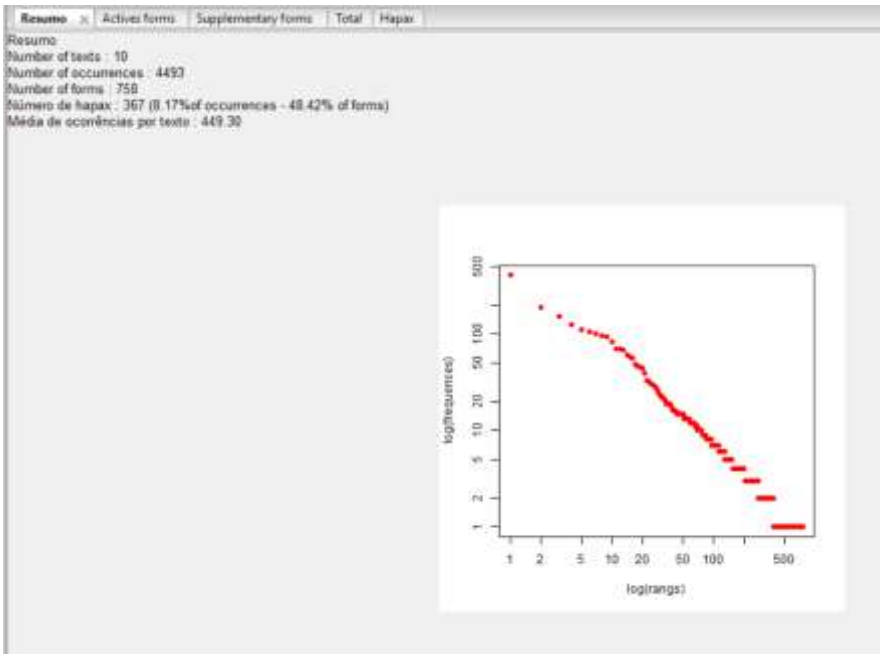


Figura 1 – resultado da análise das estatísticas textuais (autoria própria)

O número de textos representa a quantidade de registros incluídos no *corpus*. Neste caso, os registros coincidem com as seções dispostas na política de privacidade do *TikTok*: quais informações coletamos; como usamos suas informações; onde armazenamos suas informações; seus direitos e escolhas; a segurança das suas informações; por quanto tempo

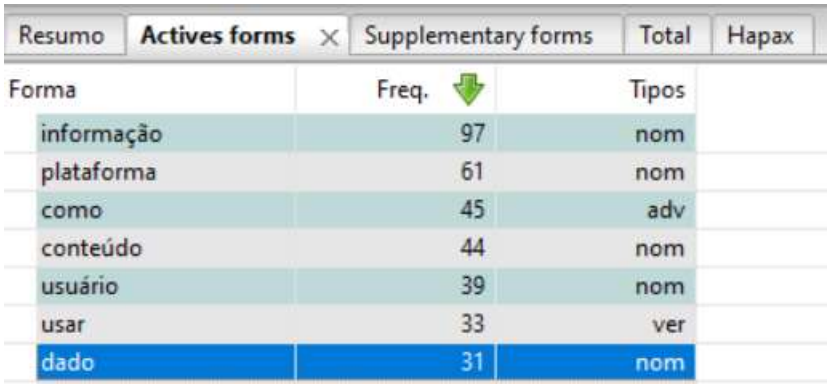
https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

mantemos suas informações; informações relacionadas a adolescentes; atualização da Política de Privacidade; contato; e Termos Complementares – Específicos da Jurisdição.

A quantidade de ocorrências indica o total de palavras presentes no *corpus*. Isso varia se o *corpus* é lematizado ou não, visto que, quando lematizado, não inclui as variações das palavras. A lematização consiste em representar as palavras por meio do infinitivo dos verbos e do masculino singular dos substantivos e adjetivos.

