

TRANSPARÊNCIA NO TRATAMENTO DE DADOS PESSOAIS POR INTELIGÊNCIA ARTIFICIAL NAS PLATAFORMAS DIGITAIS

Oscar Valente Cardoso

02-12-2024

Resumo: O uso de inteligência artificial (IA) no tratamento de dados pessoais por plataformas digitais (provedores de aplicação) apresenta desafios significativos para a concretização do princípio da transparência e para a definição de critérios de responsabilidade civil. Este artigo, de caráter teórico e analítico, busca investigar os impactos da aplicação de modelos de IA nesse contexto, considerando o ambiente jurídico brasileiro, com destaque para a Lei Geral de Proteção de Dados (LGPD) e o Marco Civil da Internet (MCI). O objetivo principal é analisar como a opacidade intrínseca de diversos modelos de IA afeta a capacidade das plataformas de informar os titulares de dados e de cumprir os deveres legais de transparência. A metodologia utilizada inclui a revisão bibliográfica dos temas pertinentes. O artigo conclui que é necessária a adoção de estratégias regulatórias mais rigorosas, aliadas ao desenvolvimento de tecnologias que promovam maior explicabilidade e interpretabilidade dos modelos de IA, a fim de propiciar segurança jurídica e a proteção adequada dos dados pessoais.

Palavras-chave: Marco Civil da Internet. Lei Geral de Proteção de Dados Pessoais. Inteligência Artificial. Princípio da Transparência. Responsabilidade Civil.

Sumário: Introdução. 1. O Princípio da Transparência no Tratamento de Dados Pessoais. 1.1. Definição do Princípio da Transparência. 1.2. Transparência na LGPD e no Marco Civil da Internet. 2. O Uso de IA pelas Plataformas Digitais no Tratamento de Dados Pessoais. 2.1. Características dos Modelos de IA Aplicados em Redes Sociais e Aplicativos de Mensagens. 2.2. Tratamento de Dados Pessoais por IA. 3. Reflexos da Utilização de IA sobre a Responsabilidade Civil das Plataformas Digitais. 3.1.

Responsabilidade das Plataformas Digitais por Danos Causados por IA. 3.2. Critérios de Responsabilização. Conclusão. Referências Bibliográficas.

1. Introdução

O avanço da inteligência artificial tem transformado significativamente o modo como as plataformas digitais tratam os dados pessoais de seus usuários, especialmente em redes sociais e aplicativos de mensagens. Esses ambientes digitais, caracterizados pelo uso intensivo de algoritmos para coleta, análise e outras operações de tratamento de dados, refletem questões polêmicas sobre privacidade, proteção de dados pessoais e a aplicação dos princípios de tratamento, como o da transparência.

Na Lei Geral de Proteção de Dados Pessoais, o princípio da transparência exige que os titulares de dados sejam adequadamente informados sobre como os seus dados são tratados. Em complemento, o Marco Civil da Internet exige a transparência em diversas regras, como na neutralidade da rede e nos direitos dos usuários.

Porém, a complexidade técnica dos modelos de IA e a sua eventual opacidade, descrita como uma “caixa-preta” (*blackbox*), cria barreiras significativas para a concretização desse princípio, o que gera discussões sobre o equilíbrio entre a inovação tecnológica e a proteção de direitos fundamentais.

O uso de IA nas plataformas digitais também traz implicações relevantes para a responsabilidade civil. Os casos de discriminação algorítmica, tratamento inadequado de dados ou falhas na comunicação com os usuários podem resultar em danos. Nesse cenário, torna-se essencial compreender como os provedores podem ser responsabilizadas pelos impactos negativos causados pela utilização da IA e quais critérios devem orientar essa responsabilização.

Este artigo tem o objetivo principal de analisar os reflexos do uso de modelos de IA no tratamento de dados pessoais pelas plataformas digitais sobre o princípio da transparência e a responsabilidade civil. A pesquisa se justifica pela crescente dependência de IA em serviços digitais e pela insuficiência de normas específicas que abordem os desafios gerados pela opacidade algorítmica e pelas falhas de comunicação.

A estrutura do artigo está organizada em três tópicos. Após esta introdução, a primeira seção apresenta os fundamentos do princípio da transparência no tratamento de dados pessoais, a segunda analisa a utilização de inteligência artificial pelas plataformas digitais, enquanto a terceira desenvolve as implicações jurídicas do uso de

IA, com ênfase na responsabilidade civil das plataformas digitais. Por fim, a conclusão sintetiza os principais pontos discutidos e sugere caminhos para pesquisas futuras.

2. O Princípio da Transparência no Tratamento de Dados Pessoais

O princípio da transparência ocupa um lugar central no regime jurídico da proteção de dados pessoais, ao constituir uma norma essencial para assegurar que os titulares compreendam de forma clara e acessível como os seus dados são tratados, por quem e para quais finalidades, entre outras características. Em um cenário marcado pelo crescimento exponencial do uso de tecnologias digitais e pelo aumento da complexidade dos sistemas de tratamento de dados, como a inteligência artificial, a aplicação desse princípio se torna ainda mais desafiadora.

