



ALEXANDRE HENRIQUE DE SOUSA OLIVEIRA

LUCAS DELMONDES MARTINS LIMA

**DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ERA DAS
INTELIGÊNCIAS ARTIFICIAIS: limites do ordenamento jurídico e da atuação da
advocacia**

TERESINA-PI

2025

ALEXANDRE HENRIQUE DE SOUSA OLIVEIRA

LUCAS DELMONDES MARTINS LIMA

**DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ERA DAS
INTELIGÊNCIAS ARTIFICIAIS: limites do ordenamento jurídico e da atuação da
advocacia**

Trabalho de Conclusão de Curso
apresentado à Afya Centro Universitário –
Uninovafapi, para obtenção do título de
Bacharel em 2026.

Orientador: Prof. Dr. Alexandre Augusto
Batista de Lima

TERESINA – PI

2025

ALEXANDRE HENRIQUE DE SOUSA OLIVEIRA

LUCAS DELMONDES MARTINS LIMA

**DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ERA DAS
INTELIGÊNCIAS ARTIFICIAIS: limites do ordenamento jurídico e da atuação da
advocacia**

Trabalho de Conclusão de Curso
apresentado à Afya Centro Universitário –
Uninovafapi, para obtenção do título de
Bacharel em 2026.

Orientador: Prof. Dr. Alexandre Augusto
Batista de Lima

TERESINA – PI

2025

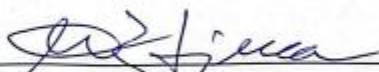
ALEXANDRE HENRIQUE DE SOUSA OLIVEIRA
LUCAS DELMONDES MARTINS LIMA

**DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ERA
DAS INTELIGÊNCIAS ARTIFICIAIS: limites do ordenamento jurídico e da
atuação da advocacia**

Artigo de Trabalho de Conclusão de Curso
apresentado à Banca Examinadora do
Afya Centro Universitário Uninovafapi,
como requisito parcial para obtenção do
grau de Bacharel em Direito.

Data de Aprovação: 13 / 11 / 2025.

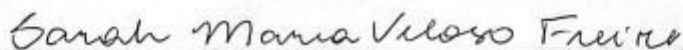
BANCA EXAMINADORA



Professor Doutor Alexandre Augusto Batista de Lima
Afya Centro Universitário Uninovafapi
(Orientador)



Professor Mestre Marcelo Martins Eulálio
Afya Centro Universitário Uninovafapi
(1º Examinador)



Professora Mestra Sarah Maria Veloso Freire
Afya Centro Universitário Uninovafapi
(2º Examinador)

FICHA CATALOGRÁFICA

148d Oliveira, Alexandre Henrique de Sousa

Desafios da proteção de dados pessoais na era das inteligências artificiais: limites do ordenamento jurídico e da atuação da advocacia / Alexandre Henrique de Sousa Oliveira; Lucas Delmondes Martins Lima. — Teresina: UNINOVAFAPI, 2025.

Orientador (a): Prof^o. Dr. Alexandre Augusto Batista de Lima. — UNINOVAFAPI, 2025.

30.p.; 23cm.

Trabalho de conclusão (Graduação em direito) – UNINOVAFAPI, Teresina, 2025.

1. Agência Nacional de Proteção de Dados. 2. Inteligência artificial. 3. Lei Geral da Proteção de Dados. 4. Prática jurídica. I. Título. II. Lima, Lucas Delmondes Martins.

