Lex Humana, v. 16, n.4, 2024, ISSN 2175-0947

A ADEQUAÇÃO DO CHATGPT ÀS EXIGÊNCIAS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

THE ADEQUACY OF THE CHATGPT TO THE REQUIREMENTS OF THE GENERAL DATA PROTECTION LAW

ENZO BAGGIO LOSSO
Pontifícia Universidade Católica do Paraná, Brasil
enzo.losso@hotmail.com

CINTHIA OBLADEN DE ALMENDRA FREITAS
Pontifícia Universidade Católica do Paraná, Brasil
cinthia.freitas@pucpr.br

Received: 10 Sept 2024
Accepted: 30 Oct 2024
Published: 30 Nov 2024

Corresponding author:
enzo.losso@hotmail.com

Resumo: O presente artigo analisa as adequações que já foram e que devem ser realizadas no *ChatGPT* frente aos princípios e fundamentos da Lei Geral de Proteção de Dados Pessoais (LGPD). A IA Generativa *ChatGPT* está crescendo exponencialmente em número de usuários, entretanto a coleta excessiva de dados pelo *chatbot* levanta preocupações em relação ao consentimento e o devido tratamento de dados de seus usuários. Por meio de uma metodologia dedutiva, foi realizada uma pesquisa bibliográfica documental sobre o tema, discutindo se a Política de Privacidade da *OpenAI*, desenvolvedora do *ChatGPT*, está de acordo com a lei de proteção de dados brasileira. Ademais, foram realizadas análises em relação à responsabilidade do controlador frente à violação da LGPD, bem como em relação a bloqueios e suspensões provisórias de *chatbots* na Itália e no Brasil em razão da violação de suas legislações de proteção de dados. Por fim, o artigo identificou pontos os quais já há uma devida adequação à LGPD pelo *ChatGPT* como direitos dos usuários frente ao tratamento de seus dados, bem como apresentou soluções como as quais podem melhorar sua adequação à LGPD.

Palavras-chave: Inteligência Artificial. ChatGPT. Lei Geral de Proteção de Dados Pessoais. Proteção de Dados. Privacidade.

Abstract: This article analyzes the adequacies that have been made or must be made in ChatGPT against the principles and fundamentals of the Brazilian General Personal Data Protection Law (LGPD). The Generative AI ChatGPT is growing exponentially in numbers of users. However, the excessive data collection by the chatbot raises concerns regarding the consent and due treatment of its user's data. Through a deductive methodology, a documental bibliographic research was conducted on the subject, discussing if the Privacy Policy of OpenAI, ChatGPT's developer, is adequate with the Brazilian data protection law. In addition, analysis were carried out regarding the responsibility of the controller in a violation of the LGPD, as well as regarding the provisional blocking and suspension of chatbots due to the violation of their data protection legislations. Finally, the article identified aspects that already has the right adequacy to the LGPD by ChatGPT like the user's rights with their data treatment, as well as solutions that could improve its adequacy to the LGPD.

Keywords: Artificial Intelligence. ChatGPT. Brazilian General Personal Data Protection Law. Data Protection. Privacy.

1. INTRODUÇÃO

Nos dias atuais, a proteção de dados pessoais vem ganhando cada vez mais força e relevância, visto que cada vez mais dados são coletados e armazenados não somente por estabelecimentos comerciais, mas principalmente na internet por sites e *big techs*. A Lei Geral de Proteção de Dados Pessoais (LGPD) foi promulgada em 14 de agosto de 2018 (BRASIL, 2018) e consolidou a proteção de dados pessoais no Brasil, sendo considerada um marco histórico neste âmbito. A lei prevê a criação da Autoridade Nacional de Proteção de Dados que, a partir de 1º de agosto de 2021, atua na vigilância, fiscalização e salvaguarda constante da LGPD e de seus princípios e fundamentos, os quais serão discutidos neste artigo.

As inteligências artificiais ganharam uma especial relevância no ano de 2023 com a popularização do *ChatGPT* e de outras Inteligências Artificiais (AIs) generativas, não somente de texto, mas também de geração de imagens e vídeos conforme descrito pelo usuário, bem como seus aperfeiçoamentos em 2024 como o *ChatGPT 4o*. Tal classe de inteligências artificiais, principalmente as que geram textos, tendo como principal exemplo o *ChatGPT*, são diariamente alimentadas por milhares de informações e dados de seus usuários, trazendo a preocupação do consentimento e tratamento dos dados pessoais dos usuários que utilizam tais *chatbots*.

Esta coleta massiva de dados pelas IAs Generativas traz à tona a problemática de adequação destes *softwares* às legislações de proteção de dados, principalmente à LGPD, não somente no trabalho que já foi feito neste âmbito, mas também as adequações que devem futuramente ser feitas, visto que é possível verificar que o consentimento e o tratamento de dados, muitas vezes é realizado de modo irregular, de modo a violar não somente a LGPD mas também outras legislações externas ao Brasil, a exemplo da Itália em relação ao *ChatGPT* bem como o Brasil no caso do bloqueio da *Meta AI*. Nestas circunstâncias, a responsabilização do controlador destes *chatbots* deve ser rígida, pois a proteção de dados nos dias atuais é considerada um direito fundamental previsto na Constituição Federal (BRASIL, 1988). Portanto, frente à excessiva coleta de dados do *chatbot* e a existência da legislação interna de proteção de dados, a questão que se traz é

se o *ChatGPT* está ou não adequado à LGPD, verificando a existência de elementos essenciais como o consentimento e o tratamento correto de dados nos conformes à LGPD.

Neste sentido, a pesquisa possui como objetivo discutir sobre a LGPD e sua influência frente ao consentimento e tratamento de dados realizados pelo *ChatGPT*, bem como a adequações que o *chatbot* deve realizar para estar de acordo com seus princípios e fundamentos, desde sua criação até as adequações que não foram implementadas e que podem vir a fazer parte da política de privacidade do serviço, realizando uma análise complexa entre os princípios e fundamentos da LGPD e a Política de Privacidade da *OpenAI*, criadora e desenvolvedora do *ChatGPT*, bem como uma análise acerca da responsabilidade que poderia a ser aplicada à desenvolvedora em caso de violação das normas presentes na LGPD. Além disso, busca-se analisar o caso de bloqueio provisório que ocorreu na Itália, bem como uma breve análise das nuances que envolvem a suspensão da *Meta AI* no Brasil, destacando a importância da adequação para a correta proteção e tratamento de dados.

Em relação à metodologia de pesquisa, foi utilizado o método dedutivo, utilizando o procedimento bibliográfico por meio de documentações diretas como artigos científicos, livros, legislação vigente nacional e exterior, bem como notícias e reportagens.

Este artigo busca contribuir para uma renovação na temática de proteção de dados, desta vez analisando o tratamento de dados no viés das inteligências artificiais, mecanismos estes que são cada vez mais utilizados, crescendo a coleta de dados de modo exponencial. Assim, é de suma importância a discussão de adequação destes para a proteção dos dados coletados, sendo este artigo uma porta para uma aplicação cada vez mais eficaz da LGPD tanto ao *ChatGPT*, quanto outras inúmeras inteligências artificiais generativas que devem ser adequadas à tal legislação.

2. CONCEITOS, FUNDAMENTOS E PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS APLICÁVEIS ÀS INTELIGÊNCIAS ARTIFICIAIS

Neste primeiro capítulo, são analisados primeiramente os conceitos, fundamentos e princípios da Lei Geral de Proteção de Dados que envolvem dados pessoais sensíveis tanto no âmbito geral de aplicação da lei como voltado para a Inteligência Artificial

Generativa. Em seguida, são analisados os limites que a LGPD impõe, por meio de seus fundamentos e princípios, em inteligências artificiais, utilizando como base o *ChatGPT*.