No Brasil, a Lei Geral de Proteção de Dados estabelece a transparência como um dos princípios de tratamento de dados pessoais, o que reforça o dever dos agentes de tratamento para fornecer aos titulares informações claras, ostensivas e compreensíveis, de modo a permitir o pleno exercício de seus direitos. Paralelamente, o Marco Civil da Internet, em vigor desde 2014, já havia introduzido importantes disposições sobre a necessidade de transparência na relação entre provedores de aplicação e usuários, com regras específicas para garantir o acesso a informações.

2.1. Definição do Princípio da Transparência

O princípio da transparência, conforme definido pelo art. 6º, inciso VI, da LGPD, estabelece a “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial”.

Esse princípio visa assegurar que os titulares tenham pleno conhecimento sobre como os seus dados pessoais são tratados, por quem e para quais finalidades, a fim de promover um ambiente de confiança e segurança¹. Sem transparência, os titulares ficam vulneráveis a abusos e usos indevidos de seus dados pessoais, o que pode resultar em danos significativos. A transparência fortalece não apenas os direitos dos titulares, mas também a responsabilização dos controladores e operadores de dados.

¹ Sobre o princípio da transparência: FONSECA, 2021, p. 77-78.

Ao exigir que as informações sejam claras, precisas e acessíveis, a LGPD impõe um padrão de comunicação que transcende formalidades e foca na efetividade da compreensão por parte do titular. Isso significa que os agentes de tratamento, ao realizarem a coleta, processamento e outras operações de tratamento sobre os dados pessoais, têm a obrigação de adotar uma linguagem que seja compreensível para o público geral, evitando o uso de termos técnicos, jurídicos ou excessivamente complexos.

Essa clareza deve ser acompanhada de acessibilidade, o que implica disponibilizar essas informações de maneira intuitiva, por exemplo, em políticas de privacidade apresentadas em *interfaces* amigáveis e de fácil navegação, ou por meio de notificações diretas aos titulares.

A abrangência do princípio da transparência também engloba a identificação clara dos agentes de tratamento. De acordo com o artigo 9º da LGPD, os titulares têm o direito de saber quem está tratando seus dados e quais atividades estão sendo realizadas. Essa exigência visa não apenas informar, mas também responsabilizar os agentes de tratamento, o que reforça o controle dos titulares sobre seus dados.

Além disso, a transparência desempenha um papel fundamental no fortalecimento dos direitos dos titulares. A LGPD, em dispositivos como o art. 9º, VII, e o art. 18, garante que os titulares sejam devidamente informados sobre as possibilidades e formas de exercer direitos como os de acesso, correção, eliminação e portabilidade de seus dados pessoais.

Portanto, a transparência vai além de um simples dever de informar, mas visa capacitar os titulares, oferecendo-lhes as ferramentas e os conhecimentos necessários para que exerçam os seus direitos de forma efetiva e consciente.

Contudo, a aplicação do princípio da transparência deve ser equilibrada com a proteção de segredos comercial e industrial, como ressalta o próprio inciso VI do art. 6º da LGPD. Isso significa que, embora os agentes tenham o dever de fornecer informações sobre as atividades de tratamento, isso não se estende à divulgação de dados que possam comprometer estratégias comerciais ou revelar informações protegidas por segredo industrial ou comercial. Este equilíbrio é importante para assegurar que a transparência não prejudique a competitividade ou a inovação tecnológica dos agentes de tratamento.

Em suma, o princípio da transparência, ao mesmo tempo em que reforça os direitos dos titulares de dados, também promove a *accountability* para os agentes de

tratamento, ao criar um ambiente em que a confiança, o respeito à privacidade e a proteção de dados pessoais possam coexistir com a eficiência das operações de tratamento.

A harmonização entre a transparência e a proteção de informações estratégicas é indispensável para garantir que o avanço tecnológico e comercial ocorra sem comprometer os direitos fundamentais dos titulares.

Implementar o princípio da transparência apresenta desafios significativos, especialmente quando de tecnologias avançadas como a inteligência artificial (IA). Os algoritmos de IA, muitas vezes descritos como “caixas-pretas”, podem ser opacos e difíceis de explicar, o que dificulta a comunicação clara e compreensível aos titulares. Além disso, o equilíbrio entre transparência e a proteção de segredos comerciais ou propriedade intelectual dos algoritmos é uma preocupação legítima para as empresas.

2.2. A Transparência na LGPD e no Marco Civil da Internet

A transparência é um princípio relevante tanto na Lei Geral de Proteção de Dados quanto no Marco Civil da Internet (MCI), e cada uma dessas leis desempenha um papel complementar na regulação da relação entre titulares de dados e controladores e operadores no ambiente digital.