A quantidade de formas aponta o número de formas presentes no *corpus*, englobando palavras ativas e suplementares. Essa quantidade também difere se o *corpus* é lematizado ou não.

Na guia Formas Ativas, apresentam-se, em ordem de ocorrência, todas as principais palavras identificadas no *corpus*, incluindo verbos, adjetivos, advérbios, substantivos e aquelas não presentes no dicionário. A lista compreende as palavras ativas (na coluna Forma), acompanhadas de suas frequências de ocorrência (na coluna Frequência) e suas categorias gramaticais (na coluna Tipo).



Forma	Freq.	Tipos
informação	97	nom
plataforma	61	nom
como	45	adv
conteúdo	44	nom
usuário	39	nom
usar	33	ver
dado	31	nom

Figura 2 – formas ativas (autoria própria)

Na Figura 2, percebe-se que os cinco substantivos com maior frequência no *corpus* textual são, nessa ordem: informação, plataforma, conteúdo, usuário e dado. Somadas, essas palavras representam 36% (trinta e seis por cento) do número de formas. Com isso, denota-se a relevância destas na composição textual da Política de Privacidade do *TikTok*. Em contrapartida, a forma *privacidade* apresenta a frequência de 12 (doze), o que representa apenas 0,01% (um centésimo por cento) do número de formas. Com isso, infere-se que essa palavra carece de relevância lexical no *corpus*.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

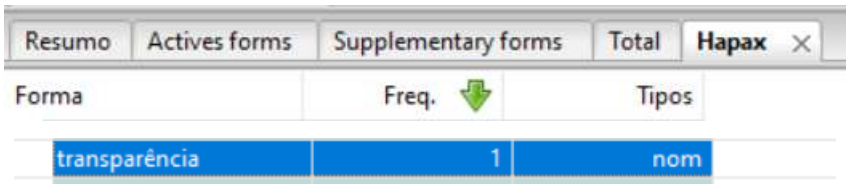


Figura 3 – hápax (autoria própria)

Na figura 3, constata-se que a forma *transparência* é utilizada apenas uma única vez em todo o *corpus* textual. A despeito disso, conforme analisado na Figura 2, a palavra *informação* é a mais recorrente na Política de Privacidade do *Tiktok*. Disto depreende-se que, se houve a correlação linguística entre *transparência* e *informação*, na melhor das hipóteses, esta ocorreu apenas uma única vez. Esse resultado é sobremaneira inquietante, pois se demonstra lexicalmente que a preocupação do *TikTok*, em sua política de privacidade, com a transparência da informação, é irrisória, se é que existe.

Na Análise Fatorial de Correspondência (AFC), verifica-se a interação entre o vocabulário (levando em conta a frequência de ocorrência de palavras) e as classes, resultando em uma representação gráfica em um plano cartesiano, no qual as oposições entre classes ou formas são visualizadas.

