Revista UNITAS
ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

RESPONSABILIDADE CIVIL PELA VIOLAÇÃO DE DADOS PESSOAIS POR MEIO DA INTELIGÊNCIA ARTIFICIAL

Vitor Luís Botton[1]
Lucas Kayser Trevisol[2]

Resumo: O presente artigo busca analisar a responsabilidade civil decorrente da violação de dados pessoais por meio da inteligência artificial. O problema do estudo está pautado na seguinte pergunta: Como a responsabilidade civil vai ser determinada na crescente utilização de Inteligência Artificial (IA) e a consequente violação dos dados pessoais dos usuários? O objetivo é analisar, primeiramente, a responsabilidade civil na Lei Geral de Proteção de Dados, fazendo um comparativo com o instituto da responsabilidade civil no Projeto de Lei N° 2338, de 2023. Posteriomente será realizado um estudo sobre o vazamento de dados de ferramentas de inteligência artificial. Através da pesquisa bibliográfica chegou-se à conclusão de que se mostra de extrema importância a aprovação, pelo congresso nacional, do Projeto de Lei N° 2338, de 2023, que visa a regulamentar o uso da Inteligência Aritficial no Brasil.

Palavras Chave: Responsabilidade Civil; Inteligência Aritficial; Lei Geral De Proteção De Dados - LGPD

Abstract: This article seeks to analyze civil liability arising from the breach of personal data through artificial intelligence. The problem of the study is based on the following question: How will civil liability be determined in the increasing use of Artificial Intelligence (AI) and the consequent violation of users' personal data? The objective is to analyze, firstly, civil liability in the General Data Protection Law, making a comparison with the institute of civil liability in Bill No. 2338, of 2023. Subsequently, a study will be carried out on the leakage of data from tools of artificial intelligence. Through bibliographical research, it was concluded that the approval, by the national congress, of Bill No. 2338, of 2023, which aims to regulate the use of Artificial Intelligence in Brazil.

Keywords: Civil responsability; Artificial Intelligence; General Data Protection Law - LGPD

1 INTRODUÇÃO

Através do presente estudo buscar-se-á demonstrar a importância da regulamentação da responsabilidade civil pela violação de dados pessoais por meio da inteligência artificial, tendo em vista os crescentes casos de vazamento de dados decorrentes da utilização de ferramentas de inteligência artificial.

[1] Mestre em Direito pela Faculdade Meridional - IMED. Pós-graduado em Direito Contratual; Direito Empresarial; Direito Civil e Processo Civil e Direito Imobiliário. Graduado em Direito pela Universidade Regional Integrada do Alto Uruguai e das Missões. Advogado no escritório Grassi Jacomini Botton Advogados Associados, inscrito na OAB/RS nº 116.112. E-mail: vitorluisbotton@gmail.com.

[2] Graduado em Direito pela Universidade Regional Integrada do Alto Uruguai e das Missões. Especialista em direito penal e processual penal. Advogado. Juiz leigo do Juizado Especial Cível e conciliador criminal da Vara Criminal da Comarca de Frederico Westphalen/RS. E-mail: trevisol.luc@gmail.com.

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

Assim, em um primeiro momento realizar-se-á um estudo geral sobre responsabilidade civil na Lei Geral de Proteção de Dados - LGPD, estudando os regimes de responsabilidade civil e analisando argumentos sob os aspectos objetivos e subjetivos.

Posteriormente, em razão da necessidade de regulamentação, especialmente no campo da responsabilidade civil, o presente estudo se dedicará um capítulo à análise da Responsabilidade Civil no Projeto de Lei N° 2338, de 2023, que está prevista especificamente no Capítulo V, artigos 27 a 29.

Ainda, examinar-se-á a nota técnica publicada pela Autoridade Nacional de Proteção de Dados, Nota Técnica nº 16/2023/CGTP/ANPD na qual a Autoridade elaborou um estudo sobre o Projeto de Lei N° 2338, de 2023.

Por fim, serão trazidos estudos e notícias a respeito do vazamento de dados de ferramentas de inteligência artificial, apontando os principais países onde ocorrem estes incidentes e como grandes empresas estão agindo para evitar o vazamento de dados por seus colaboradores.

Ademais, o objetivo deste estudo consiste em verificar a responsabilidade civil na Lei Geral de Proteção de Dados, fazendo um comparativo com o instituto da responsabilidade civil no Projeto de Lei N° 2338, de 2023.