Enquanto a LGPD foca na proteção de dados pessoais de forma abrangente, por meio de normas específicas para o tratamento de dados em diferentes contextos, o MCI regula as relações entre provedores de aplicação e usuários, com ênfase nos direitos fundamentais à privacidade e à liberdade de expressão no meio digital.

Como visto no item anterior, na LGPD a transparência é positivada como um princípio de tratamento de dados pessoais (art. 6º, VI), determina que as atividades sejam realizadas de maneira clara, adequada e ostensiva, a fim de assegurar que o titular compreenda plenamente como seus dados são tratados.

Já o Marco Civil da Internet contém regras sobre a transparência na relação entre provedores de aplicação e usuários, a fim de estabelecer a base para uma internet mais segura. Nesse contexto, o art. 7º, VI, garante ao usuário o direito à informação clara e completa sobre os contratos de prestação de serviços². O art. 9º reforça esse compromisso, ao inserir no § 2º a transparência como um dos critérios norteadores das

² Sobre o assunto: SOUZA, LEMOS, 2016, p. 30.

condutas dos provedores de conexão em cumprimento ao princípio da neutralidade de rede.

A complementaridade existente entre o MCI e a LGPD é relevante para enfrentar os desafios do uso de tecnologias avançadas, como a inteligência artificial, que frequentemente envolvem o tratamento massivo e automatizado de dados pessoais no meio digital. A opacidade inerente a muitos modelos de inteligência artificial, por exemplo, representa uma barreira significativa para a efetivação da transparência, especialmente no que se refere à explicação das decisões automatizadas para os titulares dos dados pessoais. Além disso, a falta de padronização na comunicação das políticas de privacidade pelas plataformas digitais dificulta a compreensão das informações por parte dos usuários, o que exige avanços regulatórios e tecnológicos que facilitem o cumprimento das exigências de transparência previstas nas leis.

Ao integrar o princípio da transparência em suas normas, tanto a LGPD quanto o MCI demonstram um compromisso legislativo com a proteção de direitos fundamentais no ambiente digital. Porém, a efetividade dessas normas depende de uma articulação contínua entre regulação, fiscalização e inovação tecnológica, a fim de garantir que os titulares tenham acesso a informações claras e precisas sobre o tratamento de seus dados, independentemente da complexidade das tecnologias envolvidas.

3. O Uso de IA pelas Plataformas Digitais no Tratamento de Dados Pessoais

O avanço das tecnologias baseadas em inteligência artificial transformou significativamente a forma como os dados pessoais são tratados no ambiente digital. Plataformas digitais, como redes sociais, aplicativos de mensagens e *marketplaces*, fazem uso extensivo de sistemas de IA para coletar, processar, compartilhar e efetuar diversas outras atividades de tratamento de dados, a fim de viabilizar desde recomendações personalizadas até decisões automatizadas sobre moderação de conteúdo e publicidade direcionada.

Esse fenômeno, embora amplamente associado a ganhos de eficiência e inovação, também gera preocupações substanciais sobre proteção de dados, opacidade e responsabilidade no tratamento dos dados pessoais.

A IA permite que essas plataformas processem grandes volumes de dados de forma rápida e precisa, com a identificação de padrões complexos e a apresentação

de soluções que seriam inalcançáveis por métodos tradicionais. Porém, a sofisticação desses sistemas frequentemente resulta em práticas de tratamento de dados que são pouco compreendidas pelos usuários. Essa falta de clareza, agravada pela complexidade técnica e pelo caráter proprietário dos algoritmos utilizados, desafia diretamente a implementação do princípio da transparência.

3.1. Características dos Modelos de IA Aplicados em Redes Sociais e Aplicativos de Mensagens

Os modelos de inteligência artificial utilizados por redes sociais e aplicativos de mensagens desempenham um papel relevante no tratamento de dados pessoais, influenciando desde a personalização de conteúdos até o gerenciamento de interações entre os usuários. Essas tecnologias, projetadas para operar em larga escala, são caracterizadas pela capacidade de processar e analisar grandes volumes de dados e informações em tempo real, com a extração de padrões, inferências e tendências que moldam a experiência digital de bilhões de pessoas.

Uma das características mais marcantes desses modelos é o uso de aprendizado de máquina (*machine learning*), especialmente nas formas de aprendizado supervisionado, não supervisionado e por reforço. Esses métodos permitem que os algoritmos se adaptem continuamente com base nos dados que recebem, refinando suas operações para oferecer recomendações mais precisas e decisões mais eficazes. Por exemplo, os sistemas de recomendação em redes sociais como Instagram e TikTok utilizam modelos de aprendizado profundo (*deep learning*) para prever quais conteúdos têm maior probabilidade de engajar cada usuário, com base em seus comportamentos prévios, preferências explícitas e conexões sociais.

Além disso, os modelos de IA aplicados em redes sociais frequentemente utilizam processamento de linguagem natural (PLN), uma subárea focada em interpretar e gerar linguagem humana. Nos aplicativos de mensagens, como WhatsApp e Telegram, o PLN é usado para identificar padrões de texto, classificar conteúdos e, em alguns casos, aplicar filtros automáticos para identificar *spam* ou mensagens potencialmente nocivas. O PLN também é essencial para a implementação de *chatbots* e assistentes virtuais, que interagem diretamente com os usuários, processando e respondendo às suas dúvidas ou comandos de maneira automatizada.