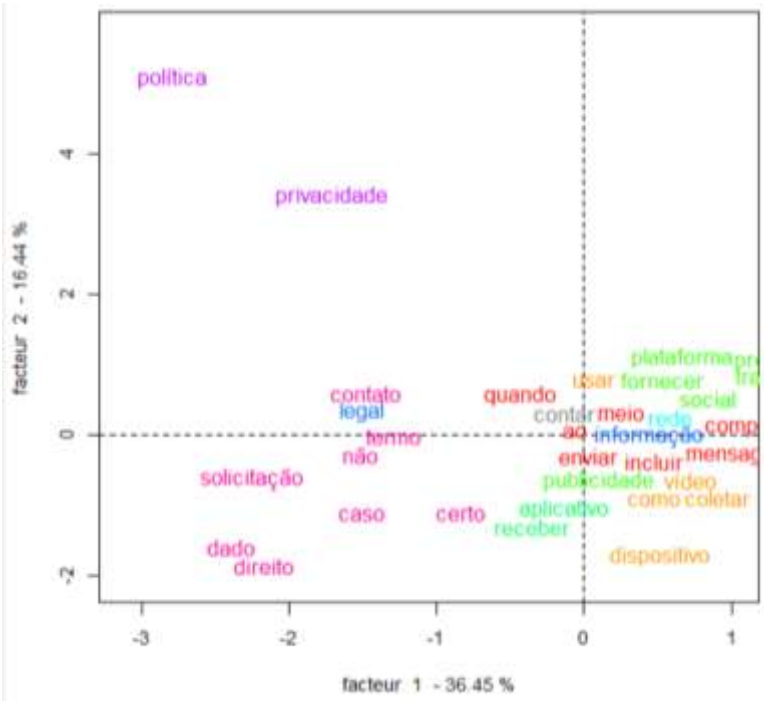


Figura 4 – Análise Fatorial de Correspondência (autoria própria)

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Na Figura 4, vislumbra-se que as formas *dado*, *informação* e *plataforma*, que estão entre as mais recorrentes, conforme apontado na Figura 1, pertencem a classes lexicais distintas, por estarem em cores diferentes. Ademais, mister salientar o distanciamento cartesiano entre *privacidade* e as três formas supracitadas. Com isso, há um afastamento não apenas de classe, como também de forma, entre as palavras mencionadas. Essa abjunção lexical sugere um apartamento gramatical, o que pode indicar que essas palavras não se relacionam (ou, se o fazem, é indiretamente), no *corpus* textual.

A AFC representa a combinação de vocabulários com as classes, considerando a frequência de ocorrência de palavras. Isso resulta em uma representação gráfica em um plano cartesiano, na qual são observadas as relações contrastantes entre classes ou formas (Salviati, 2017). Desse modo, é possível verificar a dependência (ou não) entre as classes acima representadas por cores distintas.

As associações de dependência ocorrem quando as categorias estão no mesmo quadrante e quando estão próximas de linhas ou colunas (Amaral-Rosa; Candaten, 2021). Com isso, é possível concluir que o direito à proteção de dados pessoais (cor verde), coleta de conteúdos (cor azul) e informações de perfil (cor vermelha), por estarem em quadrantes distintos, são classes independentes, e que, portanto, são abordadas em contextos não conectados no *corpus* textual. Desse modo, nota-se a ausência de interligação léxica entre essas classes na Política de Privacidade do *TikTok*.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