Este estudo emprega o método hipotético-dedutivo com enfoques qualitativos e quantitativos, conforme Mezzaroba e Monteiro (2009). Em relação à técnica procedimental, a pesquisa segue uma abordagem bibliográfica, que de acordo com Gil (2008), é realizada com base em obras já publicadas, como livros e artigos científicos.

Concluindo, procurar-se-á, no presente trabalho, a realização de um estudo sobre os aspectos gerais responsabilidade civil na Lei Geral de Proteção de Dados - LGPD, posteriormente, estudar-se-á sobre a responsabilidade civil no Projeto de Lei n° 2338, de 2023, fazendo um comparativo com a Nota Técnica nº 16/2023/CGTP/ANPD, publicada pela Autoridade Nacional de Proteção de Dados – ANPD, por fim, verificar-se-á casos de vazamento de dados de ferramentas de inteligência artificial.

2 RESPONSABILIDADE CIVIL NA LGPD

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

Um dos debates mais significativos em relação à Lei Geral de Proteção de Dados (LGPD) é referente a especécie da responsabilidade civil dos operadores de dados, afinal, a responsabilidade é objetiva ou subjetiva? A Lei Geral de Proteção de Dados não trouxe de forma expressa se a culpa é necessária para estabelecer a obrigação de indenizar.[3]

Em razão de não haver uma definição expressa na LGPD, existe um grande debate na doutrina, com entendimentos para ambos os lados, seja responsabilidade subjetiva, seja responsabilidade objetiva.[4]

No âmbito da proteção de dados pessoais, o princípio da responsabilidade adquire significativa importância, uma vez que visa garantir a reparação completa e apropriada dos danos materiais e morais causados à parte lesada. Isso se torna particularmente relevante para o presente estudo diante da violação do direito à privacidade.[5]

A LGPD introduziu um regime de responsabilidade civil específico para regular ocorrências de lesões no tratamento de dados pessoais. Apesar disso, é inegável reconhecer a importância de todo o arcabouço jurídico que aborda a responsabilidade civil e evolução do instituto ao longo do Século XX.[6]

Destaca-se que a proteção da privacidade em relação aos dados pessoais deve ser orientada por princípios, entre eles, o solidarismo entre os agentes de tratamento envolvidos em relações públicas e privadas.[7]

A LGPD estabelece que a proteção dos titulares de dados deve ser organizada, atendendo aos requisitos de segurança, boas práticas, governança e aos princípios gerais de proteção.

No entanto, é importante ressaltar que essa legislação não deve ser considerada de maneira isolada, mas sim interpretada de forma conjunta com a Constituição Federal e outros dispositivos legais.[8]

---

[3] (NOVAKOSKI, 2020)
[4] (FLORENCE, 2021).
[5] (MENDES, 2011).

[6] (NASPOLINI; NOVAKOSKI, 2020).
[7] (MISUGI; FREITAS; EFING, 2016).

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

Neste sentido, a LGPD institui uma seção específica para abordar a temática da responsabilidade e do ressarcimento de danos, que está previsto no artigo 42 ao 45, como se verá a seguir.

O Artigo 42 da LGPD[9] estabelece diretrizes fundamentais para determinar a responsabilidade em casos de danos patrimoniais, morais, individuais ou coletivos resultantes da violação de dados pessoais. Além disso, o §1º, I e II, desse artigo, destaca a possibilidade de responsabilidade solidária entre o controlador e o operador.

Avançando, o artigo 43 da LGPD[10] elenca as hipóteses de causas excludentes de responsabilidade dos agentes de tratamento dos dados pessoais, destacando que na violação à legislação de proteção de dados fica presumida a culpa dos agentes de tratamento de dados

---

[8] (SIMÃO FILHO, 2021).

[9] Art. 42. 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.

§ 1º A fim de assegurar a efetiva indenização ao titular dos dados:

I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;

II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

§ 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

§ 3º As ações de reparação por danos coletivos que tenham por objeto a responsabilização nos termos do caput deste artigo podem ser exercidas coletivamente em juízo, observado o disposto na legislação pertinente.

§ 4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso.

[10] Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:

I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou

III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

Já o artigo 44 da LGPD[11], trouxe um rol exemplificativo do que seriam circunstancias relevantes para o tratamento irregular dos dados pessoaissão elas: I – o modo pelo qual o tratamento é realizado; II – o resultado e os riscos que razoavelmente dele se esperam; e III – as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Ademais, o inciso III do artigo 44 da LGPD destaca a necessidade de se observar as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado, pois disponível não quer exatamente existente, tampouco existente significa disponível.[12]

Por fim, o artigo 45 da LGPD[13] destaca que ainda prevalecerão a proteção dos titulares dos dados no âmbito das relações de consumo em conformidade com as regras de responsabilidade previstas na legislação pertinente.