Outra característica importante desses modelos é o uso de sistemas de classificação e segmentação de usuários, que agrupam indivíduos com base em

características demográficas, comportamentais ou contextuais, entre outros critérios. Essas segmentações são frequentemente empregadas para personalizar anúncios publicitários, identificar tendências e até mesmo moderar conteúdo de forma automatizada. Entretanto, a eficácia dessas segmentações pode variar significativamente a depender da qualidade dos dados utilizados e das premissas subjacentes aos modelos de IA, o que leva a questionamentos sobre possíveis vieses e discriminação algorítmica.

A escalabilidade desses modelos destaca sua capacidade de operar em níveis globais, por meio do tratamento de dados pessoais de bilhões de usuários em múltiplos idiomas, culturas e contextos. Essa abrangência geográfica amplifica os impactos das decisões algorítmicas, tornando ainda mais relevante o alinhamento das práticas de IA às regulações locais, como a LGPD no Brasil e o GDPR na União Europeia.

Embora essas características ofereçam às plataformas digitais ferramentas mais eficientes para melhorar a experiência do usuário e otimizar os modelos de negócios, elas também expõem desafios significativos no que diz respeito à proteção de dados, à transparência e à responsabilidade civil.

3.2. Tratamento de Dados Pessoais por IA

O tratamento de dados pessoais por inteligência artificial envolve processos automatizados que extraem, organizam, analisam e utilizam os dados dos titulares para finalidades diversas, desde personalização de serviços até tomada de decisões complexas.

A inteligência artificial é aplicada em uma grande variedade de setores, como a saúde (diagnóstico de doenças, análise de imagens médicas, desenvolvimento de tratamentos personalizados e assistência virtual a pacientes), o varejo (personalização de recomendações de produtos e otimização de estoque) e a prática judiciária (análise de documentos, leitura de petições e decisões judiciais, jurimetria etc.)³.

As plataformas digitais têm se tornado dependentes desses sistemas para garantir a eficiência de suas operações, personalizar os seus serviços e atender às expectativas de seus usuários. Porém, a complexidade e a autonomia desses modelos trazem desafios significativos para a transparência e a proteção de dados pessoais.

O uso de modelos de IA no tratamento de dados pessoais começa na coleta dos dados, que frequentemente ocorre de forma massiva e contínua. Plataformas como Facebook, WhatsApp e Instagram utilizam dados de interações, comportamentos de

³ CARDOSO, 2024, p. 19-20.

navegação, geolocalização, padrões de consumo e até mesmo preferências inferidas. A etapa seguinte é o processamento desses dados por meio de algoritmos de aprendizado de máquina, capazes de identificar padrões e correlacionar variáveis que escapariam à análise humana. Essas operações alimentam funcionalidades como sistemas de recomendação, anúncios personalizados e filtros automáticos de conteúdo.

Embora esses processos possam trazer benefícios práticos, como a maior relevância no conteúdo apresentado aos usuários, eles também geram preocupações sobre como e por que determinados dados são utilizados. Em muitos casos, os titulares não têm clareza sobre quais dados são coletados, para quais finalidades específicas e quais são os critérios utilizados para as decisões automatizadas. Essa falta de visibilidade contraria o princípio da transparência estabelecido pela LGPD, o que exige regulamentação da ANPD e práticas mais robustas para mitigar os riscos associados.

Assim, apesar dos avanços, a IA enfrenta desafios, particularmente em relação à transparência e explicabilidade. Os sistemas de inteligência artificial, especialmente aqueles baseados em aprendizado profundo (“*deep learning*”), muitas vezes operam como “caixas-pretas” (*black boxes*), com processos internos opacos e difíceis de interpretar.

O termo “*black box*” na inteligência artificial refere-se à natureza opaca e complexa de muitos modelos de IA, especialmente aqueles baseados em aprendizado profundo (“*deep learning*”). Esses modelos são denominados de caixas-pretas porque, embora sejam capazes de produzir resultados precisos, o processo pelo qual eles chegam a essas conclusões é, muitas vezes, difícil (ou impossível) de interpretar ou entender, tanto pelos usuários finais quanto pelos desenvolvedores.

A expressão “caixa-preta” ganhou notoriedade no campo da inteligência artificial a partir das reflexões de Frank Pasquale, que atribuiu a ela um duplo significado. Primeiro, como um dispositivo de registro e, segundo, como um sistema cujo funcionamento interno não pode ser completamente explicado. Na IA, o termo refere-se à incapacidade de observar ou compreender como uma entrada específica gera uma saída em um modelo algorítmico. Embora os dados de entrada e os resultados possam ser visíveis, os processos internos que conectam os dois permanecem obscuros, ou seja, é possível observar as entradas e saídas da caixa-preta, mas não é possível afirmar como uma entrada se transforma em uma das saídas⁴.