CDD 340.12

RESUMO

Este artigo busca investigar o problema que o advento das Inteligências Artificiais (IAs) representa para a proteção de dados pessoais no Brasil, e a limitação do arcabouço legal, bem como uma reconfiguração do papel da prática/advocacia jurídica que é exigida por elas, resultado desses desafios. A transformação dos dados pessoais, a matéria-prima da economia digital e da humanidade, pessoal assim como uma instância da dignidade humana é onde a borracha encontra a estrada da transformação ao ser ameaçada pela pura complexidade técnica e pela não transparência do processo de tomada de decisão algorítmica, referido como a "caixa preta algorítmica". A hipótese central do estudo é que a Lei Geral de Proteção de Dados (LGPD) é, de certa forma, insuficiente para enfrentar os problemas particulares da IA, nomeadamente aqueles associados à transparência, responsabilidade e prevenção de violações de direitos fundamentais como o direito à autodeterminação informacional. Essa lacuna normativa, juntamente com a velocidade da inovação, resulta em um descompasso com a resposta legislativa. O artigo responde à natureza multidimensional da prática jurídica. O advogado tem que atuar tanto na arena rancorosa onde a reparação de danos e a inversão do ônus da prova quanto na fase proativa, com conformidade digital e auditorias algorítmicas. A conclusão é que aprimorar a proteção de dados na era da IA requer legislação aprimorada fortalecimento institucional da Autoridade Nacional de Proteção de Dados (ANPD) bem como uma profissão jurídica autoritária e ética que não apenas assegure que a tecnologia proteja os direitos fundamentais

Palavras-chave: Agência Nacional de Proteção de Dados; Inteligência Artificial; Lei Geral da Proteção de Dados; Prática Jurídica.

ABSTRACT

This article seeks to investigate the problem that the advent of Artificial Intelligences (AIs) represents for the protection of personal data in Brazil, and the limitation of the legal framework, as well as a reconfiguration of the role of legal practice/advocacy that is demanded by them, resulting from these challenges. The transformation of personal data, the raw material of the digital economy and of humanity, both personal and as an instance of human dignity, is where the rubber meets the road of transformation when threatened by the sheer technical complexity and non-transparency of the algorithmic decision-making process, referred to as the "algorithmic black box". The study's central hypothesis is that the General Data Protection Law (Lei Geral de Proteção de Dados - LGPD) is, to a certain extent, insufficient to face the particular problems of AI, namely those associated with transparency, accountability, and the prevention of violations of fundamental rights such as the right to informational self-determination. This normative gap, along with the speed of innovation, results in a mismatch with the legislative response. The article responds to the multidimensional nature of legal practice. The lawyer has to act both in the contentious arena where compensation for damages and the reversal of the burden of proof take place, and in the proactive phase, with digital compliance and algorithmic audits. The conclusion is that enhancing data protection in the AI era requires improved legislation, institutional strengthening of the National Data Protection Authority (ANPD), as well as an authoritative and ethical legal profession that not only ensures that technology protects fundamental rights.

Keywords: National Data Protection Authority; Artificial Intelligence; General Data Protection Law; Legal Practice.

SUMÁRIO

1 INTRODUÇÃO	9
2 ARTIGO	12
2.1 O PAPEL DA ADVOCACIA DIANTE DAS VIOLAÇÕES DE DADOS RELACIONADAS AO USO DE TECNOLOGIAS BASEADAS EM IA	15
2.2 A EVOLUÇÃO DOS SISTEMAS JUDICIAIS ATUAIS PARA RISCO, DISRUPÇÃO E REPARAÇÃO DE DANOS EM CASOS DE ALGORITMOS	20
2.3 O IMPACTO DOS VAZAMENTOS DE DADOS NO SETOR PÚBLICO BRASILEIRO E SUAS IMPLICAÇÕES LEGAIS À LUZ DO PAPEL DA PROFISSÃO JURÍDICA NA ERA DIGITAL	24
3 CONSIDERAÇÕES FINAIS	29
REFERÊNCIAS.....	30
ANEXO A	31

INTRODUÇÃO

A digitalização de toda a vida e, mais recentemente, o surgimento das Inteligência Artificial (IA) são um imperativo para a humanidade, mudando forças sociais, econômicas e legais como nada mais de forma rápida. Central para essa mudança está a informação individual: a matéria-prima da economia da informação, uma ferramenta de poder e, antes de tudo, uma manifestação da dignidade da pessoa humana.

À medida que os algoritmos avançam, cada vez mais sofisticados e autônomos, as formas como armazenamos, processamos e usamos nossos dados pessoais vão além dos limites e limitações convencionais da supervisão humana direta, levando os sistemas normativos nos quais baseamos nossa prática ética ao limite até agora.