Diante da análise dos artigos referentes à responsabilidade civil na LGPD, verifica-se que a lei não prevê o elemento de culpa, mas também não o exclui explicitamente.

Dessa forma, pode-se constar o surgimento de um modelo mais maduro de responsabilidade civil, que vai além da responsabilidade do agente, principalmente para evitar danos.[14]

3 RESPONSABILIDADE CIVIL NO PROJETO DE LEI N° 2338, DE 2023.

Realiazo um estudo sobre a responsabilidade civil na LGPD, passar-se-á a analisar a responsabilidade civil no Projeto de Lei N° 2338, de 2023, que dispõe

---

[11] Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais:

I - o modo pelo qual é realizado;

II - o resultado e os riscos que razoavelmente dele se esperam;

III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.

Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano.

[12] (BIONI; DIAS, 2020).

[13] Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente.

[14] (MORAES; QUEIROZ, 2019).

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

sobre o uso da Inteligência Artificial, trouxe um capítulo inteiro (CAPÍTULO V) dedicado à responsabilidade civil da Inteligência Artificial, artigos 27 à 29.

O Artigo 27[15] estabelece normas específicas para a responsabilidade civil no contexto de sistemas de inteligência artificial. Ele determina que fornecedores ou operadores são obrigados a reparar integralmente danos patrimoniais, morais, individuais ou coletivos causados por sistemas de IA, independentemente do grau de autonomia.

Para sistemas de alto risco, a responsabilidade é objetiva, enquanto para sistemas de menor risco, a culpa do agente causador é presumida, favorecendo a vítima na inversão do ônus da prova. Esse artigo representa uma abordagem legislativa destinada a garantir a justa compensação em casos de danos relacionados à inteligência artificial.

É de grande importância a disposição dos § 1º e § 2º do artigo 27, do Projeto de Lei N° 2338, de 2023, pois ao trazer expressamente os regimes de responsabilidade dos fornecedores e operadores, não deixa dúvidas de qual será o regime aplicado ao caso concreto.

Entretanto, no aspecto prático, poderá ser levantada a questão do que seria um sistema de inteligência artificial de alto risco ou de risco excessivo, o que acarretaria, em regimes diferentes de responsabilidade. Desta forma, será necessária a delimitação e definição objetiva desses conceitos.

Já o artigo 28[16] do Projeto de Lei N° 2338, de 2023, trouxe um rol taxativo de hipóteses excludentes de responsabilidade, quais sejam, quando: I – comprovarem

---

[15] Art. 27. O fornecedor ou operador de sistema de inteligência artificial que cause dano patrimonial, moral, individual ou coletivo é obrigado a repará-lo integralmente, independentemente do grau de autonomia do sistema.

§ 1º Quando se tratar de sistema de inteligência artificial de alto risco ou de risco excessivo, o fornecedor ou operador respondem objetivamente pelos danos causados, na medida de sua participação no dano.

§ 2º Quando não se tratar de sistema de inteligência artificial de alto risco, a culpa do agente causador do dano será presumida, aplicando-se a inversão do ônus da prova em favor da vítima.

[16] Art. 28. Os agentes de inteligência artificial não serão responsabilizados quando:

I – comprovarem que não colocaram em circulação, empregaram ou tiraram proveito do sistema de inteligência artificial; ou

II – comprovarem que o dano é decorrente de fato exclusivo da vítima ou de terceiro, assim como de caso fortuito externo.

Art. 29. As hipóteses de responsabilização civil decorrentes de danos causados por sistemas de inteligência artificial no âmbito das relações de consumo permanecem sujeitas às regras previstas

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

que não colocaram em circulação, empregaram ou tiraram proveito do sistema de inteligência artificial; ou II – comprovarem que o dano é decorrente de fato exclusivo da vítima ou de terceiro, assim como de caso fortuito externo. Fica evidanciado, assim, a adoção do regime de responsabilidade objetiva.

No mesmo sentido do artigo 45 da LGPD, o artigo 29 do Projeto de Lei N° 2338, de 2023, estabelece que a responsabilização civil decorrente de danos causados por sistemas de inteligência artificial permanecerá protegida no âmbito das relações de consumo, pelo Código de Defesa do Consumidor.