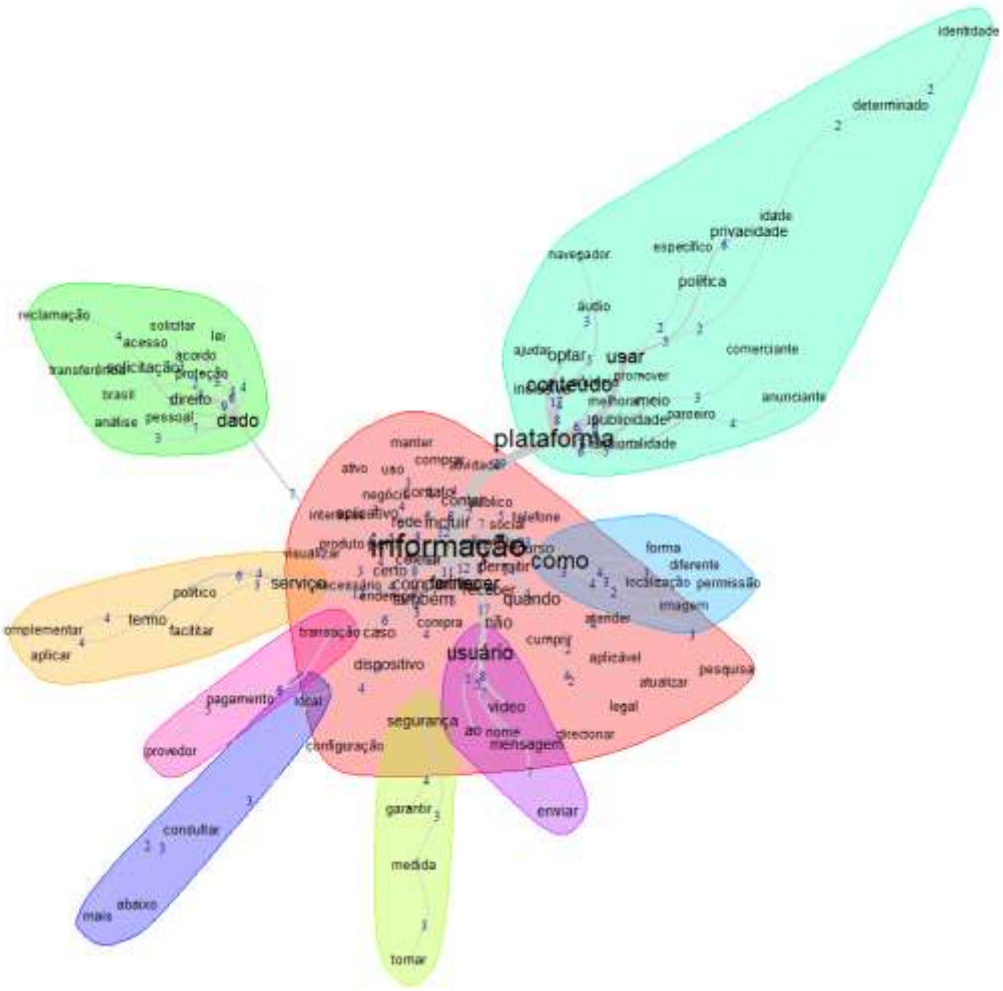


Figura 5 – Análise de Similitude - Apresentação Fruchterman Reingold
Escore Coocorrência, com escore nas bordas (autoria própria)

A árvore de coocorrência é constituída por um núcleo central, a partir do qual se desdobram várias ramificações. Na Figura 5, a palavra *informação* representa o núcleo central, dando origem a ramificações descendentes. Os ramos que apresentam maior grau de conexão com o núcleo são, nessa ordem: plataforma, dado e usuário. Além disso, quatro outros núcleos possuem relevância menor: segurança, local, transação e serviço. Desse modo, percebe-se que a similitude com o núcleo central é maior com os dados dos usuários e menor com a segurança na coleta, armazenamento e tratamento destas informações pessoais. A partir disso, infere-se que a Política de Privacidade do *TikTok* atribui menor valor lexical à segurança no ambiente virtual.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Figura 6 – nuvem de palavras (autoria própria)

A análise através de nuvem de palavras revela um conjunto de palavras agrupadas, organizadas e estruturadas em formato de nuvem. As palavras são exibidas em tamanhos diferentes, sendo as maiores aquelas que possuem maior relevância no *corpus* textual, conforme indicado pela frequência. Trata-se de uma análise lexical mais simplificada, mas que permite a rápida identificação das palavras-chave no *corpus*. Outrossim, proporciona uma visualização rápida do conteúdo, pois as palavras mais importantes ficam mais próximas do centro e são representadas graficamente com fontes maiores (Amaral-Rosa; Candaten, 2021).

Na Figura 6, nota-se que as palavras com maior ocorrência e relevância na Política de Privacidade do *TikTok* são, nessa ordem: informação, plataforma, usuário, conteúdo e dado. Palavras centrais para a expressão do direito à privacidade e à intimidade dos usuários dessa plataforma ocupam um espaço de menor relevância, como, por exemplo: privacidade e direito. Não há quaisquer sinônimos ou expressões que as substituam ou complementem no *corpus* textual. A partir disso, percebe-se como as discussões sobre o direito à privacidade ou

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

à intimidade são superficiais e, além disso, como os assuntos correlatos são totalmente escamoteados na Política de Privacidade do *TikTok*.