⁴ PASQUALE, 2015, p. 3.

Uma “caixa-preta” na IA caracteriza-se por ser um sistema cujas operações e decisões não são facilmente compreensíveis ou explicáveis por seres humanos, nem mesmo por aqueles que o desenvolveram. Isso implica que, ainda que se consiga observar os insumos e os resultados, o caminho lógico percorrido pelo algoritmo para chegar a uma decisão ou previsão é praticamente ininteligível. Essa opacidade não é acidental, mas, ao contrário, é frequentemente um produto da alta complexidade dos modelos utilizados.

Diversos fatores podem contribuir para que os modelos de IA sejam considerados caixas-pretas, tais como a complexidade do algoritmo (por exemplo, as redes neurais profundas possuem estruturas com várias camadas e conexões entre neurônios artificiais, o que dificulta a rastreabilidade do processo de decisão), o processamento de grandes volumes de dados (a análise de grandes quantidades de dados em padrões não intuitivos resulta em modelos precisos, mas com lógica interna quase impossível de ser interpretada.), o aprendizado não supervisionado (em sistemas que não utilizam dados previamente rotulados, as conexões formadas entre variáveis podem ser imprevisíveis e ininteligíveis), a interdependência de características (algoritmos frequentemente criam relações complexas entre características dos dados, dificultando a identificação de fatores decisivos para um resultado) e a natureza probabilística (muitos modelos operam com base em estimativas e distribuições de probabilidade, o que torna suas decisões inerentemente incertas e difíceis de justificar).

A opacidade dos modelos de inteligência artificial apresenta diversas dificuldades, especialmente no contexto da proteção de dados pessoais e da conformidade com as normas da LGPD.

Entre os impasses que podem surgir com a utilização de ferramentas de IA no tratamento de dados pessoais, destacam-se os seguintes:

(a) Falta (ou insuficiência) de transparência: a ausência de transparência (ou sua redução) impede que os usuários compreendam como e por que uma decisão foi tomada, o que pode gerar desconfiança e resistência ao uso de tecnologias de IA;

(b) Vieses, ruídos e discriminação: os modelos de IA podem inadvertidamente absorver vieses e ruídos presentes nos dados de treinamento, o que potencialmente resulta em decisões discriminatórias⁵. Associada a isso, a falta de transparência dificulta a identificação e a correção desses vieses e ruídos;

⁵ Sobre vieses e ruídos: KAHNEMAN, SIBONY, SUNSTEIN, 2021.

(c) Dificuldades na realização de auditorias e verificações de conformidade: a falta de explicabilidade dificulta a tarefa de auditar os sistemas de IA e verificar sua conformidade com os deveres legais, como o registro de operações de tratamento (art. 37 da LGPD) e o cumprimento dos princípios de responsabilização e prestação de contas (art. 6º, X);

(d) Responsabilização: quando uma decisão tomada por um sistema de inteligência artificial (ou por uma pessoa, a partir de dados processados por ele) produz um resultado adverso ou controverso ao titular de dados pessoais, a falta (ou a insuficiência) de explicabilidade dificulta a atribuição de responsabilidade, tanto para os desenvolvedores quanto para os operadores do modelo de IA.

Essa falta de transparência apresenta desafios críticos para a proteção de dados pessoais. Por exemplo, titulares que questionam o uso de seus dados ou os critérios de uma decisão automatizada enfrentam barreiras para obter respostas claras, especialmente dos provedores de aplicações de redes sociais, o que compromete a sua capacidade de exercer direitos garantidos pela LGPD, como o acesso (arts. 9º e 18, II, da LGPD), a retificação (art. 18, III, da LGPD) e a explicação de decisões automatizadas (art. 20 da LGPD).

A opacidade dos modelos de IA também cria dificuldades para atribuição de responsabilidade na eventual ocorrência de danos aos titulares de dados pessoais. Se um usuário for prejudicado por uma decisão algorítmica (como ser erroneamente bloqueado em uma plataforma ou receber anúncios discriminatórios), pode ser difícil identificar o responsável direto pelo dano: o desenvolvedor do modelo, a plataforma que o implementou ou um terceiro que forneceu os dados. Essa fragmentação de responsabilidades contrasta com as normas de *accountability* previstas na LGPD, que exige que os agentes de tratamento sejam capazes de demonstrar conformidade com a lei e de reparar os danos causados por suas atividades.

Portanto, o tratamento de dados pessoais por IA, apesar de seu potencial de transformação e eficiência, apresenta desafios significativos para a transparência e a proteção de direitos. Para mitigar esses problemas, as plataformas digitais devem adotar práticas adequadas de governança algorítmica, o que inclui a explicabilidade dos modelos, a realização de auditorias independentes e a comunicação clara com os titulares. O fortalecimento da transparência e da responsabilidade civil é indispensável para assegurar que os avanços tecnológicos respeitem os direitos fundamentais dos usuários e contribuam para um ambiente digital mais equilibrado e confiável.