O novo paradigma representa um desafio significativo para o arcabouço legal. Uma IA que é tecnicamente sofisticada também viola e obscurece princípios básicos de transparência, propósito, consentimento livre e autodeterminação sobre quais informações fornecer, ou não, e está sujeita à caixa preta algorítmica ou regras de caixa preta de tomada de decisão opaca.

A Lei Geral de Proteção de Dados (Lei nº 13,709, de 14 de agosto de 2018, LGPD) no Brasil representa um salto normativo à frente, mas à medida que o desenvolvimento técnico continua a todo vapor e sem aviso, há certos elementos em que a lei pode ficar aquém na realidade de hoje. Regulamentações específicas para sistemas de IA, e como elas podem aplicar a lei clássica em ambientes automatizados, parecem refletir uma desconexão entre a inovação tecnológica e as respostas legislativas.

Por outro lado, advogados que servem como agentes da lei e garantidores da legalidade são confrontados com um novo conjunto de responsabilidades. Anteriormente guiados por instrumentos legais estáveis e compreensíveis que eram uma marca de sua prática, mas que agora exigem conhecimento técnico multidisciplinar, atualização perpétua e uma capacidade de traduzir normas em uma situação em mudança.

Nesse sentido, o presente documento irá tratar de aspectos relevantes na discussão sobre melhorias na atuação da advocacia juntamente com o sistema jurídico brasileiro como o papel da advocacia diante das violações de dados

relacionadas ao uso de tecnologias baseadas em IA; a evolução dos sistemas judiciais atuais para risco, disrupção e reparação de danos em casos de algoritmos e por fim abordar sobre o impacto dos vazamentos de dados no setor público brasileiro e suas implicações legais à luz do papel da profissão jurídica na era digital.

Assim tenta-se fornecer uma visão detalhada sobre as capacidades e deficiências das leis atuais, especialmente a LGPD, os desafios práticos para os profissionais em termos de proteger esses direitos fundamentais sobre a privacidade e autodeterminação informacional em sistemas automatizados.

Também se postula que, a esse respeito, assume-se que o sistema jurídico brasileiro atual, tendo recebido em alguns aspectos o desenvolvimento da LGPD, não está totalmente preparado para lidar com os requisitos específicos gerados pela aplicação de tecnologias de IA, particularmente em relação à responsabilidade, transparência algorítmica e prevenção de violações de direitos fundamentais.

Além disso, se confirma que a indústria jurídica enfrenta barreiras práticas e éticas na defesa dos titulares de dados porque a regulamentação sobre IAs, a complexidade tecnológica das tecnologias envolvidas e a necessidade de treinamento contínuo para acompanhar os avanços técnicos podem impedir a prática jurídica.

Os objetos de pesquisa são o problema do que o sistema jurídico brasileiro e a atividade jurídica terão que ser desafiados para proteger os dados pessoais do povo brasileiro quando tecnologias de Inteligência Artificial forem desenvolvidas. A principal missão deste artigo é, em geral, examinar as principais dificuldades da estrutura jurídica brasileira e da prática jurídica, na questão da proteção pessoal de dados devido ao surgimento das IAs.

Além de sua relevância prática e social, é também uma análise interdisciplinar do fenômeno, aliando fundamentos jurídicos, reflexões éticas e desafios enfrentados pela advocacia contemporânea. Assim, pretende-se contribuir com o desenvolvimento do pensamento jurídico voltado à proteção de dados em ambientes altamente tecnologizados, fomentando uma abordagem que una inovação, responsabilidade e respeito aos direitos fundamentais.

Portanto, o estudo utiliza revisão bibliográfica narrativa como formato da metodologia do estudo, utilizando uma abordagem qualitativa, exploratória e descritiva. O estudo foi desenvolvido com base em estudos sobre a legislação constitucional e infraconstitucional relevante para a política ou pesquisa,

especialmente na LGPD, e doutrina especializada em proteção de dados e direito digital, com a intenção de reforçar a teoria e as conclusões derivadas.