2.1. CONCEITOS, FUNDAMENTOS E PRINCÍPIOS DA LGPD E SEU PAPEL REGULATÓRIO NA PROTEÇÃO DE DADOS PESSOAIS E SENSÍVEIS

A Lei Geral de Proteção de Dados Pessoais (LGPD), ao ser promulgada em 14 de agosto de 2018, apesar de não iniciar a tutela de proteção de dados pessoais no Brasil, pode ser considerada como um marco legal e histórico, possuindo um papel central muito importante na estruturação e organização da temática de proteção de dados pessoais no país, como bem destaca Doneda (2021, p. 10):

> (...) o fato é que é muito recente no Brasil o elemento indutor que, finalmente, organizou em torno da proteção de dados toda uma verdadeira 'fenomenologia' jurídica, comportada por situações jurídicas nas quais o elemento principal ou determinante diz respeito a um tratamento de dados pessoais.

A LGPD, em vista desta estruturação e organização, obteve uma posição ambivalente no ordenamento jurídico, possuindo um caráter especial, na medida que as disposições da mesma prevalecerão quando as disposições de outros regulamentos se mostrarem incompatíveis entre si, prevalecendo a LGPD como norma específica de proteção de dados pessoais. Além disso, a regulação pode possuir ao mesmo tempo um aspecto geral, pois "a norma produz efeitos horizontais sobre todas as áreas econômicas e sobre quase todos os campos de atuação do Poder Público" (WIMMER, 2021, p. 377).

Destaca-se a relevância da lei em razão de, por meio de seu art. 1º, a proteção de dados pessoais passa a possuir o *status* de interesse nacional, além de destacar o caráter geral do marco regulatório, ultrapassando assim a espera privada, mas atingindo a espera pública que, antes da promulgação da mesma, geralmente não se atingia.

Interessante mencionar também a grande influência do RGPD (Regulamento Geral de Proteção de Dados ou também conhecida pela sua sigla em inglês *GDPR - General Data Protection Regulation)* europeu na legislação brasileira de proteção de dados, que se reflete principalmente pela aplicação do modelo da racionalidade *ex ante*, sendo esta imposta a todo e qualquer ato de tratamento de dados pessoais (OLIVEIRA, 2022, p. 89-90). Neste sentido, é necessário haver justificativa da coleta ou qualquer outro ato de tratamento de dados mesmo antes de realizá-la, enquadrando nas hipóteses

previstas no art. 7º da LGPD. A partir deste modelo, parte-se do pressuposto que todos os dados pessoais são relevantes para a tutela jurídica, em razão do crescimento exponencial do processamento de dados pessoais na sociedade, demandando assim tutela do tratamento de dados pessoais.

Com tais conceitos e institutos presentes na LGPD, já se evidenciam fundamentos e princípios, nos quais os dados pessoais são regulamentados. Primeiramente, os fundamentos, previstos no art. 2º da LGPD (BRASIL, 2018), sustentam a área da proteção de dados pessoais, os quais desempenham um papel essencial na realização dos objetivos e escopo desejados pelo legislador para o marco regulatório, quais sejam eles: (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; (VII) os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Em primeira vista, conforme bem enumerado por Dânton Zanetti de Oliveira (2022, p. 92), "tais fundamentos são verdadeiros elementos constituintes e organizadores da LGPD, mesmo que alguns deles possam, à primeira vista parecer incompatíveis entre si". Entretanto, tal conflito se dá em razão de, apesar da lei favorecer a privacidade e os direitos fundamentais do cidadão, a lei também busca o desenvolvimento econômico, pois os parâmetros estabelecidos garantem maior segurança jurídica.

Vale, portanto, destacar os princípios da LGPD, os quais alguns já podem ser evidenciados por meio da própria lei e de seus fundamentos e conceitos já enumerados anteriormente. A LGPD, conforme detalha Dânton Zanetti de Oliveira, foi introduzida como uma lei principiológica, na qual preza por cláusulas gerais ou abertas que, conforme conceitua o Ministro Luís Roberto Barroso (2005, p. 9-10), tratam-se de conceitos jurídicos indeterminados os quais não é possível extrair o conceito ou solução pela simples leitura da letra da lei, necessitando da integração do comando jurídico e de uma avaliação casuística para interpretar a lei. Tal questão do aspecto principiológico contribui para que a lei tenha uma grande longevidade, visto que caso determinasse de forma taxativa e exaustiva todos os atos lícitos e ilícitos, a norma se tornaria rapidamente obsoleta em razão dos contínuos avanços tecnológicos. Um exemplo é a coleta de dados realizada para fins de aplicação de técnicas de Inteligência Artificial. Rodotà (RODOTÀ

apud LIMA, 2020, p. 175) destaca a importância de a lei possuir cláusulas gerais para se adaptar às mudanças contínuas da sociedade:

> (...) em qualquer caso, assume particular importância o tipo de técnica legislativa utilizada, que deve ter em conta as características da matéria a regulamentar, caracterizada por uma fonte dinâmica e uma tendência contínua para a mudança. Já foi dito que a legislação deve partir de cláusulas gerais, adaptáveis a novas situações pela atividade interpretativa dos juízes ou pelas prescrições regulamentares das autoridades.

Para uma apertada síntese ao contexto histórico dos princípios que regem a proteção de dados pessoais brasileira, o Ministro Ricardo Villas Bôas Cueva (2017), em análise à insuficiente proteção de dados pessoais no Brasil previamente à promulgação da LGPD, já demonstrava a existência de muitos princípios para a proteção de dados aplicados na prática, como por exemplo, pelas diretrizes para a Cooperação e Desenvolvimento Econômico (OCDE), que já propunham muitos princípios básicos para a proteção de dados, sendo os mesmos aplicados no Brasil.

Nos dias atuais, a LGPD consolidou e até ampliou os princípios já existentes e aplicados nacionalmente e até internacionalmente, estando os mesmos previstos nos incisos do art. 6º da LGPD (BRASIL, 2018), quais sejam: finalidade, adequação, necessidade, livre acesso, qualidade de dados, transparência, segurança, prevenção, não discriminação e prestação de contas. Além destes princípios, o art. 6º da lei também define que em todas as atividades de tratamento de dados pessoais deve-se observar a boa-fé, sendo este um componente basilar para tais atividades.

Conforme já visto, dá-se uma grande importância ao princípio da finalidade, que, nas palavras da própria LGPD, é a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades". Tal princípio encontra-se presente em muitos regulamentos, inclusive no regulamento europeu, demonstrando a relevância de tal princípio para o instituto da proteção dos dados pessoais. Danilo Doneda (2011, p. 91-108) ainda explica que "qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados". Tal princípio realça também a racionalidade *ex ante* da lei, sempre exigindo a comunicação e o consentimento do titular dos dados. No contexto da pesquisa, o princípio se mostra ainda mais relevante, devendo tal tratamento de dados ser informado e justificado ao usuário do *chatbot*, antes mesmo da utilização da Inteligência Artificial Generativa, a exemplo do *ChatGPT*.

Além disso, é indispensável citar a importância, não só de todos os outros princípios, mas também os princípios da necessidade e transparência. O princípio da necessidade se trata, nas palavras da lei (BRASIL, 2018), da "limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados". As empresas responsáveis pelo desenvolvimento de *chatbots*, neste caso, devem se atentar para quais dados irão coletar de seus usuários, devendo esta coleta ser de dados somente necessários e sempre explicando o motivo do tratamento destes. Nesta seara, o conceito de minimização de dados se mostra importante, na qual deve-se coletar o mínimo possível de dados do usuário e mantê-los o mínimo de tempo possível armazenados, somente cumprindo sua finalidade estabelecida e consentida pelo usuário.

Ainda, o princípio da transparência (BRASIL, 2018) trata da "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". Este princípio traz à tona perguntas para as quais as respostas devem sempre ser claras e precisas ao usuário de aplicações que envolvam técnicas de Inteligência Artificial, a exemplo de: o que é coletado?, para que e porquê coletam? e qual o uso destes dados?.