4. Reflexos da Utilização de IA sobre a Responsabilidade Civil das Plataformas Digitais

O uso intensivo de inteligência artificial pelas plataformas digitais causa profundas transformações nos modelos de negócios, na interação com os usuários e, principalmente, nas formas de tratamento de dados pessoais. Essa evolução tecnológica também leva a questões complexas sobre a responsabilidade civil desses provedores de aplicação, em consequência dos danos causados pelo uso de sistemas automatizados. Na medida em que os algoritmos tomam decisões que afetam diretamente a vida dos usuários, torna-se imprescindível discutir como as normas de responsabilidade civil se aplicam a esse novo contexto, especialmente diante das características de opacidade e autonomia da IA.

O marco regulatório brasileiro, representado pela Lei Geral de Proteção de Dados Pessoais e pelo Código Civil, estabelece normas sobre o dever de reparação por danos causados a terceiros. No entanto, a aplicação desses preceitos enfrenta desafios significativos no âmbito da IA. Entre os problemas centrais estão a dificuldade de identificar responsáveis diretos, a opacidade dos modelos algorítmicos (que dificulta a comprovação de culpa ou nexo causal) e a necessidade de compatibilizar as inovações tecnológicas com a proteção dos direitos fundamentais, como a proteção de dados pessoais.

4.1. Responsabilidade das Plataformas Digitais por Danos Causados por IA

As plataformas digitais desempenham um papel central no tratamento de dados pessoais por meio de sistemas de inteligência artificial. Essas tecnologias, embora indispensáveis para o funcionamento eficiente de muitas aplicações, também podem gerar danos aos usuários, desde prejuízos econômicos até violações de direitos fundamentais, como a privacidade e a não discriminação. Nesse contexto, a responsabilidade civil das plataformas digitais é um tema que afeta a regulação dos usos de IA e exige uma análise detalhada de como as normas jurídicas podem ser aplicadas ou adaptadas para tratar as peculiaridades de tais atividades.

No direito brasileiro, a responsabilidade civil pode ser fundamentada em duas teorias principais: a da culpa e a do risco. A primeira exige a comprovação de culpa, nexo causal e dano, enquanto a segunda dispensa a análise da culpa,

concentrando-se no risco inerente à atividade desempenhada⁶. A aplicação de cada uma dessas teorias às plataformas digitais depende de diversos fatores, como a natureza do dano, o nível de controle que a plataforma exerce sobre o sistema de IA e a previsibilidade dos riscos associados ao uso da tecnologia.

A principal regra está no caput do art. 927 do Código Civil: “Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo”. Em resumo, quem causar um dano a alguém tem o dever legal de repará-lo, a fim de reequilibrar a relação jurídica e, na medida do possível, retornar ao estado jurídico anterior (*status quo ante*).

Os sistemas de IA introduzem novos desafios para a aplicação dessas normas e teorias. A opacidade dos algoritmos dificulta a identificação do nexo causal entre o funcionamento do modelo e o dano sofrido pelo usuário. Por exemplo, se uma decisão automatizada discriminatória for tomada por um sistema de recomendação baseado em IA, como provar que essa decisão específica resultou de um viés algorítmico e não de um erro humano ou de fatores externos? Essa dificuldade na rastreabilidade do processo decisório dificulta a atribuição de responsabilidade e, inclusive, a verificação da licitude – ou não – da ação questionada.

Outro aspecto relevante está na autonomia das plataformas no desenvolvimento e implementação de sistemas de IA. Ao atuarem como controladores dos dados, os provedores de aplicação são responsáveis por definir as finalidades do tratamento e os meios utilizados para tal, com a consequente adequação à LGPD. Esse papel implica um dever reforçado de diligência na supervisão do funcionamento dos algoritmos, na garantia da transparência e na adoção de medidas que minimizem riscos para os titulares de dados. A ausência ou insuficiência dessas medidas pode configurar omissão culposa (quando se aplicar a responsabilidade subjetiva), o que gera a responsabilização da plataforma pelos danos decorrentes.

Além disso, a LGPD inclui o princípio da *accountability* (art. 6º, X) entre aqueles que norteiam as atividades de tratamento de dados, o que reforça o dever dos agentes de tratamento de demonstrar conformidade com a lei e adotar práticas adequadas e eficazes para proteger os dados pessoais. Esse princípio tem implicações diretas na responsabilidade civil das plataformas digitais, pois exige que estas não

⁶ Sobre o conceito e os aspectos históricos da regulação jurídica da responsabilidade civil, ver Capítulo 1 de: PEREIRA, 2018.

apenas cumpram as normas de proteção de dados, mas também sejam capazes de provar que suas práticas são adequadas para prevenir danos.