2 ARTIGO

DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ERA DAS INTELIGÊNCIAS

ARTIFICIAIS: limites do ordenamento jurídico e da atuação da advocacia

CHALLENGES OF PERSONAL DATA PROTECTION IN THE AGE OF ARTIFICIAL

INTELLIGENCES: limits of the legal framework and the role of legal
practice/advocacy

RESUMO: Este artigo busca investigar o problema que o advento das Inteligências Artificiais (IAs) representa para a proteção de dados pessoais no Brasil, e a limitação do arcabouço legal, bem como uma reconfiguração do papel da prática/advocacia jurídica que é exigida por elas, resultado desses desafios. A transformação dos dados pessoais, a matéria-prima da economia digital e da humanidade, pessoal assim como uma instância da dignidade humana é onde a borracha encontra a estrada da transformação ao ser ameaçada pela pura complexidade técnica e pela não transparência do processo de tomada de decisão algorítmica, referido como a "caixa preta algorítmica". A hipótese central do estudo é que a Lei Geral de Proteção de Dados (LGPD) é, de certa forma, insuficiente para enfrentar os problemas particulares da IA, nomeadamente aqueles associados à transparência, responsabilidade e prevenção de violações de direitos fundamentais como o direito à autodeterminação informacional. Essa lacuna normativa, juntamente com a velocidade da inovação, resulta em um descompasso com a resposta legislativa. O artigo responde à natureza multidimensional da prática jurídica. O advogado tem que atuar tanto na arena rancorosa onde a reparação de danos e a inversão do ônus da prova quanto na fase proativa, com conformidade digital e auditorias algorítmicas. A conclusão é que aprimorar a proteção de dados na era da IA requer legislação aprimorada fortalecimento institucional da Autoridade Nacional de Proteção de Dados (ANPD) bem como uma profissão jurídica autoritária e ética que não apenas assegure que a tecnologia proteja os direitos fundamentais

Palavras-chave: Agência Nacional de Proteção de Dados; Inteligência Artificial; Lei Geral da Proteção de Dados; Prática Jurídica.

ABSTRACT: This article seeks to investigate the problem that the advent of Artificial Intelligences (AIs) represents for the protection of personal data in Brazil, and the limitation of the legal framework, as well as a reconfiguration of the role of legal practice/advocacy that is demanded by them, resulting from these challenges. The transformation of personal data, the raw material of the digital economy and of humanity, both personal and as an instance of human dignity, is where the rubber meets the road of transformation when threatened by the sheer technical complexity and non-transparency of the algorithmic decision-making process, referred to as the "algorithmic black box". The study's central hypothesis is that the General Data Protection Law (Lei Geral de Proteção de Dados - LGPD) is, to a certain extent, insufficient to face the particular problems of AI, namely those associated with transparency, accountability, and the prevention of violations of fundamental rights

such as the right to informational self-determination. This normative gap, along with the speed of innovation, results in a mismatch with the legislative response. The article responds to the multidimensional nature of legal practice. The lawyer has to act both in the contentious arena where compensation for damages and the reversal of the burden of proof take place, and in the proactive phase, with digital compliance and algorithmic audits. The conclusion is that enhancing data protection in the AI era requires improved legislation, institutional strengthening of the National Data Protection Authority (ANPD), as well as an authoritative and ethical legal profession that not only ensures that technology protects fundamental rights.

Keywords: National Data Protection Authority; Artificial Intelligence; General Data Protection Law; Legal Practice.

INTRODUÇÃO

A digitalização de toda a vida e, mais recentemente, o surgimento das Inteligência Artificial (IA) são um imperativo para a humanidade, mudando forças sociais, econômicas e legais como nada mais de forma rápida. Central para essa mudança está a informação individual: a matéria-prima da economia da informação, uma ferramenta de poder e, antes de tudo, uma manifestação da dignidade da pessoa humana.

À medida que os algoritmos avançam, cada vez mais sofisticados e autônomos, as formas como armazenamos, processamos e usamos nossos dados pessoais vão além dos limites e limitações convencionais da supervisão humana direta, levando os sistemas normativos nos quais baseamos nossa prática ética ao limite até agora.

O novo paradigma representa um desafio significativo para o arcabouço legal. Uma IA que é tecnicamente sofisticada também viola e obscurece princípios básicos de transparência, propósito, consentimento livre e autodeterminação sobre quais informações fornecer, ou não, e está sujeita à caixa preta algorítmica ou regras de caixa preta de tomada de decisão opaca.