Por fim, o princípio da prestação de contas, também chamado de princípio da *accountability*, possui um papel muito importante na LGPD. A prestação de contas traz a questão de demonstração da eficácia das medidas de proteção de dados pessoais utilizada pelo operador de dados, trazendo consigo um os deveres de responsabilização bem como a prestação de contas, conforme destaca Bruno Bioni (2022, p. 42):

> Com isso, a principiologia da LGPD passa a ter uma racionalidade precaucionária. Isso porque, ao lado do princípio da prevenção de danos existentes em todas as fases da LGPD, passa a haver um novo princípio que não se satisfaz apenas com a mera adoção de medidas de contenção de danos. Devem ser prestadas contas a seu respeito, inclusive com um ônus argumentativo acerca da eficácia de tais medidas.

Tal princípio é relevante no contexto da aplicação de Inteligência Artificial, pois a todo momento, ou a requerimento, o operador deve demonstrar como os dados pessoais dos usuários estão sendo protegidos frente à exposição aos métodos e técnicas de Inteligência Artificial, bem como e respectivo tratamento de dados.

Tais princípios regem a maneira nas quais o tratamento de dados pessoais deve ser realizado, destacando ainda a questão principiológica da LGPD; bem como ressaltam o conceito de consentimento, que é uma das bases da proteção de dados pessoais não só no âmbito da IA, mas sim no âmbito geral de incidência da lei, conforme destaca Patricia Peck Pinheiro (2023, p. 39) "a linha mestra para o tratamento de dados pessoais é o consentimento pelo titular, que deve ser aplicado aos tratamentos de dados informados e estar vinculado às finalidades apresentadas". A presença na lei do termo consentimento é tão impactante que, inclusive é citado 35 vezes na LGPD. Bruno Bioni (2019, p. 135) ainda explica a relação entre os princípios da LGPD e o consentimento: "É uma carga principiológica que procura conformar, justamente, a ideia de que o titular dos dados pessoais deve ser empoderado com o controle de suas informações pessoais e, sobretudo, na sua autonomia da vontade"[18]. O consentimento abarca todos os princípios, portanto, exceto previsão legal, é imprescindível o consentimento para o tratamento dos dados do titular dos dados pessoais, ainda mais envolvendo tratamento de dados por meio de IA, a exemplo do *ChatGPT*.

2.2.OS LIMITES IMPOSTOS PELA LGPD À INTELIGÊNCIA ARTIFICIAL GENERATIVA

Os *chatbots* como o *ChatGPT*, que resultam da aplicação de métodos e técnicas de Inteligência Artificial Generativa, sofreram um estouro de popularidade no final de 2022 para início de 2023, atingindo, no caso do *ChatGPT*, a marca de 100 milhões de usuários ativos mensais em janeiro de 2023, apenas dois meses após o lançamento, tornando-se o aplicativo com crescimento mais rápido da história (FORBES, 2023). Em acessos totais da atualidade os números do *ChatGPT* são ainda mais expressivos, com 2,4 bilhões de acessos à IA em janeiro de 2024, um crescimento de 178,10% comparado ao mesmo mês do ano antecedente, sendo os acessos de brasileiros correspondendo a 5,16% deste tráfego mundial do *ChatGPT* (FREITAS, 2024). Tais dados mostram que tais ferramentas baseadas em Inteligência Artificial Generativa, como o *ChatGPT*, estão crescendo no mercado, não só mundial mas também brasileiro.

A tendência do mercado de ferramentas baseadas em Inteligência Artificial é só aumentar, tendo como principal ponto de ascensão de popularidade o *ChatGPT* com seu rápido crescimento. Nesta seara, é imprescindível que haja exigências por estabelecer

adequações ao *ChatGPT* e outras ferramentas de Inteligência Artificial que estão emergindo neste mercado.

O vazamento e tratamento irregular de dados pessoais e sensíveis pelo controlador do *ChatGPT* pode vir a ser catastrófico, de modo a violar o princípio da privacidade e as normas estabelecidas pela LGPD. Verifica-se, por exemplo, que tais veículos de comunicações supracitados obtiveram certas informações dos usuários, como o sexo, idade e nacionalidade dos mesmos, deixando claro que há o acesso de dados pessoais dos usuários do referido *chatbot*, neste caso, inclusive, sem o consentimento específico para tal fim. O vazamento de dados pessoais sensíveis de usuários pode acarretar danos imensuráveis aos usuários. Diante deste contexto, é necessário que sejam impostos limites, visando a preservação dos dados pessoais dos titulares usuários do serviço, devendo tais limites observar a LGPD, bem como outros regramentos brasileiros, a exemplo do Marco Civil da Internet, do Código de Defesa do Consumidor e da Lei de Acesso à Informação.

Cumpre destacar novamente o princípio da finalidade, pelo qual o *chatbot* deve comunicar e solicitar autorização para tratamento dos dados pessoais de seus usuários que, caso não seja cumprido, a *OpenAI* empresa criadora do *ChatGPT*, a título exemplificativo, pode ser penalizada pela violação da LGPD. Além disso, deve-se atentar nestes casos ao princípio da segurança, no qual, conforme conceituado por Danilo Doneda (2011, p. 91-108), "os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado". Em vista disso, é necessário que as empresas responsáveis pelos *chatbots* implementem medidas de segurança suficientemente e adequadamente seguras para proteger os dados pessoais, a fim de evitar vazamentos de dados. Além disso, é destacado na seção 2 da Política de Privacidade da *OpenAI* (2023) que há a coleta e utilização de dados inseridos no *ChatGPT*, que são utilizados como meio de realizar melhorias nos serviços providos pela mesma, bem como no algoritmo da IA Generativa, podendo tais dados serem utilizados como resposta do *chatbot* para terceiros, ocorrendo assim uma gravíssima violação de dados pessoais. Philipe Monteiro Cardoso (2023), exemplifica a utilização de dados pessoais como resposta para terceiros:

> (...) podemos pedir para a inteligência artificial estruturar uma lista de e-mails, com isso ao fornecer estes e-mails, estamos compartilhando os dados que tivemos acesso com a base de dados da *OpenAI*, e consequentemente estes dados podem ser utilizados como resposta para terceiros.

Em relação aos dados sensíveis, verifica-se que a *OpenAI*, ainda em sua Política de Privacidade no tópico "Informações agregadas ou desidentificadas" da Seção 2 (OPENAI, 2023), busca impedir que seu *chatbot* utilize dados pessoais sensíveis como identificações pessoais, em razão de sua natureza privada, "desidentificando" e anonimizando dados pessoais dos usuários. Entretanto, ao acaso do usuário inserir dados sensíveis, ele não possui cognição para entender a situação e filtrar tais dados, podendo não diferenciar uma informação sensível de uma não sensível, assim em tese processar e utilizar dados sensíveis em respostas para terceiros, violando gravemente a privacidade do titular do dado utilizado (FERREIRA, 2023).

Conforme é possível verificar, a existência de mecanismos como a "desidentificação" e anonimização dos dados dos usuários demonstram que há muitas limitações impostas ao *ChatGPT*, não somente pela legislação brasileira de proteção de dados pessoais, mas por muitas legislações protetivas ao redor do mundo que tutelam os dados dos usuários do *chatbot*. Entretanto, é necessário atentar com falhas e vulnerabilidade no sistema da *OpenAI*, que podem prejudicar os usuários ao inserirem dados pessoais, sendo eles não sensíveis e, na pior das hipóteses, dados sensíveis, questões as quais estão tratadas adiante no texto.