Nas hipóteses de responsabilidade objetiva, o foco recai sobre o risco inerente à atividade desenvolvida pelas plataformas. Essa abordagem é relevante para as situações em que a inteligência artificial for utilizada em contextos de alto impacto, como sistemas de segurança, análises financeiras ou classificação automatizada de conteúdo. Nesses casos, a simples demonstração do dano e do nexo causal entre a conduta da plataforma e o prejuízo sofrido pode ser suficiente para fundamentar a responsabilização, independentemente da existência de culpa.

Porém, a aplicação desse regime de responsabilidade deve ser compatibilizada com o princípio da transparência, que exige mais do que a simples observância de regras genéricas. No caso de remoção ou bloqueio de conteúdo por plataformas digitais, por exemplo, a transparência impõe que o provedor seja claro e específico quanto aos motivos que justificam sua decisão. Alegações vagas ou genéricas, como a suposta “violação das normas da comunidade” ou o descumprimento dos “termos e condições de uso”, não atendem a esse padrão e não devem ser consideradas como válidas.

Além disso, a transparência demanda que o usuário seja ouvido previamente, para garantir que possa apresentar a sua versão dos fatos antes da adoção de qualquer medida restritiva. Esse procedimento não é apenas uma exigência de boa-fé contratual e respeito ao usuário, mas também uma salvaguarda do direito fundamental à liberdade de expressão, assegurado pelo art. 5º, IV, da Constituição. A ausência de mecanismos adequados para ouvir os usuários, aliados ao uso de justificativas genéricas, pode configurar abuso por parte das plataformas e resultar em restrições arbitrárias ou desproporcionais ao exercício da manifestação do pensamento.

Dessa forma, nos casos em que a inteligência artificial for utilizada para moderar ou excluir conteúdo, o respeito à transparência deve ser observado em todas as etapas do processo decisório. Isso inclui a disponibilização de informações claras sobre os critérios aplicados pelo algoritmo, a explicitação das razões que levaram à decisão automatizada e a garantia de que os usuários possam contestar essas decisões, de forma prévia a qualquer medida restritiva. O não cumprimento dessas exigências pode não apenas justificar a responsabilização objetiva da plataforma, mas também configurar uma violação de direitos fundamentais dos usuários, especialmente a liberdade de expressão e a proteção de seus dados pessoais.

Assim, a transparência, quando efetivamente aplicada, não se limita a um compromisso de comunicação clara, mas opera como um princípio estrutural que equilibra o poder das plataformas digitais com os direitos e garantias dos indivíduos, a fim de promover um ambiente digital mais justo e democrático.

4.2. Critérios de Responsabilização

A responsabilização das plataformas digitais por danos causados pelo uso de inteligência artificial no tratamento de dados pessoais exige uma análise criteriosa dos fundamentos jurídicos aplicáveis, com destaque para os critérios de culpa, risco e dever de informação. Cada um desses critérios oferece uma perspectiva distinta para abordar a responsabilidade civil, para equilibrar a proteção dos direitos dos titulares de dados com o estímulo à inovação tecnológica.

A responsabilidade subjetiva, ainda adotada como regra geral pelos arts. 186 e 927 do Código Civil, exige a comprovação de três elementos: culpa do agente, dano sofrido pela vítima e nexo causal entre ambos. Nas plataformas digitais, a culpa ou o dolo do agente de tratamento pode manifestar-se de diferentes formas, como:

- Falta de diligência no desenvolvimento ou implementação da IA: se a plataforma utilizar um modelo de IA que apresentar falhas conhecidas, como vieses algorítmicos ou vulnerabilidades de segurança, pode ser responsabilizada por negligência;

- Omissão no monitoramento e atualização dos sistemas: a ausência de auditorias ou de atualizações regulares para identificar problemas no funcionamento da IA também pode configurar uma conduta culposa;

- Falta de transparência: a falha em informar adequadamente os titulares sobre o uso de IA ou os critérios das decisões automatizadas adotados na decisão pode ser interpretada como imprudência, especialmente diante das exigências legais de clareza e acessibilidade previstas na LGPD.

Porém, a teoria da responsabilidade subjetiva e a aplicação do critério da culpa enfrenta desafios significativos diante de danos causados por ato ou decisão adotado por sistema de IA, em virtude de sua complexidade técnica e da dificuldade de identificar com precisão os responsáveis diretos pelas decisões que levaram ao ato lesivo.

Por sua vez, a responsabilidade objetiva (especialmente aquela fundamentada na teoria do risco, prevista na parte final do parágrafo único do art. 927

do Código Civil) dispensa a análise de culpa, ao se concentrar na atividade desempenhada e no dano causado. Esse critério é particularmente relevante no caso de plataformas digitais que utilizam IA, considerando o potencial de riscos inerentes ao tratamento automatizado de dados pessoais.

Na LGPD, o risco é amplificado pela escala das operações das plataformas digitais, que frequentemente envolvem o tratamento de dados pessoais sensíveis e a tomada de decisões automatizadas com impactos diretos sobre os titulares.