Considerações finais

A LGPD surge como um mecanismo que se propõe a evitar a exposição de dados pessoais sem a autorização dos usuários das redes sociais. Em virtude dos constantes casos de invasão de privacidade e dos usos indevidos de informações por terceiros, a legislação brasileira vem investindo em medidas voltadas para a segurança no meio digital.

A LGPD é voltada para a proteção de informações pessoais dos usuários, exigindo maior transparência na captação e tratamento dos dados no mundo digital, o que inclui as redes sociais, como o *TikTok*.

Nesse contexto, a norma estabelece algumas regras para que o *TikTok* cientifique o público sobre o que farão com os dados coletados, bem como quem terá acesso a eles. Em caso de descumprimento, os infratores ficarão sujeitos a punições jurídicas e administrativas e ainda receberão avaliações negativas por conta da péssima experiência do usuário.

Assim, o *TikTok*, por coletar, tratar, armazenar e compartilhar os dados pessoais de seus usuários, deve adequar seus processos, políticas e termos de uso para se adaptar à legislação brasileira. Além disso, a Lei também estabelece dez princípios que devem reger todas as operações que envolvam o tratamento de dados pessoais, quais sejam, adequação; necessidade; transparência; livre acesso; princípio da qualidade dos dados; segurança; prevenção; responsabilização e prestação de contas; não discriminação; e finalidade. Esses princípios visam garantir o respeito à privacidade dos usuários.

A finalidade, por exemplo, obriga o *TikTok* a determinar um objetivo direto para a coleta dos dados pessoais do usuário. Tal preceito vai ao encontro do princípio da necessidade, que obriga a organização a coletar somente os dados pessoais, que são estritamente necessários para a finalidade proposta.

A transparência, por sua vez, determina que os titulares tenham direito de acessar os dados armazenados, a forma como serão utilizados e se as informações serão compartilhadas com outras organizações, sejam elas públicas ou privadas.

Dessa forma, com o advento e entrada e vigor da LGPD, passou-se a exigir do *TikTok* condutas mais leais e claras em relação a coleta e ao tratamento de dados de seus usuários.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

No entanto, conforme analisado neste artigo, os termos da Política de Privacidade dessa rede social são pouco claros e trazem informações genéricas, que não se coadunam nem com a legislação brasileira nem internacional. Isso restou demonstrado tanto pelas discussões teóricas desenvolvidas, quanto pelos resultados produzidos e discutidos, a partir do *software Iramuteq*.

A análise lexical da política de privacidade do *TikTok* demonstrou que a plataforma ainda precisa se adequar às exigências da LGPD, especialmente em relação à transparência e ao consentimento na coleta e no tratamento de dados pessoais. A falta de especificidade sobre como os dados são utilizados, compartilhados e protegidos levanta preocupações sobre a efetiva proteção da privacidade dos usuários.

Esses resultados reforçam a hipótese de que a Política De Privacidade do *TikTok* apresenta lacunas em sua conformidade com a legislação brasileira. Além disso, a análise de similaridade realizada com o *Iramuteq* destacou que, mesmo em tópicos onde a plataforma aborda a *segurança*, o termo apresenta uma conexão lexical fraca com *informação* e *dados*, o que pode indicar um foco insuficiente nas práticas de proteção de dados dos usuários.

Assim, conclui-se que a LGPD impõe que as plataformas digitais promovam transparência e detalhamento no tratamento de dados pessoais, o que o *TikTok* aparenta não alcançar plenamente, segundo os dados apresentados e com os resultados discutidos neste artigo. Desse modo, para cumprir os requisitos normativos e assegurar plenamente os direitos fundamentais à privacidade e à intimidade de seus usuários, o *TikTok* precisa aprimorar significativamente suas práticas de proteção de dados, incorporando a privacidade e a segurança de maneira mais robusta em suas normas internas.