Outrossim, o artigo 30[17] do Projeto de Lei N° 2338, de 2023 dispõe sobre a autonomia dos agentes de inteligência artificial para elaborar códigos de boas

---

na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), sem prejuízo da aplicação das demais normas desta Lei.

[17] Art. 30. Os agentes de inteligência artificial poderão, individualmente ou por meio de associações, formular códigos de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, inclusive sobre reclamações das pessoas afetadas, as normas de segurança, os padrões técnicos, as obrigações específicas para cada contexto de implementação, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e as medidas de segurança técnicas e organizacionais apropriadas para a gestão dos riscos decorrentes da aplicação dos sistemas.

§ 1º Ao se estabelecerem regras de boas práticas, serão consideradas a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes, a exemplo da metodologia disposta no art. 24 desta Lei.

§ 2º Os desenvolvedores e operadores de sistemas de inteligência artificial, poderão:

I – implementar programa de governança que, no mínimo:

a) demonstre o seu comprometimento em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à não maleficência e proporcionalidade entre os métodos empregados e as finalidades determinadas e legítimas dos sistemas de inteligência artificial;

b) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como ao seu potencial danoso;

c) tenha o objetivo de estabelecer relação de confiança com as pessoas afetadas, por meio de atuação transparente e que assegure mecanismos de participação nos termos do art. 24, § 3º, desta Lei;

d) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;

e) conte com planos de resposta para reversão dos possíveis resultados prejudiciais do sistema de inteligência artificial; e

f) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

§ 3º A adesão voluntária a código de boas práticas e governança pode ser considerada indicativo de boa-fé por parte do agente e será levada em consideração pela autoridade competente para fins de aplicação de sanções administrativas.

§ 4º A autoridade competente poderá estabelecer procedimento de análise de compatibilidade do código de conduta com a legislação vigente, com vistas à sua aprovação, publicização e atualização periódica.

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

práticas e governança. Ademais, já estabelece diretrizes que esses códigos devem abordar, tais como a organização, o funcionamento, procedimentos para reclamações de pessoas afetadas, normas de segurança, padrões técnicos, obrigações específicas para diferentes contextos de implementação, ações educativas, mecanismos internos de supervisão e mitigação de riscos, medidas de segurança técnicas e organizacionais adequadas para gerenciar os riscos associados à aplicação dos sistemas de inteligência artificial.

Resta previsto, no artigo 30, §1º, que para a elaboração das regras de boas práticas, deve-se observar a finalidade, a probabilidade e a gravidade dos riscos e dos benefícios decorrentes.

Por fim, os desenvolvedores e operadores de sistemas de inteligência artificial, poderão implementar programa de governança que, siga os padrões mínimos estabelecidos pelo artigo 30, §2º do Projeto de Lei N° 2338, de 2023.

4 NOTA TÉCNICA DA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

Diante do debate crescente sobre a regulamentação da Inteligência Artificial, a ANPD - Autoridade Nacional de Proteção de Dados, elaboroua a Nota Técnica nº 16/2023/CGTP/ANPD analisando o Projeto de Lei N° 2338, de 2023.

> A proposta reflete o amadurecimento, os avanços e os aprendizados acumulados desde a apresentação do PL nº 21/2020 e busca estabelecer um equilíbrio entre a promoção da inovação e a garantia dos direitos fundamentais dos cidadãos. A análise e discussão desse projeto são cruciais para definir os rumos da IA no País, e a ANPD se coloca como uma instituição-chave nesse processo.[18]

A nota prevê que é de suma importância enfatizar o papel proativo da Autoridade Nacional de Proteção de Dados (ANPD) na discussão sobre a regulamentação da Inteligência Artificial (IA), tendo em vista que a ANPD está comprometida em assegurar que a regulamentação da IA esteja em conformidade

[18] (BRASIL, p. 01, 2023)

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

com os princípios e diretrizes estipulados pela Lei Geral de Proteção de Dados Pessoais (LGPD).[19]

Destaca-se que a competência e a perspectiva da ANPD são fundamentais para garantir que os direitos dos cidadãos sejam preservados no âmbito da utilização da IA, especialmente no que se refere à proteção de dados pessoais.[20]

Inobstante, "a relação entre o Projeto de Lei nº 2338/2023 e a Lei Geral de Proteção de Dados Pessoais é intrínseca e fundamental para entender o panorama regulatório da Inteligência Artificial no Brasil."[21]