3. A RESPONSABILIDADE DO CONTROLADOR NO TRATAMENTO DE DADOS ARMAZENADOS PELO CHATGPT

Este item trata os aspectos da responsabilidade do controlador conforme definido na LGPD, prevista na Seção III do Capítulo VI da lei na qual se intitula "Da Responsabilidade e do Ressarcimento de Danos", bem como aspectos relevantes como a método utilizado pelo *ChatGPT* para tratamento de dados dos usuários e sua compatibilidade com os princípios e fundamentos já elencados no item anterior. Além destas questões, outro ponto que merece destaque é o consentimento do usuário frente à coleta e armazenamento de dados pelo *chatbot*, tanto para adultos como o consentimento específico para crianças e adolescentes.

3.1. A CAPTURA DE DADOS E O MÉTODO UTILIZADO PELO CHATGPT

O tratamento de dados realizado no *ChatGPT* pela empresa desenvolvedora *OpenAI* está previsto em sua Política de Privacidade, estabelecendo um método no qual a plataforma coleta, armazena e, por fim, elimina os dados dos usuários de seu sistema.

Primeiramente, a Política de Privacidade estabelece, em sua Seção 1 (OPENAI, 2023), os dados pessoais que são coletados pela plataforma, sendo estes: I) informações associadas à conta, como nome, informações de contato, credenciais da conta, informações do cartão de pagamento e histórico de transações; II) conteúdo do usuário, como dados incluídos nas contribuições realizadas *chatbot*, *uploads* de arquivos ou *feedback* fornecidos pelo usuário ao *chatbot*; III) informações do usuário que entrar em contato com a *OpenAI* e quaisquer informações providenciadas pelos usuários à desenvolvedora, e IV) informações de mídia social quando o usuário entra em contato com qualquer uma das redes sociais da *OpenAI*, coletando, a exemplo, dados de contato. Além destes dados, ainda se prevê na mesma seção da Política de Privacidade a coleta de outros dados que são recebidos automaticamente pelo uso do *ChatGPT* como: a) dados de registro e de uso, como informações acerca do navegador, localização ou até fuso horário do usuário; b) dados do dispositivo como nome e sistema operacional, além dos cookies, os quais são conceituados pela própria Política de Privacidade (OPENAI, 2023): "um "*cookie*" é um pedaço de informação enviada ao seu navegador por um site que você visita".

Conforme se verifica, há uma coleta enorme de dados durante o uso do *ChatGPT*, coletando desde a informações como nome e informações de pagamento à geolocalização e fuso horário dos usuários. Esta coleta de dados em conjunto com a alta quantidade de usuários, como já apresentado no item anterior, cria uma ampla base de dados. Verifica-se que esta captura e armazenamento de dados podem possivelmente violar o princípio da necessidade, visto que há uma excessiva coleta de dados, ultrapassando o mínimo necessário para a finalidade afirmada na Política de Privacidade na Seção 2, tanto que a coleta excessiva dos dados dos usuários foi o motivo do bloqueio e proibição que ocorreu na Itália, temática que será tratada posteriormente.

Ainda, mesmo com esta coleta excessiva, não há, de modo detalhado, a devida prestação de contas em relação aos dados armazenados na base de dados da *OpenAI*, sendo que os usuários do serviço permanecem em um limbo a partir do como seus dados são utilizados, sendo o rol listado na Seção 2 da Política de Privacidade (OPENAI, 2023) muito aberto em comparação a quantidade de dados coletada. A ausência de transparência

e prestação de contas em relação à quantidade de dados coletados e armazenados é preocupante, ainda mais quando é possível que dados capturados possam ser dados pessoais sensíveis.

Além de todas estas questões, verifica-se novamente uma possível violação aos princípios da necessidade e finalidade da LGPD, na medida que a Política de Privacidade, na Seção 8 denominada "Segurança e Detenção", não estabelece o tempo pelo qual os dados dos usuários permanecerão na base de dados da *OpenAI*, havendo a possibilidade de manutenção dos dados além da finalidade proposta pela *OpenAI* causando uma violação a tais princípios.

Apesar destas questões, a Seção 4 da Política de Privacidade, intitulada "Seus direitos", dispõe ao usuário - titular de dados - uma listagem de direitos trazidos pelas diversas legislações de proteção de dados ao redor do mundo, incluindo o GDPR e, consequentemente, a LGPD, apesar de não ser citada expressamente na Política de Privacidade. É disposto que são direitos dos usuários o acesso às suas informações e a forma de processamento das mesmas, a exclusão de suas informações dos registros da *OpenAI*, ratificar ou atualizar informações pessoais, transferência de informações pessoais à terceiros, restringir o processamento de seus dados, retirar seu consentimento para qualquer tratamento de seus dados, se opor ao modo no qual são processadas suas informações e, por fim, realizar uma reclamação formal junto à autoridade local de proteção de dados, no caso do Brasil, a Agência Nacional de Proteção de Dados (ANPD). Tais direitos trazidos pela Política de Privacidade da *OpenAI* estão de acordo com os direitos apresentados pela LGPD em seu art. 7º. Apesar de não constar todos os direitos previstos na LGPD, o rol trazido é exemplificativo, conforme dita a própria Política de Privacidade (OPENAI, 2023) "Dependendo do local, os indivíduos podem ter certos direitos estatutários em relação às suas Informações Pessoais. Por exemplo, você pode ter o direito de (...)", assim, a política deixa em aberto os direitos dos usuários aplicáveis ao *ChatGPT* para que haja a aplicação dos direitos do titular diante de qualquer legislação de proteção de dados do mundo, independente da rigidez da mesma. Além disso, estão também de acordo com os fundamentos e princípios trazidos pela LGPD, visto que muitos desses direitos condizem com o conceito de vários princípios como, a exemplo, o princípio da qualidade dos dados, na qual a *OpenAI* se dispõe a ratificar e atualizar informação pessoais, ou até o princípio da transparência, na medida que dispõe o acesso às informações dos usuários, bem como a forma de processamento das mesmas.

O discurso de violação dos princípios da LGPD pelo *ChatGPT* está direcionado, na verdade, à algumas questões mais específicas como, por exemplo, a exagerada coleta de dados frente à tamanha quantidade de usuários, não especificando quais destes dados são coletados e qual sua finalidade de modo mais específico, ainda mais se tratando de uma possível coleta de dados pessoais sensíveis, a qual necessita de uma política mais rigorosa por parte da *OpenAI*.

3.2.PREOCUPAÇÕES COM O CONSENTIMENTO DO USUÁRIO

O consentimento, conforme definido pela própria LGPD por meio de seu Art. 5º, XII (BRASIL, 2018), trata da "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada", e se apresenta como um dos conceitos basilares da proteção de dados pessoais. Laura Schertel Mendes e Danilo Doneda (2018, p.469-483) definem os requisitos para a validade do consentimento:

> Os requisitos para que um consentimento seja considerado válido pela Lei estão previstos já na sua definição (art. 5º, XII), segundo o qual o consentimento deve ser livre, informado, inequívoco e com uma finalidade determinada. Em caso de tratamento de dados sensíveis, o consentimento deve ser ainda fornecido ainda de forma específica e destacada, nos termos do art. 11, I, da LGPD. Caso o consentimento seja formulado de forma genérica ou a partir de informações enganosas prestadas ao titular, o consentimento será nulo, conforme determinam respectivamente os arts. 8º, §§ 4º e 9º, § 1º da Lei.

Conforme ainda é destacado, o tratamento de dados sensíveis ainda traz uma camada extra de requisitos em razão da natureza dos dados para os quais está sendo dado consentimento. Os dados sensíveis, nas palavras da própria LGPD, por meio de seu art. 5º, II (BRASIL, 2018), trata do "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Conforme se verifica, estes dados são dados que demandam maior proteção pela sua natureza mais privada, necessitando de um consentimento específico e destacado para ser válido. A questão dos dados sensíveis é pouco tratada na Política de Privacidade da *OpenAI*, devendo esta conter uma cláusula destacada e solicitar o consentimento específico, o que aparentemente não é realizado,

somente afirmando (OPENAI, 2023) "também não tratamos Informações Pessoais sensíveis com o objetivo de inferir características sobre um consumidor".