A Lei Geral de Proteção de Dados (Lei nº 13,709, de 14 de agosto de 2018, LGPD) no Brasil representa um salto normativo à frente, mas à medida que o desenvolvimento técnico continua a todo vapor e sem aviso, há certos elementos em que a lei pode ficar aquém na realidade de hoje. Regulamentações específicas para sistemas de IA, e como elas podem aplicar a lei clássica em ambientes automatizados, parecem refletir uma desconexão entre a inovação tecnológica e as respostas legislativas.

Por outro lado, advogados que servem como agentes da lei e garantidores da legalidade são confrontados com um novo conjunto de responsabilidades. Anteriormente guiados por instrumentos legais estáveis e compreensíveis que eram uma marca de sua prática, mas que agora exigem conhecimento técnico multidisciplinar, atualização perpétua e uma capacidade de traduzir normas em uma situação em mudança.

Nesse sentido, o presente documento irá tratar de aspectos relevantes na discussão sobre melhorias na atuação da advocacia juntamente com o sistema jurídico brasileiro como o papel da advocacia diante das violações de dados relacionadas ao uso de tecnologias baseadas em IA; a evolução dos sistemas judiciais atuais para risco, disrupção e reparação de danos em casos de algoritmos e por fim abordar sobre o impacto dos vazamentos de dados no setor público brasileiro e suas implicações legais à luz do papel da profissão jurídica na era digital.

Assim tenta-se fornecer uma visão detalhada sobre as capacidades e deficiências das leis atuais, especialmente a LGPD, os desafios práticos para os profissionais em termos de proteger esses direitos fundamentais sobre a privacidade e autodeterminação informacional em sistemas automatizados.

Também se postula que, a esse respeito, assume-se que o sistema jurídico brasileiro atual, tendo recebido em alguns aspectos o desenvolvimento da LGPD, não está totalmente preparado para lidar com os requisitos específicos gerados pela aplicação de tecnologias de IA, particularmente em relação à responsabilidade, transparência algorítmica e prevenção de violações de direitos fundamentais.

Além disso, se confirma que a indústria jurídica enfrenta barreiras práticas e éticas na defesa dos titulares de dados porque a regulamentação sobre IAs, a complexidade tecnológica das tecnologias envolvidas e a necessidade de treinamento contínuo para acompanhar os avanços técnicos podem impedir a prática jurídica.

Os objetos de pesquisa são o problema do que o sistema jurídico brasileiro e a atividade jurídica terão que ser desafiados para proteger os dados pessoais do povo brasileiro quando tecnologias de Inteligência Artificial forem desenvolvidas. A principal missão deste artigo é, em geral, examinar as principais dificuldades da estrutura jurídica brasileira e da prática jurídica, na questão da proteção pessoal de dados devido ao surgimento das IAs.

Além de sua relevância prática e social, é também uma análise interdisciplinar

do fenômeno, aliando fundamentos jurídicos, reflexões éticas e desafios enfrentados pela advocacia contemporânea. Assim, pretende-se contribuir com o desenvolvimento do pensamento jurídico voltado à proteção de dados em ambientes altamente tecnologizados, fomentando uma abordagem que una inovação, responsabilidade e respeito aos direitos fundamentais.

Portanto, o estudo utiliza revisão bibliográfica narrativa como formato da metodologia do estudo, utilizando uma abordagem qualitativa, exploratória e descritiva. O estudo foi desenvolvido com base em estudos sobre a legislação constitucional e infraconstitucional relevante para a política ou pesquisa, especialmente na LGPD, e doutrina especializada em proteção de dados e direito digital, com a intenção de reforçar a teoria e as conclusões derivadas.

2.1 O PAPEL DA ADVOCACIA DIANTE DAS VIOLAÇÕES DE DADOS RELACIONADAS AO USO DE TECNOLOGIAS BASEADAS EM IA

A privacidade dos dados pessoais domina as discussões atuais sobre o impacto da IA na sociedade. No Brasil, esse direito é garantido pela Constituição Federal de 1988, que assegura a inviolabilidade da intimidade, a privacidade da vida entre os indivíduos e a confidencialidade das comunicações (de acordo com os art. 5º, X e XII).