Embora o Projeto de Lei nº 2338/2023 e a Lei Geral de Proteção de Dados Pessoais tenham focos diferentes, ambas convergem em diversos pontos, à exemplo da da tutela de direitos dos cidadãos e da governança de tecnologias emergentes.[22]

O PL nº 2338/2023 prevê a necessidade de haver uma autoridade competente para regulamentar a Inteligência Artificial, conforme disposto no artigo 32 do referido projeto de lei, cabendo à autoridade competente zelar pela proteção a direitos fundamentais; promover a elaboração, atualização e implementação da Estratégia Brasileira de Inteligência Artificial; promover e elaborar estudos sobre boas práticas no desenvolvimento e utilização de sistemas de inteligência artificial; estimular a adoção de boas práticas; promover ações de cooperação com autoridades de proteção e de fomento ao desenvolvimento e à utilização dos sistemas de inteligência artificial, entre outras.[23]

A inteligência artificial requer uma governança sólida e eficiente. Experiências globais indicam que uma abordagem centralizada, fundamentada em uma única entidade, apresenta vantagens evidentes.[24]

Uma autoridade centralizada possui a habilidade de reagir de forma rápida e coordenada a desafios emergentes. Em um domínio tão dinâmico quanto o da IA, a

[19] (BRASIL, 2023)
[20] (BRASIL, 2023)
[21] (BRASIL, p. 02, 2023)
[22] (BRASIL, 2023)
[23] (BRASIL, 2023)
[24] (BRASIL, 2023)

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

agilidade na tomada de decisões pode ser essencial para prevenir ou reduzir riscos.[25]

Outrossim, a criação de uma entidade centralizada para regulamentar a IA fornece uma orientação clara e consistente para todos os envolvidos (desenvolvedores, empresa, poder público, usuários, etc.), eliminando ambiguidades e garantindo que todos tenham um entendimento uniforme das regras. Destaca-se, no entando, que uma regulamentação centralizada não impede que reguladores específicos desenvolvam suas próprias regras para o uso da Inteligência Artificial, desde que estejam, obviamente, alinhadas a diretrizes estabelecidas pela autoridade central.[26]

Dito isso, na Nota Técnica nº 16/2023/CGTP/ANPD, a ANPD faz uma referência de que a IA, em razão da capacidade de processamento e análise de dados, se alinha diretamente às competências da ANPD, destacando que o modelo de centralização da governança da IA em torno da ANPD é uma estratégia promissora.[27]

5 VAZAMENTO DE DADOS DE FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL

Recentemente, descobriu-se que mais de 100.000 contas ChatGPT foram comprometidas por invasores cibernéticos (*crackers*), de acordo com relatórios do Group-IB[28], que é líder em segurança cibernética global com sede em Cingapura.[29]

A pesquisa apontou que mais de 100.000 (cem mil) dispositivos foram infiltrados com *malware* que acabou roubando dados e informações confidenciais, incluindo credenciais de *login* armazenadas no aplicativo ChatGPT. Pode-se afirmar que este incidente representa um novo desafio significativo para o campo da segurança cibernética.

As credenciais comprometidas foram rastreadas até registros de *malware* que roubaram informações, que foram negociadas na *dark web* por pelo menos um ano.

[25] (BRASIL, 2023)
[26] (BRASIL, 2023)
[27] (BRASIL, 2023)
[28] https://www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials/
[29] (SHESTAKOV, 2023)

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

A investigação do Grupo-IB revelou que, em maio de 2023, o problema atingiu o ápice, com 26.802 (vinte e seis mil, oitocentos e dois) destes dados disponíveis na *dark web*. Deste modo, é de extrema importância o desenvolvimento de medidas corretivas.[30]

Durante o estudo realizado pelo Grupo-IB, constatou-se especialmente a necessidade de uma abordagem específica na região da Ásia-Pacífico para enfrentar a ameaça emergente decorrente da má utilização do ChatGPT, tendo em vista a elevada concentração de credenciais vendidas na área.

É sabido que para o desenvolvimento de *software* e na comunicação empresarial, existe uma tendência crescente de uso do ChatGPT pelos funcionários para agilizar tarefas. Os especialistas do Group-IB, no entanto, alertam que isso traz seu próprio conjunto de perigos – o ChatGPT arquiva automaticamente as consultas dos usuários e as respostas da IA. Isto deixa a empresa e os seus funcionários abertos a compromissos, uma vez que informações sensíveis podem ser acessadas através de meios não autorizados através de ataques cibernéticos.[31]

A popularidade dos *chatbots* com tecnologia de IA está aumentando, como evidenciado por um número crescente de contas comprometidas em registros realiazados pelo Group-IB.