Outra questão que possui grande relevância é o modo como o consentimento é manifestado por parte do titular, podendo este ser escrito ou outro meio no qual se demonstre a vontade livre e consciente do titular, devendo refletir na verdadeira vontade e escolha do titular. No caso de o consentimento ser escrito, ele deverá ser uma cláusula destacada das demais cláusulas. Ainda, tal consentimento deve observar uma finalidade determinada, conforme o próprio princípio da finalidade, não podendo tal consentimento ser utilizado para uma finalidade diversa de tratamento de dados que não foi expressamente consentida. Ainda, destaca Débora Sirotheau (2022) sobre o tratamento de dados além do consentimento:

> Insta mencionar que o consentimento não legitima o tratamento de dados desnecessários, bem como não afasta as demais disposições previstas na LGPD como, por exemplo, a adoção, pelo agente de tratamento, de medidas técnicas e administrativas aptas a proteger os dados pessoais.

Por outro lado, é possível que, caso o consentimento seja realizado de forma genérica ou até seja formulado com base em informações enganosas, o mesmo será considerado nulo. Diante disso, os requisitos presentes na LGPD são essenciais para que o consentimento seja válido, inclusive sob pena de responsabilização do controlador. Além disso, o instituto dos vícios de consentimento do direito civil se aplica à LGPD, na medida que qualquer vício presente no ato do consentimento invalida o ato, não podendo o titular, a exemplo, ser coagido a dar consentimento para o tratamento de seus dados (art. 138 a 165 do Código Civil [BRASIL, 2002]), sendo, nestes casos, anulável o consentimento (art. 171, II, do Código Civil [BRASIL, 2002]), conforme destaca Débora Sirotheau (2022) "caso o titular de dados possua apenas um controle ilusório de seus dados, estaremos diante de um vício de consentimento e, consequentemente, de uma ilicitude no tratamento de dados pessoais".

O consentimento é indispensável para que se autorize o tratamento dos dados dos usuários do *ChatGPT*, sendo este adquirido quando se cria uma conta e determina a necessidade de aceitação dos Termos de Uso e Política de Privacidade para uso do serviço. Além disso, em qualquer momento, conforme devidamente elucidado na Política de Privacidade (OPENAI, 2023), é possível retirar o consentimento do tratamento de dados a qualquer momento, conforme Seção 4 da Política de Privacidade.

Ademais, é necessário também discutir sobre o consentimento frente à coleta de dados de crianças e, principalmente, adolescentes. Apesar do *ChatGPT* não permitir usuários abaixo de 13 anos, conforme será elucidado e aprofundado no item 4 deste artigo, o *chatbot* ainda permite que adolescentes acima de 13 anos completos utilizem de sua plataforma. Entretanto, conforme estabelece o art. 14, § 1º, da LGPD (BRASIL, 2018), "O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal", ou seja, é possível verificar a ausência de tal adequação à legislação brasileira de proteção de dados, visto que tal consentimento específico e em destaque, em nenhum momento, é solicitado, podendo qualquer adolescente acessar o *ChatGPT*, podendo, conforme será visto no subtópico seguinte, responsabilização pela ausência de consentimento específico, conforme prevê a LGPD.

O consentimento é um aspecto essencial para o tratamento de dados, devendo este ser por qualquer meio que exprima a vontade livre e consciente do titular, ausente de vícios de consentimento, sendo que, por meio escrito deve ser por meio de cláusula com destaque entre as demais cláusulas, devendo possuir uma finalidade determinada, além de não poder ser genérica ou por meio de informações enganosas, sob pena de nulidade do consentimento e, além disso, uma possível responsabilização do controlador.

3.3.A RESPONSABILIDADE DO CONTROLADOR FRENTE AOS DADOS PESSOAIS E SENSÍVEIS OBTIDOS E ARMAZENADOS PELA EMPRESA CONTROLADORA DA IA

A responsabilidade civil do controlador de dados se manifesta quando há alguma violação às normas e princípios estabelecidos não só na LGPD mas no microssistema da legislação de proteção de dados, sendo a LGPD sua base estrutural nos dias atuais. Walter Capanema (2020) destaca a analogia que deve ser feita à conceituação de "legislação tributária" do art. 96 do CTN, inserindo não só a LGPD, mas também outras legislações como o Marco Civil da Internet, Código Civil, Código do Consumidor, bem como normas administrativas expedidas pela ANPD neste microssistema.

Além disso, é importante ressaltar que a mera violação deste microssistema de legislação de proteção de dados do art. 42, o art. 44, em seu parágrafo único, traz outra possibilidade de responsabilização, na medida que traz a responsabilização diante da

ausência de adoção de medidas de segurança conforme estabelece o art. 46 da LGPD, o qual traz a necessidade para agentes de segurança adorarem medidas protetivas.

Em regra, conforme definido pelo art. 42 da LGPD, ou o controlador ou o operador será responsabilizado civilmente por quaisquer danos patrimoniais, morais, individuais ou coletivos, sendo assim estabelecida uma alternância. Entretanto, há uma exceção à regra, quando o parágrafo 1º do artigo traz duas possibilidades de responsabilidade solidária, primeiramente caso o operador descumpra as obrigações da legislação de proteção de dados ou caso o mesmo não seguir as instruções lícitas dadas pelo controlador, ou caso o controlador estiver diretamente envolvido no tratamento que decorreu os danos ao titular do direito.

Além da solidariedade na responsabilização, a LGPD inova ao trazer um critério binário, estando presentes a responsabilidade objetiva e subjetiva em um mesmo ordenamento jurídico, ou seja, a legislação não prevê o elemento culpa, mas também não o excluí, não sendo exatamente clara em qual responsabilidade é aplicada ao caso, seja subjetiva ou objetiva.

Entretanto, Fernando Tasso (2020, p. 104) elenca os 02 (dois) critérios objetivos para a responsabilidade do controlador ou operador na LGPD "(...) requisito da obrigação de reparar a circunstância de ter sido a operação de tratamento lesiva realizada em violação à legislação de proteção de dados", sendo estes requisitos previstos no próprio texto de lei no art. 42 da LGPD. Além disso, em caso de relação de consumo, há o diálogo das fontes, na medida que há uma comunicação entre o direito do consumidor, por meio da responsabilidade objetiva prevista no CDC e a LGPD, por meio do art. 45 da LGPD, na qual prevê claramente a possibilidade de aplicação do CDC em caso de violação de direitos consumeristas. Fernando Tasso (2020, p. 113), por fim, conclui:

> (...) verifica-se que a Lei Geral de Proteção de Dados elegeu o sistema de responsabilidade civil subjetiva em perfeito alinhamento com o Código Civil, inserindo-se de forma harmoniosa no mosaico legislativo, o mesmo ocorrendo em relação ao Código de Defesa do Consumidor que, dado o tratamento Constitucional da defesa do consumidor, atrai para seu sistema de responsabilidade objetiva os fatos jurídicos dessa natureza.

O *ChatGPT*, inclusive pode ser considerado uma relação de consumo pois disponibiliza um serviço para o usuário, podendo neste caso ser aplicado não só a própria LGPD, mas também o Código de Defesa do Consumidor no sentido de responder objetivamente pelos danos causados, conforme prevê o art. 14 do CDC (BRASIL, 1990).

Ademais, tal aplicação do CDC incide sobre o serviço tanto gratuito como pago do *ChatGPT*, visto que é pacífico na jurisprudência, inclusive nos tribunais superiores (BRASIL, 2012), que serviços gratuitos na internet ainda constituem relação de consumo, em razão da obtenção de lucro se dar de forma indireta como, por exemplo, anúncios personalizados, sendo aplicável o CDC. Ademais, o usuário é tratado múltiplas vezes como um consumidor na Política de Privacidade e nos Termos de Uso dos serviços da *OpenAI*, utilizando termos como consumidor, para se referir ao usuário, e tratar o *ChatGPT* como serviço, reforçando este ponto, podendo assim ser objetivamente responsável.