É uma promessa fundamental ligada à dignidade humana. Segundo Doneda (2019 p.45), a proteção de dados é um direito fundamental autônomo, e protege a autonomia individual em uma sociedade altamente informatizada. Na mesma linha, Sarlet (2019, p. 212) sugere que a autodeterminação informacional é central para os direitos da personalidade e, portanto, a necessidade de proteção legal suficiente contra o uso intensivo de informações

O marco regulatório explícito da privacidade neste domínio é relativamente novo e só foi estabelecido desde 2018 com a promulgação da LGPD que estabelece princípios, direitos e deveres para governar o tratamento de informações pessoais. É de fato um avanço significativo, mas a LGPD também é um produto de aplicações bastante diferentes projetadas em inteligência artificial. Bioni (2021, p. 102) destaca que o papel do consentimento como justificativa para o tratamento de dados não é suficiente em situações de coleta massiva de dados e inferência algorítmica.

Pereira e Rocha (2020, p. 77) sugerem que a opacidade dos sistemas automatizados, “a chamada 'caixa preta algorítmica’”, mina diretamente a transparência e a explicabilidade garantidas no Artigo 20 da LGPD. Essa situação coloca a advocacia sob uma luz diferente de desafio. Advogados têm realizado cursos individualizados e conjuntos que são uma resposta para defender o titular dos dados (para proteger o titular dos dados, inclusive na situação acalorada de vazamentos de dados/privacidade/uso indevido).

Nesta área, os advogados têm a ação coletiva em seus próprios assuntos e ações coletivas para salvar sujeitos que foram prejudicados por isso, tanto legalmente quanto de outra forma, buscando danos morais, físicos em violação de perda pessoal ou patrimonial no caso de as informações pessoais serem divulgadas ao público.

Casos simbólicos ilustram as fraquezas das práticas de segurança e os desafios de responsabilizar os atores envolvidos na violação de dados de 2018 no Banco Inter e a exposição de dados de milhões de usuários pela Serasa em 2021 fornecem dois casos poderosos a esse respeito. Como Mendes e Doneda (2021, p. 156) observam, a advocacia deve buscar uma interpretação protetiva da LGPD que aceite a vulnerabilidade informativa do indivíduo e acomode hipóteses de responsabilidade objetiva.

Além da ação judicial, a advocacia tornou-se mais relevante como um ato preventivo, particularmente em aspectos como conformidade digital. Escritórios de advocacia criaram programas de auditoria algorítmica, cláusulas contratuais de proteção de dados e due diligence tecnológica no processo de fusão e aquisição. Essas ações são projetadas para limitar o risco de violação e reforçar a governança digital nas organizações.

Assim como Zuboff (2020, p. 131) argumenta, a exploração generalizada de dados e a nova forma de capitalismo de vigilância implicam um novo pacto de governança informacional que pode conter abusos por grandes corporações digitais. A advocacia medeia entre a inovação tecnológica e os direitos básicos garantidos pelas regras e ordem do relacionamento.

Em segundo lugar, surgem questões importantes, no caso do uso de ferramentas de IA para advocacia, quando as considerações éticas e diretrizes que regem o campo colidem. Prática: software de jurimetria, análise de documentos e

previsão de sentenças já fazem parte da prática profissional, mas devem ser usados sem sacrificar o sigilo profissional e proteger os dados confidenciais dos clientes.

Mendes e Bioni (2021, p. 230) observam que "a advocacia não pode terceirizar sua responsabilidade ética para as máquinas" e, portanto, os advogados ainda são responsáveis por preservar a confidencialidade (seja por meios tecnológicos). Este debate serve para destacar a necessidade de a Ordem dos Advogados do Brasil (OAB) facilitar a regulamentação da IA na prática do direito de acordo com certos limites definidos.

A advocacia também é interlocutora em questões institucionais e político-legais. Profissionais têm participado de consultas públicas organizadas pela Autoridade Nacional de Proteção de Dados (ANPD), têm trabalhado juntos no desenvolvimento de normas setoriais e têm desempenhado um papel nos blocos de construção da jurisprudência protetiva no Judiciário.