A orientação repassada pelo Group-IB destaca a importância de os usuários implementarem a autenticação de dois fatores em seus dispositivos e atualizarem regularmente suas senhas como medidas de segurança proativas em resposta a esta ameaça. A ativação da autenticação de dois fatores aumenta a segurança, exigindo que os usuários insiram um segundo código de verificação, que geralmente é enviado para dispositivos móveis, antes que possam acessar suas contas ChatGPT.[32]

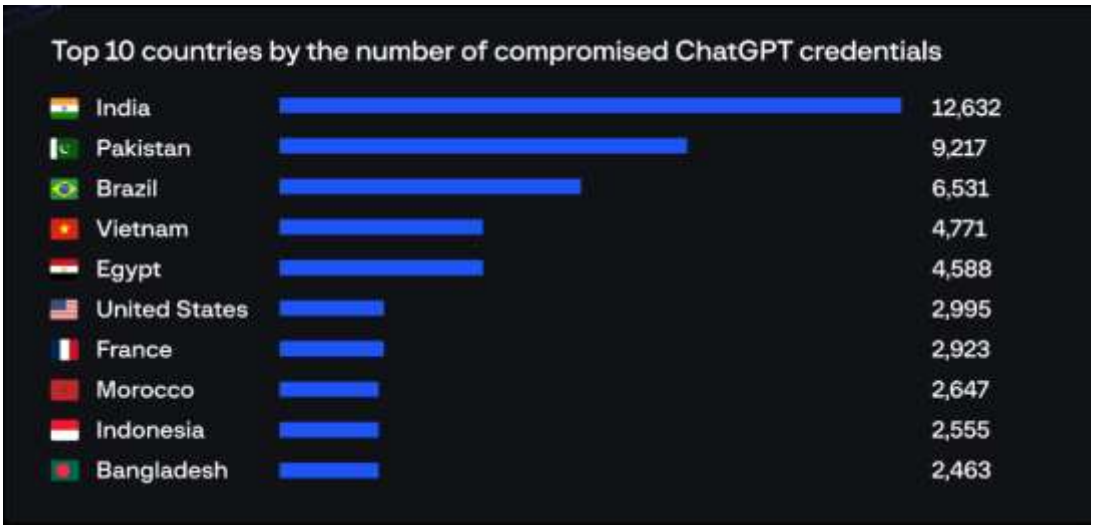
Não obstante, a visibilidade nas comunidades da *dark web* permite que as organizações identifiquem ameaças cibernéticas em tempo real. Com essa informação, as empresas de segurança cibernética podem tomar medidas proativas

[30] (SHESTAKOV, 2023)
[31] (SHESTAKOV, 2023)
[32] (SHESTAKOV, 2023)

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

para mitigar o impacto de um ataque, notificar os indivíduos afetados e fortalecer sua postura de segurança.[33]

Um outro ponto que chama atenção no estudo, é de que o Brasil é o terceiro país com mais vazamento de dados do ChatGPT, conforme pode-se verificar na figura abaixo, ficando atrás apenas da Índia e do Paquistão.



Fonte: (SHESTAKOV, 2023)

De olho nisso, com receio de que funcionários utilizassem ferramentas de IA para desenvolver e pesquisar os segredos internos, muitas empresas acabaram por proibir o uso delas, como por exemplo o Banco JPMorgan Chase, Bank Of America, Samsung[34] e a Apple[35], entre outras.

Outra situação que chama atenção é que está previsto, nas políticas de privacidade do Google Bard, que revisores humanos treinados precisam processar suas conversas com o intuito de melhorar os modelos de aprendizado de máquina, orientando, ainda, que não sejam inseridas informações confidenciais nas conversas no Bard.

> Revisores humanos leem, fazem anotações e processam suas conversas no Bard para aprimorar a qualidade dos nossos serviços e produtos, como

[33] (SHESTAKOV, 2023)

[34] https://www.bloomberglinea.com.br/2023/05/02/samsung-proibe-funcionarios-de-usar-o-chatgpt-apos-vazamento-de-codigo-fonte/

[35] https://forbes.com.br/carreira/2023/05/apple-e-a-mais-nova-empresa-a-proibir-que-funcionarios-usem-o-chatgpt/

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

> os modelos generativos de aprendizado de máquina que o Bard usa. Esse processo inclui medidas para proteger sua privacidade. Por exemplo, desvincular suas conversas no Bard da Conta do Google antes do acesso e anotações dos revisores. Não insira informações confidenciais nas conversas no Bard, nem dados que você não quer que sejam revisados ou usados para aprimorar nossos produtos, serviços e tecnologias de aprendizado de máquina.[36]

Assim, foi possível visualizar estudos sobre vazamento de dados de ferramentas de inteligência artificial realizados pelo Group-IB, e constatar que grandes empresas estão preocupadas com a utilização dessas ferramentas por parte de seus funcionários, tendo em vista o grande risco de vazamentos de dados e segredos empresariais.