Referências bibliográficas

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, Belo Horizonte, v. 27, n. 3, p. 26-45, 2022. Disponível em: https://periodicos.ufmg.br/index.php/pci/article/view/25905. Acesso em: 03 nov. 2024.

AMARAL-ROSA, Marcelo Prado; CANDATEN, Angela Enderle. Análise qualitativa mediada pelo software IRaMuTeQ: Interpretações a partir do ontem e do hoje no Sistema Único de Saúde do Brasil. **New Trends in Qualitative Research**, Oliveira de Azeméis, v. 8, p. 505-513,

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

2021.

ARISTÓTELES. **Ética a Nicômaco**. Tradução Edson Bini. 2ª ed. São Paulo: Edipro, 2007.

BONNA, Alexandre Pinheiro. Fundamentação filosófica do direito à privacidade no contexto da era da sociedade da informação. **Revista Brasileira de Direito Civil em Perspectiva**, Belém, v. 5, n. 2, p. 174-193, 2019. Disponível em: https://www.indexlaw.org/index.php/direitocivil/article/view/5965. Acesso em: 3 out. 2023.

BRANDÃO, André Martins. INTERPRETAÇÃO JURÍDICA E DIREITO À PRIVACIDADE NA ERA DA INFORMAÇÃO: UMA ABORDAGEM DA HERMENÊUTICA FILOSÓFICA. **Revista Paradigma**, Ribeirão Preto, n. 22, p. 232-257, 2013. Disponível em: https://revistas.unaerp.br/paradigma/article/view/237. Acesso em: 3 out. 2023.

CANEDO, Fabiolla Labelle Ornelas. **Privacidade e ética na Sociedade de Dados**: Uma reflexão filosófica sobre a Lei Geral de Proteção de Dados brasileira, 124f. Dissertação de mestrado – Pontifícia Universidade Católica de São Paulo – PUC-SP, 2021; Disponível em: https://repositorio.pucsp.br/handle/handle/24533. Acesso em: 03 nov. 2023

CANOTILHO, José Joaquim Gomes. **Direito Constitucional e Teoria da Constituição**. Coimbra: Almedina, 2012.

CASTRO NETA, Abília Ana; CARDOSO, Berta Leni Costa. The use of the iramuteq software in data analysis in qualitative or quali-quanti research. **Cenas Educacionais**, Caetité, v. 4, p. e11759–e11759, 2021. Disponível em: https://revistas.uneb.br/index.php/cenaseducacionais/article/view/11759. Acesso em: 17 set. 2023.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico Journal of Law**, Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011. Disponível em: https://portalperiodicos.unoesc.edu.br/espacojuridico/article/ view/1315. Acesso em: 02 out. 2023.

DONEDA, Danilo. **Da privacidade à proteção de dados**. Rio de Janeiro: Editora Renovar, 2005.

FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. O titular de dados como sujeito de direito no capitalismo de vigilância e mercantilização dos dados na Lei Geral de Proteção de Dados. **Revista Direito e Práxis**, Rio de Janeiro, v. 12, n. 2, p. 1002-1033, 2021.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

Disponível em: https://doi.org/10.1590/2179-8966/2020/46944. Acesso em: 03 nov. 2024.

GIL, Antonio C. **Como Elaborar Projetos de Pesquisa**. São Paulo: Grupo GEN, 2022.

GIL, Antonio C. **Métodos e Técnicas de Pesquisa Social**. 7. ed. São Paulo: Grupo GEN, 2019.

LIN, Pellaeon. **TikTok vs Douyin A Security and Privacy Analysis**. Citizen Lab Research Report No. 137. University of Toronto: Toronto, 2021.

MARTINS, Flavio. **Curso de Direito Constitucional**. 3. ed. São Paulo: Saraiva, 2022.