Como principal exemplo, estão os algoritmos de moderação de conteúdo que resultam em remoções indevidas e os sistemas de recomendação que perpetuam discriminações negativas. Nesses casos, a demonstração de que o dano é resultado do uso de IA pode ser suficiente para responsabilizar a plataforma, independentemente da prova de culpa.

Ressalta-se que a LGPD não contém um regime próprio e específico de responsabilidade civil no tratamento de dados pessoais, mas apenas regras que especificam o que é um tratamento irregular (art. 44), indicam quem são os responsáveis por danos ou atos ilícitos (art. 42), ressalvam as excludentes de responsabilidade (art. 43) e remetem à lei própria (que é o Código de Defesa do Consumidor) a aplicação das regras de responsabilidade sobre o tratamento de dados nas relações de consumo (art. 45).

O *caput* do art. 42 da LGPD prevê que “o controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”.

Em consequência, o agente de tratamento deve demonstrar que realiza as suas atividades de acordo com as normas legais e regulamentadoras cabíveis (inclusive eventuais regras definidas no consentimento do titular) e a eficácia das medidas adotadas para a proteção dos dados pessoais.

Por isso, o agente poderia ser responsabilizado objetivamente pelos danos causados ao titular dos dados pessoais em virtude do exercício de suas atividades de tratamento, em decorrência do descumprimento das normas legais e do dano derivado dessa conduta, independentemente de culpa.

5. Considerações Finais

O artigo analisou os impactos do uso de inteligência artificial pelas plataformas digitais no tratamento de dados pessoais, com foco nos reflexos sobre o princípio da transparência e a responsabilidade civil. Buscou-se demonstrar que a opacidade dos modelos de IA, associada à complexidade técnica e à dificuldade de rastreabilidade das decisões automatizadas, representa o maior desafio para a proteção dos direitos dos titulares de dados. A ausência de explicabilidade compromete não apenas a compreensão das decisões pelos usuários, mas também a conformidade com as exigências legais, como as previstas na LGPD e no Marco Civil da Internet.

Ao longo do texto, destacam-se as dificuldades impostas pelo uso de IA na concretização do princípio da transparência, especialmente diante do problema da “caixa-preta”. Também foram discutidas as implicações dessas tecnologias na responsabilidade civil das plataformas digitais, com destaque para as teorias objetiva e subjetiva, além do dever de informação. Constatou-se que, embora a IA traga benefícios inegáveis para a personalização de serviços e a eficiência operacional, seu uso exige salvaguardas adequadas para proteger os direitos fundamentais, como os dados pessoais, a privacidade, a não discriminação e a liberdade de expressão.

Ressalta-se a importância de equilibrar a inovação tecnológica com a proteção dos direitos fundamentais. É essencial que as plataformas digitais adotem práticas mais transparentes, incluindo o desenvolvimento de modelos de IA que sejam explicáveis e auditáveis, bem como desenvolvam mecanismos acessíveis de comunicação e contestação para os usuários. Ao mesmo tempo, o papel do legislador e dos órgãos reguladores é importante para a criação de um ambiente jurídico que incentive a inovação, mas que não negligencie a proteção dos titulares de dados pessoais.

A responsabilização das plataformas digitais por danos causados por IA é um elemento indispensável para equilibrar inovação tecnológica e proteção de direitos fundamentais. A crescente dependência de sistemas automatizados no tratamento de dados pessoais exige não apenas a adaptação das normas existentes, mas também a criação de novos mecanismos regulatórios que considerem as especificidades da IA. Esses mecanismos devem incluir a exigência de explicabilidade dos algoritmos, auditorias regulares, testes de vieses e discriminação, além da imposição de sanções eficazes em caso de descumprimento.

Conclui-se que o avanço da inteligência artificial nas plataformas digitais demanda um compromisso conjunto entre tecnologia e regulação. A proteção de dados

peçoais e o respeito aos direitos fundamentais não devem ser vistos como barreiras ao desenvolvimento, mas como elementos estruturantes de uma sociedade digital mais responsável. O principal desafio está em transformar a inovação tecnológica em uma aliada na promoção desses valores, para criar um ambiente em que usuários e plataformas possam coexistir em harmonia e com segurança jurídica.

Referências

CARDOSO, Oscar Valente. *Inteligência artificial, direito e processo*. São Paulo: Dialética, 2024.

FONSECA, Edson Pires da. *Lei Geral de Proteção de Dados Pessoais - LGPD*. Salvador: JusPodivm, 2021.

KAHNEMAN, Daniel; SIBONY, Olivier; SUNSTEIN, Cass R. *Noise: a flaw in human judgment*. New York: Little, Brown Spark, 2021.

PASQUALE, Frank. *The black box society: the secret algorithms that control money and information*. Cambridge: Harvard University Press, 2015.

PEREIRA, Caio Mário da Silva. *Responsabilidade civil*. 12. ed. Rio de Janeiro: Forense, 2018.

SOUZA, Carlos Affonso; LEMOS, Ronaldo. *Marco civil da internet: construção e aplicação*. Juiz de Fora: Editar, 2016.