6 CONCLUSÃO

Através do presente estudo buscou demonstrar a importância da regulamentação da responsabilidade civil em decorrência dos casos de vazamentos de dados pessoais através da inteligência artificial, tendo em vista a crescente onda de casos de vazamento de dados decorrentes da utilização de ferramentas de inteligência artificial.

Inicialmente, o presente estudo dedicou-se a um estudo geral sobre a responsabilidade civil na Lei Geral de Proteção de Dados - LGPD, estudando os regimes de responsabilidade civil sob os aspectos objetivos e subjetivos. Verificou-se que a LGPD estabeleceu diferenças entre as figuras do controlador e do operador, o que acarreta em responsabilidades igualmente diferentes, trazendo um regime totalmente inovador.

Posteriormente, realizou-se uma análise minuciosa a respeito da Responsabilidade Civil no Projeto de Lei N° 2338, de 2023, estudando, de forma pormenorizada, o Capítulo V e os artigos 27 a 29.

Isso posto, constatou-se que o artigo 27 do Projeto de Lei N° 2338, de 2023 estabelece normas específicas para a responsabilidade civil no contexto de sistemas de inteligência artificial. Quando o sistema é de alto risco, a responsabilidade é objetiva, enquanto para sistemas de menor risco, a culpa do agente causador é

[36] (GOOGLE, 2023)

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

presumida. Além do mais, o artigo 28 do Projeto de Lei N° 2338, de 2023, trouxe um rol taxativo de hipóteses excludentes de responsabilidade. Por fim, o artigo 30 do Projeto de Lei N° 2338, de 2023 dispõe sobre a autonomia dos agentes de inteligência artificial para elaborar códigos de boas práticas e governança.

Foi possível constatar que a nota técnica publicada pela Autoridade Nacional de Proteção de Dados, Nota Técnica nº 16/2023/CGTP/ANPD, na qual a Autoridade elaborou um estudo sobre o Projeto de Lei N° 2338, de 2023, trouxe importantes análises sobre o projeto, destacando que a Inteligência Artificial, em razão da capacidade de processamento e análise de dados, se alinha diretamente às competências da ANPD, se canditandando como autoridade para regulamentar a Inteligência Artificil, tendo em vista que centralização da governança da IA em torno da ANPD é uma estratégia promissora.

Ademais, verificou-se através de um estudo publicado pelo Group-IB, que o Brasil é o terceiro país que mais teve vazamentos de dados pessoais, pelo ChatGPT, ficando atrás apenas da Índia e do Paquistão. O estudo expôs que foram vazadas credenciais de acesso ao ChatGPT, e também as informações que os usuários inseriram na ferramenta, o que gera grande preocupação com a segurança das informações.

Constatou-se que grandes empresas como por exemplo o Banco JPMorgan Chase, Bank Of America, Samsung e a Apple, estão agindo para evitar o vazamento de dados, proibindo que os seus funcionários utilizem as ferramentas externas de *chatbots* no seu trabalho.

Assim, através do método hipotético-dedutivo e da pesquisa bibliográfica, diante do crescente número de casos de vazamento de dados pessoais, por meio das ferramentas de inteligência artificial, bem como a comercialização destes dados na *dark web,* verificou-se a necessidade da regulamentação da Inteligência Artificial no Brasil, especialmente no que diz respeito à responsabilidade civil por violação de dados pessoais decorrentes da IA, o que constatou-se estar abordado no Projeto de Lei N° 2338, de 2023 de forma satisfatória, impondo responsabilidades tanto à sistemas de alto risco, quando a responsabilidade é objetiva, quanto para sistemas de menor risco, que a culpa do agente causador será presumida.

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

REFERENCIAS

BIONI, Bruno; DIAS, Daniel. Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor. **Civilistica.com**, v. 9, n. 3, p. 1-23, 2020. Disponível em: https://civilistica.emnuvens.com.br/redc/article/view/662. Acesso em: 01 dez. 2023.