NASCIMENTO, Valéria Ribas do. Neoconstitucionalismo e ciberdemocracia: desafios para implementação da cibercidadania na perspectiva de Pérez Luño. **Revista de Informação Legislativa**, Brasília, v. 49, n. 194, abr./jun., 2012. Disponível em: http://www2.senado.leg.br/bdsf/handle/id/496580. Acesso em:
03 nov. 2024.

NASCIMENTO, Bruna Laís Campos do; SILVA, Edilene Maria da. Lei Geral de Proteção de Dados e repositórios institucionais: reflexões e adequações. **Em Questão**, Porto Alegre, v. 29, e-127314, 2023. Disponível em: https://doi.org/10.1590/1808-5245.29.127314. Acesso em: 03 nov. 2024.

PINHEIRO, V. S.; BONNA, A. P. Sociedade da informação e direito à privacidade no Marco Civil da Internet: fundamentação filosófica do Estado de Direito. **Revista de Direitos e Garantias Fundamentais**, Vitória, v. 21, n. 3, p. 365–394, 2020. Disponível em: https://sisbib.emnuvens.com.br/direitosegarantias/article/view/1555. Acesso em: 4 out. 2023.

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

SALVIATI, Maria Elisabeth. **Manual do aplicativo Iramuteq**. Planaltina, mar. 2017. Disponível em: http://www.iramuteq.org/documentation/fichiers/manual-do-aplicativo-iramuteq-par-maria-elisabeth-salviati. Acesso em: 08 out. 2023.

SARLET, Ingo Wolfgang; SAAVEDRA, Giovani Agostini. Fundamentos jusfilosóficos e âmbito de proteção do direito fundamental à proteção de dados pessoais. **RDP**, Brasília, vol. 17, n. 93, p.33-57,maio/jun.2020. Disponível em:

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645

https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4315. Acesso em: 03 nov. 2023

WEINREB, L. L. The Right to Privacy. **Social Philosophy and Policy**, Cambridge, v. 17, n. 2, p. 25-44, 2000. Disponível em: https://www.cambridge.org/core/journals/social-philosophy-and-policy/article/abs/right-to-privacy/A3211E795F3FA687F8D76B44214C3F355. Acesso em: 3 out. 2023.

Sobre os autores

Elvis Gomes Marques Filho
Mestre (PPGD/UFMS) e Doutorando (PPGD/UFPA) em Direitos Humanos. Professor Dedicação Exclusiva da UESPI. Líder do GEPEG/UESPI/CNPq. E-mail: elvisfilho@pcs.uespi.br. ORCID: https://orcid.org/0000-0003-2681-6094.

Carlos Mendes Monteiro da Rocha
Bacharel e Mestre em Direito pela UFPI. E-mail: carlosmendes@uespi.br. ORCID: https://orcid.org/0000-0002-1943-1930.

Ernandes Antônio de Sousa
Bacharelando em Direito pelo IERSA. E-mail: ernandessousa343@gmail.com. ORCID: https://orcid.org/0000-0001-5532-692X.

Francisco de Assis de Oliveira Santos
Bacharelando em Direito pela UESPI. E-mail: franciscodeassisdeosantos@aluno.uespi.br. ORCID: https://orcid.org/0009-0001-4302-3726.

Thyago Felype de Moura Brito
Bacharelando em Direito pela UESPI. E-mail: tfdemourabrito@aluno.uespi.br. ORCID: https://orcid.org/0000-0002-3436-3219.

Ludimila Lorrane de Sousa Campelo
Bacharelanda em Direito pela UESPI. E-mail: ludimila.l.de.sousa.campelo@aluno.uespi.br. ORCID: https://orcid.org/0009-0007-1129-965X.

Guilherme Isidorio da Rocha Abreu
Bacharelando em Direito pela UESPI. E-mail: guilhermeisidoriodara@aluno.uespi.br. ORCID: https://orcid.org/0009-0003-7772-9713.

Os autores contribuíram igualmente para redação do artigo.

https://doi.org/10.1590/2179-8966/2025/80645 | ISSN: 2179-8966 | e80645