Da mesma forma, Pereira e Rocha (2020, p. 89) sustentam que a advocacia deve ser central para a ação coletiva estratégica para enfrentar as práticas abusivas da IA, para contrabalançar os desequilíbrios de poder informacional entre indivíduos e grandes empresas.

Uma análise alternativa do impacto do papel da advocacia no contexto de violações de dados por sistemas de IA é outra consideração que é de natureza comparativa. No cenário internacional, o progresso na regulamentação da IA é notável, com um foco renovado particularmente no Ato de Inteligência Artificial da União Europeia de 2021. Este sistema regulatório visa estabelecer categorias de risco para sistemas de IA que especificam requisitos de transparência, explicabilidade e governança para sistemas que atendem à classificação de "alto risco".

Isso está muito em desacordo com a experiência brasileira, onde a LGPD não define que tipo de impacto está sendo exercido em casos com alguma variante dos algoritmos que geram incerteza jurídica e amplificam os desafios da advocacia para empresas envolvidas na defesa de titulares de dados.

Pereira e Rocha (2020, p. 93) argumentam que quando não há tais limites e diretrizes, pode ser difícil construir as estratégias legais que importam, então, por sua vez, os advogados dependerão de interpretação principiológica e analogia com instâncias estrangeiras.

Enquanto nos Estados Unidos da América não há uma lei federal sobre proteção de dados, algumas leis estaduais, como a Lei de Privacidade do Consumidor da Califórnia (CCPA), impõem responsabilidades às empresas pela coleta e uso de informações pessoais. Advogados americanos têm sido empregados nesse espaço não apenas para litígios, mas também para aconselhar reguladores, aconselhando empresas a se moverem dentro de um mosaico normativo fragmentado. Esta experiência destaca que a advocacia brasileira terá que se concentrar em uma prática mais multidisciplinar, orientada pela análise de riscos regulatórios e pela prevenção de litígios em ambientes altamente tecnologizados.

Mesmo que a ANPD seja central para a regulação no Brasil, ela tem consistentemente enfrentado dificuldades com limites estruturais e de escopo. Mendes e Bioni (2021, p. 247) observam que a advocacia deve preencher essas lacunas com litígios que aprimorem a jurisprudência e fortaleçam entendimentos protetivos em questões de IA. É por isso que advogados que defendem clientes sob a lei de ação coletiva contra grandes plataformas digitais defendem não apenas direitos individuais, mas também ajudam a construir um cenário jurídico mais seguro e equilibrado.

E essa é outra razão pela qual os advogados nesse setor se destacam na operação de negócios, devido à dimensão preventiva da advocacia que se torna realmente central. Em um mercado cada vez mais competitivo, a adesão à LGPD e às práticas internacionais de proteção de dados tornou-se um diferencial estratégico. Os advogados devem elaborar políticas de privacidade apropriadas e regras de conduta, além de estabelecer programas de treinamento interno para organizações na coleta ética de dados.

Há um novo apetite por auditorias independentes de algoritmos que testem se os sistemas aderem a princípios de não discriminação e respeito à privacidade. Tais atividades não apenas minimizam a exposição das empresas a litígios, mas também elevam significativamente o papel da advocacia preventiva, o novo parceiro estratégico das organizações que estão se transformando digitalmente.

Outra questão é a posição do advogado na educação digital. Devido à complexidade das intervenções de IA, os profissionais do direito não podem mais ser apenas proficientes em legislação, mas também devem servir como tradutores de princípios técnicos para clientes e o judiciário. Doneda (2019, p. 91) destaca que

termos técnicos de ciência de dados devem ser reformulados em termos jurídicos para proteger os direitos primários dos titulares. Essa função pedagógica da advocacia é inestimável em processos legais envolvendo evidências digitais complexas, onde o funcionamento de um algoritmo pode ser crucial para o desfecho do caso.

Agora, a ênfase sobre onde recai o ônus da prova quando a IA viola dados merece uma pausa. A opacidade dos algoritmos torna praticamente impossível para o titular justificar como essa informação foi usada em uma decisão automatizada específica.