BLOOMBERG. **Samsung proíbe funcionários de usar o ChatGPT após vazamento de código-fonte**, 2023. Disponível em:

BRASIL, Autoridade Nacional de Proteção de Dados - ANPD. **Nota Técnica nº 16/2023/CGTP/ANPD.** 2023, Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/Nota_Tecnica_16ANPDIA.pdf Acesso em: 01 dez. 2023.

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, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 01 dez. 2023.

BRASIL. Projeto de Lei n° 2338, de 2023. **Dispõe sobre o uso da Inteligência Artificial.**. Brasília: DF, 2023. Disponível em: https://legis.senado.leg.br/sdleg-getter/documento?dm=9347593&ts=1701182930205&disposition=inline&_gl=1*5qajfo*_ga*Mzc4NjQ5MzEzLjE3MDExMzE3ODE.*_ga_CW3ZH25XMK*MTcwMjAwMTAyMy4zLjEuMTcwMjAxMzM4NS4wLjAuMA.. Acesso em: 01 dez. 2023.

FLORENCE, Tatiana Magalhães; FORTES, Thais Gonçalves. Apontamentos sobre a responsabilidade civil no tratamento de dados. **Revista Brasileira de Direito Civil**, v. 30, n. 04, p. 223, 2021.

FORBES. **Apple é a mais nova empresa a proibir que funcionários usem o ChatGPT.** 2023. Disponível em: https://forbes.com.br/carreira/2023/05/apple-e-a-

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

mais-nova-empresa-a-proibir-que-funcionarios-usem-o-chatgpt/ Acesso em: 01 dez. 2023.

GIL, Antonio Carlos. **Dados e técnicas de pesquisa social**. Editora Atlas, 6ª ed. São Paulo, 2008.

GOOGLE. **Central de Ajuda de Privacidade do Bard.** 2023, Disponível em: https://support.google.com/bard/answer/13594961?visit_id=638375973274804818-3878918026&p=privacy_notice&rd=1#privacy_notice Acesso em: 01 dez. 2023.
https://www.bloomberglinea.com.br/2023/05/02/samsung-proibe-funcionarios-de-usar-o-chatgpt-apos-vazamento-de-codigo-fonte/ Acesso em: 01 dez. 2023.
https://www.group-ib.com/media-center/press-releases/stealers-chatgpt-credentials/ Acesso em: 01 dez. 2023.

MENDES, Laura Schertel. O direito fundamental à proteção de dados pessoais. **Revista de Direitos do Consumidor**, São Paulo, v. 20, 2011.

MEZZAROBA, Orides; MONTEIRO, Claudia S. **Manual de metodologia da pesquisa no direito.** Editora Saraiva, 5ª ed. São Paulo, 2009.

MISUGI, Guilherme; FREITAS, Cinthia Obladen de Almendra; EFING, Antonio Carlos. Releitura da privacidade diante das novas tecnologias: realidade aumentada, reconhecimento facial e Internet das coisas. **Revista Jurídica Cesumar-Mestrado**, v. 16, n. 2, p. 427-453, 2016. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/4433. Acesso em 05 dez. 2023.

MORAES, Maria Celina Bodin de; QUEIROZ, João Quinelato de. Autodeterminação informativa e responsabilização proativa: novos instrumentos de tutela da pessoa humana na LGDP. **IN: Cadernos Adenauer**, v. 3, 2019.

ISSN 2525-4243 / Nº 8 / Ano 2023 / p. 136-152

NASPOLINI, Samyra Haydêe Dal Farra; NOVAKOSKI, André Luis Mota. Responsabilidade civil na LGPD: problemas e soluções. **Conpedi Law Review**, v. 6, n. 1, p. 158-174, 2020. Disponível em: https://www.indexlaw.org/index.php/conpedireview/article/view/7024. Acesso em 05 dez. 2023.

NOVAKOSKI, André Luis Mota; NASPOLINI, S. H. D. F. Responsabilidade civil na LGPD: problemas e soluções. Conpedi Law Review, Florianópolis, v. 6, n. 1, p. 158-174, 2020.

SHESTAKOV, Dmitry. **Group-IB Discovers 100K+ Compromised ChatGPT Accounts on Dark Web Marketplaces; Asia-Pacific region tops the list.** 2023. Disponível em:

SIMÃO FILHO, Adalberto. Limites e contornos da responsabilidade civil dos agentes de tratamento de dados. **Revista IBERC**, v. 4, n. 3, p. 38-52, 2021.