Um possível vazamento de dados no *ChatGPT*, a exemplo, poderia ser catastrófico, visto que pode ser potencializado pela exploração criminosa dos dados vazados, podendo causar ainda mais danos, como por exemplo o vazamento de dados de *login* e senhas, como já ocorreu em inúmeros vazamentos de redes sociais (POZZEBOM, 2019). Neste caso, destaca-se ainda o art. 944 do Código Civil (BRASIL, 2002), que estabelece que "a indenização mede-se pela extensão do dano", agravando ainda mais a situação de um possível vazamento de dados, podendo alcançar inclusive danos na esfera moral.

A responsabilidade civil no microssistema da proteção de dados pessoais, com a legislação basilar na LGPD, traz um aspecto inovador ao instituto da responsabilidade civil visto que se apresenta como um critério binário de aplicação da responsabilidade, apresentando responsabilização objetiva e subjetiva no mesmo ordenamento, sendo a relação entre o controlador do *ChatGPT* e o usuário uma relação de consumo, podendo ser aplicada a responsabilidade objetiva em caso de dano patrimonial, moral, individual ou coletivo.

Ademais, destaca-se neste quesito as sanções administrativas advindas de uma possível responsabilização da *OpenAI*, estando estas previstas no art. 52 da LGPD (BRASIL, 2018) que se encontra no Capítulo VIII, Seção II "Das Sanções Administrativas", no qual enumera várias penalidades, entretanto, a que mais se destaca é a do inciso II, na qual determina que caso haja qualquer infração às normas previstas na LGPD acarretará na "multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais)

por infração". Tal sanção destaca a importância da proteção de dados no Brasil, reforçando seu status de interesse nacional perante a sociedade.

Apesar do *ChatGPT* estar adequado a grande parte das legislações de proteção de dados em muitos aspectos anteriormente elencados, já houve e ainda há muitas brechas que acabam violando fundamentos, princípios e direitos presentes nas legislações protetivas de dados, o que pode acionar os órgãos e agências reguladoras de muitos países, como o bloqueio do *ChatGPT* na Itália e a suspensão da *Meta AI* no Brasil.

4. O BLOQUEIO DO CHATGPT E OUTRAS IAS E O FUTURO

Por fim, este capítulo trata sobre o bloqueio temporário do *ChatGPT* na Itália realizado pelo órgão regulador italiano e seus fundamentos apresentados para tal decisão bem como as nuances da suspensão da *Meta AI* no Brasil, impedindo que os *chatbots* fossem utilizados em seus em seus respectivos territórios. Ademais, são discutidas as expectativas em relação à adequação do *ChatGPT* à LGPD no futuro, estabelecendo novas regras à proteção e tratamento de dados pelo uso da Inteligência Artificial Generativa.

4.1. FUNDAMENTOS PARA O BLOQUEIO DO CHATGPT NA ITÁLIA E A ATUAÇÃO DA ANPD NA SUSPENSÃO DA META AI NO BRASIL

Em 31 de março de 2023, a autoridade de proteção de dados pessoais italiana, a "*Garante per la Protezione dei Dati Personali*", bloqueou provisoriamente o *ChatGPT* em território italiano em razão de violação à legislação vigente de proteção de dados, o Regulamento Geral de Proteção de Dados Pessoais europeu (RGPD) (INTELLIGENZA ARTIFICIALE, 2023), abrindo uma investigação e determinando que houvesse a imediata pausa na coleta e tratamento de dados no país. A autoridade italiana alegou estar preocupada com o tratamento de dados realizada pela *OpenAI* em seu *chatbot,* tendo a decisão se fundamentado em duas justificativas: (i) possível coleta excessiva de dados desnecessários e sem finalidade específica, tratando-se de uma coleta ilegal de dados e (ii) o risco da coleta de dados de crianças menores de 13 anos.

Primeiramente, conforme já tratado anteriormente, a excessiva coleta de dados realizada pelo *ChatGPT* é uma preocupação real, tanto que foi um dos motivos do

bloqueio pela autoridade italiana. A questão dos princípios da proteção de dados, bem como os direitos do titular de dados vieram à tona por meio do RGPD. Os princípios presentes no RGPD são muito similares aos princípios da LGPD brasileira, tendo a legislação europeia os seguintes princípios, conforme prevê o art. 5º da mesma (UNIÃO EUROPEIA, 2016): licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade. Neste sentido, haveria clara violação ao princípio da transparência, finalidade e minimização de dados, visto que a excessiva coleta de dados, sem a devida transparência em relação à finalidade desta massiva coleta e tratamento de dados, além da minimização dos dados que se resume pela própria excessiva coleta de dados, contrariando completamente o princípio.

Voltando um pouco à LGPD, é possível verificar que a legislação brasileira possui um número maior de princípios, isso acontece visto que a LGPD é, de certo modo, "espelho" da legislação europeia, entretanto, foi adaptada à realidade brasileira. Ademais, a similaridade entre ambas se dá também em razão da necessidade de reconhecimento da legislação brasileira pela União Europeia, conforme explica Oliveira (2022, p. 89):

> (...) desde a concepção do projeto de lei que culminou no texto sancionado da LGPD, muito já se falava na notória influência do RGPD sobre a estrutura da norma brasileira, com a qual conserva o modelo regulatório e a identidade de diversas premissas, fundamentos e regras. Aliás, tal convergência entre ambas as normas era inclusive desejada pelo legislador pátrio, uma vez que a paridade do regime protetivo proporcionado pela LGPD com aquele já proposto pelo RGPD é essencial para que a lei brasileira venha a ter sua idoneidade reconhecida pelo bloco europeu, o que facilitará o fluxo informacional e o transacionamento de dados pessoais entre Brasil e Europa.

Outro fundamento trazido pela decisão que bloqueou o *ChatGPT* na Itália é a questão do tratamento de dados de crianças menores de 13 anos, na medida que, de acordo com os Termos de Uso da *OpenAI* (2023), pela sua seção 1 "Registro e Acesso", o usuário deve possuir pelo menos 13 anos para utilizar o serviço. Apesar de constar tal informação nos Termos de Uso, previamente o *ChatGPT* não possuía nenhum tipo de verificação de idade para impedir o acesso de menores de 13 anos no serviço. Tanto o RGPD como a LGPD trazem um consentimento específico para crianças e adolescentes, tendo pelo lado do RGPD uma idade pré-definida para tal, conforme estabelece o art. 8º do RGPD (UNIÃO EUROPEIA, 2016), que define que "caso a criança tenha menos de 16 anos, o tratamento só é lícito se e na medida em que o consentimento seja dado ou autorizado

pelos titulares das responsabilidades parentais da criança". Ainda, o mesmo artigo traz que os Estados-Membros podem flexibilizar tal idade para até, no mínimo, 13 anos. Este consentimento consiste na autorização parental ou do responsável legal para que seja possível o tratamento de dados. Já na LGPD, o tratamento de dados de crianças e adolescentes é tratado em seu artigo 14, utilizando-se do conceito de criança e adolescente utilizado no Estatuto da Criança e do Adolescente (ECA) por meio de seu artigo 2º (BRASIL, 1990), sendo criança a pessoa com até 12 anos incompletos e o adolescente entre 12 e 16 anos, verificando-se novamente a similaridade prática entre as duas legislações.

Tal bloqueio, por mais que provisório, trouxe mudanças significativas em algumas práticas realizadas pela *OpenAI*. A partir deste, ao criar uma conta no *ChatGPT*, há um verificador de idade, necessitando inserir a data de nascimento do usuário, entretanto, é demonstrada a fragilidade de tal mecanismo na medida que o mesmo pode ser facilmente burlado por meio inserção de uma data de nascimento falsa, sem qualquer verificação posterior. A partir desta análise, é possível verificar que nada mudou na prática, pois o verificador de idade pode ser facilmente burlado, não sendo um mecanismo realmente efetivo. Além desta medida, foram incluídas novas informações na Política de Privacidade da *OpenAI* (2023) em relação ao tratamento de dados em todos os aspectos, incluindo a de dados pessoais de crianças e adolescentes, por meio da seção 6 "Crianças", bem como informações mais precisas frente à coleta e tratamento de dados para o fim de melhorias nos serviços da *OpenAI* como o *ChatGPT*. Estas mudanças resultaram no posterior desbloqueio do *chatbot* na Itália, tendo a *OpenAI* se adaptado à legislação de proteção de dados, não só europeia, mas também dos Estados Unidos e entre outras como a própria LGPD.

Além do bloqueio realizado na Itália, outra notícia que ganhou especial atenção em relação à temática, em especial no território brasileiro, é a suspensão da Política de Privacidade e dos Termos de Uso da *Meta* pela ANPD e da consequente suspensão dos recursos da *Meta AI* no Brasil. Como no caso da Itália, houve um contexto por trás do bloqueio, se iniciando com a empresa *Meta* alterando seus Termos de Uso e Política de Privacidade para utilizar dados públicos de usuários como publicações de texto e imagens presentes em suas redes sociais como Facebook e Instagram para treinar sua IA Generativa, conhecida como *Meta AI* (G1, 2024). Desta maneira, diversas autoridades tanto brasileiras como europeias questionaram tal previsão, tendo no Brasil alertado a

ANPD sobre possíveis violações expressas à LGPD (G1, 2024), como a falta de transparência e, similarmente ao caso da Itália, o tratamento de dados pessoais de crianças e adolescentes sem as devidas precauções legais. Desta maneira, a Agência Nacional de Proteção de Dados (2024) proferiu uma medida preventiva, suspendendo a nova política de privacidade da empresa para, nas palavras da autarquia, "evitar dano grave e irreparável ou de difícil reparação". Tal suspensão pela autarquia federal fez com que a Meta deixasse de lançar oficialmente sua IA e suspendesse seus recursos no país. Mediante a apresentação de um Plano de Conformidade pela *Meta*, a ANPD (2024) proferiu decisão suspendendo a proibição imposta à empresa de usar dados pessoais para treinar sua inteligência artificial. Desta maneira, a partir de 30/08/2024, data a qual foi proferida a referida decisão, a *Meta* está autorizada a coletar dados para treinamento de sua IA, entretanto com ressalvas, demonstrando novamente a importância das agências reguladoras para a correta adequação dos termos de uso e políticas de privacidade dos *chatbots* à LGPD.

4.2.O QUE ESPERAR DO CHATGPT EM TERMOS DE ADEQUAÇÃO À LGPD

Frente à estes bloqueios no Brasil e na Itália, verifica-se que Inteligências Artificiais Generativas devem ser sempre fiscalizadas pelas autoridades de proteção de dados como foi feito pela autoridade italiana e brasileira. Não somente na fiscalização, mas também no incremento de medidas de segurança como a inclusão de um verificador de idade e outros meios efetivos para controle das faixas etárias que acessam o serviço, em razão da não efetividade do atual modelo de verificação utilizado pelo *ChatGPT*, bem como medidas protetivas para impedir vazamentos de dados armazenados pela *OpenAI*. Tais medidas devem sempre ser implementadas a estes *softwares*, adequando cada vez mais não somente o *ChatGPT*, mas outras IAs Generativas como *Microsoft Copilot*, *Google Gemini*, *Meta AI*, entre outras, às legislações de proteção de dados ao redor do mundo como o RGPD, no caso da Europa, e a LGPD, no caso do Brasil.

É possível verificar que em nenhum momento a Política de Privacidade da *OpenAI* trata da legislação brasileira. Isso se dá pelo fato de o *ChatGPT* ainda não ser completamente implementado no Brasil, tanto que a própria plataforma da IA, bem como seus termos e Política de Privacidade somente recentemente foram traduzidos ao Português do Brasil.

Há que se ponderar pela adequação por meio da localização e regionalização do *ChatGPT* e as plataformas da *OpenAI* ao Brasil, com o intuito de dar melhor acesso aos usuários não só ao *chatbot* em si, mas também aos termos e Política de Privacidade da *OpenAI*. Em continuidade, apesar da similaridade entre o RGPD e a LGPD, a *OpenAI* deve adaptar sua Política de Privacidade à LGPD, visto que há diferenças estruturais entre a Europa e o Brasil, como por exemplo o maior número de princípios presentes na LGPD.

Portanto, o bloqueio do *ChatGPT* na Itália e as medidas implementadas no mesmo pela *OpenAI* trouxeram uma nova perspectiva de adequação dos *chatbots* de IAs Generativas às leis de proteção de dados pelo mundo, inserindo a tutela de proteção de dados dos seus usuários como prioridade, gerando uma crescente implementação de novas medidas para o tratamento de dados conforme as leis de proteção de dados, não somente da LGPD mas de muitas outras legislações neste tema ao redor do mundo.

5. CONCLUSÃO

O artigo aprofundou a temática da legislação de proteção de dados pessoais aplicada às Inteligências Artificiais Generativas, mais especificamente o *ChatGPT* como parâmetro principal, em razão da excessiva coleta de dados pelo *chatbot*, o que desencadeou uma grande preocupação em relação ao consentimento e o tratamento legal de dados dos usuários do serviço. Assim, foi realizado uma análise de conceitos, princípios e fundamentos da LGPD e como o *chatbot* da *OpenAI* já foi e pode, futuramente, ser adequado a esta legislação. Ademais, foram discutidas as consequências desta violação, por meio da responsabilidade em casos de violação dos princípios presentes na LGPD, por fim, refletindo sobre o recente caso do bloqueio do *ChatGPT* na Itália em razão da violação de regulamentos de proteção de dados europeia, bem como possíveis inovações na adequação do *chatbot* à legislação de proteção de dados pessoais, não só brasileira, mas também do RGPD e outras legislações ao redor do mundo.

Verificou-se que o *ChatGPT* já possui uma Política de Privacidade adaptada à legislação de proteção de dados europeia, mas que, por mais que haja similaridade com a LGPD, a referida Política e os Termos de Uso podem ser melhorados para atender aos interesses dos usuários frente à coleta de dados pessoais como, por exemplo, realizar melhorias no sistema verificador de idade, o qual se demonstra pouco eficaz, ou um maior aprofundamento na finalidade e transparência sobre os dados coletados pelo *ChatGPT*.

Sendo assim, entende-se que a adequação do *ChatGPT* à LGPD já foi realizada de modo parcial, em razão da similaridade entre as legislações brasileira e europeia. Entretanto, deve haver uma adequação específica à LGPD, bem como uma regionalização do produto ao Brasil, de acordo com o CDC e outras legislações brasileiras. Um exemplo, é adequar às exigências do Estatuto da Criança e Adolescente – ECA, de modo a incluir um método no qual seria possível haver um consentimento específico para adolescentes até 13 anos, idade mínima para utilizar o *ChatGPT*, e 18 anos para uso dos serviços, visto que tais questões ainda não foram adequadas ao Brasil na Política de Privacidade e nos Termos de Uso da *OpenAI*.

Portanto, entende-se por alcançado o objetivo geral do artigo em analisar a adequação realizada pelo *ChatGPT* em relação às normas e exigências da LGPD, em razão das preocupações atuais de proteção aos dados pessoais da sociedade informacional e novas tecnologias como as IAs Generativas.

Para futuras pesquisas, será necessário acompanhar atentamente as adequações realizadas não só pela *OpenAI* mas pelas demais empresas que desenvolvem sistemas de IA Generativa, analisando possíveis brechas e melhorias a serem implementadas nestes sistemas visando sempre a proteção dos dados pessoais dos usuários. A temática tratada é muito importante visto que o mercado de aplicações de IA Generativa ainda tem muito a crescer e a adequação à LGPD é de suma importância para a conciliação entre privacidade e proteção de dados pessoais de titulares, sem deixar de lado a evolução da Inteligência Artificial Generativa.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. **Despacho Decisório nº 33/2024/PR/ANPD**. Conselho Diretor. Relatora: Arthur Pereira Sabbat, 30 Ago. 2024. Disponível em: https://www.in.gov.br/en/web/dou/-/despacho-decisorio-n-33/2024/pr/anpd-581192714. Acesso em: 03 set. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. **VOTO Nº 11/2024/DIR-MW/CD**. Conselho Diretor. Relatora: Miriam Wimmer, 01 Jul. 2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-determina-suspensao-cautelar-do-tratamento-de-dados-pessoais-para-treinamento-da-ia-da-meta/SEI_0130047_Voto_11.pdf. Acesso em: 26 ago. 2024.

BARROSO, Luís Roberto. Neoconstitucionalismo e constitucionalização do Direito (o triunfo tardio do direito constitucional no Brasil). *In*: **Revista de Direito Administrativo**. Rio de Janeiro, n. 240, abr./jun. 2005.

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

BIONI, Bruno Ricardo. **Regulação e Proteção de Dados Pessoais**: O Princípio da Accountability. Rio de Janeiro: Editora Forense, 2022.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Diário Oficial da República Federativa do Brasil. Brasília, DF: Presidência da República, 05 out. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 10 ago. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002**. Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 10 ago. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 ago. 2024.

BRASIL**. Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Diário Oficial da União, Brasília, DF, 14 jul. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 10 ago. 2024.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial, REsp 1316921/RJ 2011/0307909-6**. Terceira Turma. Relator: Ministra Nancy Andrighi. Julgamento: 26/06/2012. Disponível em: https://processo.stj.jus.br/SCON/GetInteiroTeorDoAcordao?num_registro=201103079096&dt_publicacao=29/06/2012. Acesso em: 10 ago. 2024.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 165, jan./mar. 2020. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/142288. Acesso em: 01 out. 2023. (Qualis B4)

CARDOSO, Philipe Monteiro. LGPD vs. inteligência artificial: A proteção dos dados pessoais em tempos de chatbots avançados. **Revista Jus Navigandi**, ISSN 1518-4862, Teresina, ano 28, n. 7173, 20 fev. 2023. Disponível em: https://jus.com.br/artigos/102545/lgpd-vs-inteligencia-artificial-a-protecao-dos-dados-pessoais-em-tempos-de-chatbots-avancados. Acesso em: 10 ago. 2024.

CUEVA, Ricardo Villas Bôas. A insuficiente proteção de dados pessoais no Brasil. **Revista de Direito Civil Contemporâneo**. vol. 13. ano 4. p. 59-67. São Paulo: Ed. RT, out./dez. 2017.

DONEDA, Danilo. **A Proteção dos Dados Pessoais como um Direito Fundamental**. Joaçaba, v. 12, n. 2, p. 91-108, jul./dez. 2011.

DONEDA, Danilo. **Panorama histórico da Proteção de Dados Pessoais**. *In*: DONEDA, Danilo *et al*. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

FERREIRA, Márcia. Impactos do uso do ChatGPT na perspectiva da LGPD. **Revista Consultor Jurídico**, 24 jun. 2023. Disponível em: https://www.conjur.com.br/2023-jun-24/marcia-ferreira-uso-chatgpt-perspectiva-lgpd. Acesso em: 10 ago. 2024.

FORBES. ChatGPT tem recorde de crescimento da base de usuários. **FORBES,** 01 fev. 2023. Disponível em: https://forbes.com.br/forbes-tech/2023/02/chatgpt-tem-recorde-de-crescimento-da-base-de-usuarios/. Acesso em: 10 ago. 2024.

FREITAS, Felipe. Brasil é o quarto país que mais acessa o ChatGPT. **Tecnoblog**, 26 mar. 2024. Disponível em: https://tecnoblog.net/noticias/brasil-e-o-quarto-pais-que-mais-acessa-o-chatgpt/. Acesso em: 24 ago. 2024.

G1. Entenda o que a Meta diz sobre a coleta de informações de usuários para treinar IA e saiba passo a passo para desativar. **O Globo,** 23 jun. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/06/23/entenda-o-que-a-meta-diz-sobre-a-coleta-de-informacoes-de-usuarios-para-treinar-ia-e-saiba-passo-a-passo-para-evitar.ghtml. Acesso em: 26 ago. 2024.

G1. Meta diz que suspendeu recursos de inteligência artificial generativa no Brasil. **O Globo,** 17 jul. 2024. Disponível em: https://g1.globo.com/tecnologia/noticia/2024/07/17/meta-diz-que-suspendeu-recursos-de-inteligencia-artificial-generativa-no-brasil.ghtml. Acesso em: 26 ago. 2024.

INTELLIGENZA ARTIFICIALE. **il Garante blocca ChatGPT**. Raccolta illecita di dati personali. Assenza di sistemi per la verifica dell'età dei minori. Garante per la Protezione dei Dati Personali. 31 mar. 2023. Disponível em: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9870847#english. Acesso em: 10 ago. 2024.

LIMA, Cíntia Rosa pereira de. **Autoridade Nacional de Proteção de Dados e a Efetividade da Lei Geral de Proteção de Dados: de acordo com a Lei Geral de Proteção de Dados (Lei n. 13.709/2018 e as alterações da Lei n. 13.853/2019), o Marco Civil da Internet (Lei 12.965/2014) e as sugestões de alteração do CDC (PL 3.514/2015).** São Paulo: Almedina, 2020.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova Lei Geral de Proteção de Dados. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 469-483, nov./dez. 2018.

OLIVEIRA, Dânton Hilário Zanetti de. **Big Data e a Lei Geral de Proteção de Dados Pessoais**. Rio de Janeiro: Editora Lumen Juris, 2022.

OPENAI. Política de Privacidade. **OpenAI OpCo**, LLC. 14 nov. 2023. Disponível em: https://openai.com/pt-BR/policies/privacy-policy/. Acesso em: 24 ago. 2024.

OPENAI. Termos de Uso. **OpenAI OpCo**, LLC. 14 nov. 2023. Disponível em: https://openai.com/pt-BR/policies/terms-of-use/. Acesso em: 24 ago. 2024.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 4 ed. São Paulo: Saraiva Jur, 2023.

POZZEBOM, Rafaela. Arquivo com 2,2 bilhões de logins e senhas vaza na internet. **Oficina da Net**. 5 fev. 2019. Disponível em: https://www.oficinadanet.com.br/seguranca/24780-arquivo-com-22-bilhoes-de-logins-e-senhas-vaza-na-internet. Acesso em: 10 ago. 2024.

SIROTHEAU, Débora. O consentimento na LGPD. **Revista Consultor Jurídico**, 21 mai. 2022. Disponível em: https://www.conjur.com.br/2022-mai-21/debora-sirotheau-consentimento-lgpd. Acesso em: 10 ago. 2024.

TASSO, Fernando Antônio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. **Cadernos Jurídicos**, São Paulo, v. 21, n. 53, p. 104, jan./mar. 2020. Disponível em: https://bdjur.stj.jus.br/jspui/handle/2011/142293. Acesso em: 10 ago. 2024. (Qualis B4)

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Jornal Oficial da União Europeia, Bruxelas, 4 mai. 2016. Disponível em: https://eur-lex.europa.eu/eli/reg/2016/679/oj. Acesso em: 10 ago. 2024.

WIMMER, Miriam. **Os desafios do *enforcement* na LGPD**: fiscalização, aplicação de sanções administrativas e coordenação intergovernamental. *In*: DONEDA, Danilo *et al*. Tratado de proteção de dados pessoais. Rio de Janeiro: Forence, 2021.