Nesse contexto, Mendes e Doneda (2021, p. 189) defendem a adoção da inversão do ônus da prova, que funciona como no atual Código de Defesa do Consumidor, com o controlador sendo responsável por demonstrar a conformidade de seus processos. Nesse contexto, a advocacia torna-se crítica em sua aplicação das leis para solicitar tais medidas: tratamento mais democrático de pessoas vulneráveis e grandes empresas de tecnologia.

Além da ação judicial e preventiva, a advocacia deve reconsiderar suas práticas à medida que os profissionais usam ferramentas de IA como parte de suas rotinas diárias. O uso de software de análise de documentos, plataformas de previsão de sentenças e sistemas de jurimetria oferecem potencial de eficiência, mas introduzem dilemas éticos. Sarlet (2019, p. 340).

Portanto, afirma que "a ética profissional deve prevalecer sobre a lógica da eficiência", e, como resultado, a IA usada pela advocacia deve ser relegada a uma posição de respeito ao sigilo, confidencialidade e dignidade do cliente. Isso significa que o advogado deve estar atento às capacidades de tal ferramenta, para que não coloquem decisões legais que precisam da habilidade humana em destaque com uma máquina.

Novos casos no Brasil fornecem evidências de adaptação quando se trata de advocacia. Em 2020, uma ação civil pública foi movida contra uma empresa de tecnologia que implantou sistemas de reconhecimento facial em espaços públicos sem o consentimento dos cidadãos. O caso focou não apenas na legalidade desses conjuntos de dados biométricos, mas também nos critérios vagos aplicados à operação do algoritmo.

Os advogados que representaram o caso enfatizaram que era vital garantir desde cedo que o direito à explicabilidade incluído na LGPD estivesse em vigor, mas

que isso era necessário desde o início. Este caso ilustra as maneiras pelas quais a advocacia pode ser protagonista em um debate entre inovação tecnológica e a salvaguarda de direitos.

A longo prazo, a advocacia brasileira terá que estar pronta para abordar regulamentações específicas em torno da IA, às quais o público brasileiro terá que se acostumar nos anos de legislação relacionada à regulamentação. A tendência global indica a implementação de regras regulatórias setoriais para abordar aspectos de alto impacto, como saúde, segurança pública e finanças.

Nessa situação, os advogados devem não apenas "dar sentido a essas novas normas", mas também "ser incluídos em sua constituição", por meio de associações de classe, órgãos de pesquisa e cooperação com agências reguladoras. O protagonismo da advocacia dominará e garantirá que a regulamentação da inteligência artificial no Brasil seja construída sobre a base dos direitos fundamentais, onde a lógica econômica não substitui o valor da privacidade e da dignidade humana.

Portanto, o papel da advocacia em responder a violações de dados por IA é multifacetado, tendo implicações contenciosas, preventivas, éticas, educativas e institucionais. A situação é de oportunidades, mas também uma série de desafios que têm o potencial de aprimorar a prática jurídica.

Nesse sentido, apresentando-se como uma força para o bem, a advocacia não apenas representa a proteção dos direitos individuais, mas também constrói uma arquitetura de proteção de dados robusta que é capaz de enfrentar tecnologias cada vez mais rápidas. Como Zuboff observa, construir um futuro humano contra o edifício do poder algorítmico depende da capacidade de resistir aos abusos do capitalismo de vigilância, e a advocacia está no coração dessa resistência (2020, p. 274).

2.2 A EVOLUÇÃO DOS SISTEMAS JUDICIAIS ATUAIS PARA RISCO, DISRUPÇÃO E REPARAÇÃO DE DANOS EM CASOS DE ALGORITMOS

O debate sobre a adequação dos processos legais atuais para gerenciar os riscos de responsabilidade, preempção e reparação de danos associados aos algoritmos está entre os mais difíceis e desafiadores de enfrentar no direito atual. Esses desenvolvimentos da IA e seu uso em grandes áreas ricas em dados expuseram a inadequação do sistema jurídico brasileiro em lidar com transgressões que estão fora dos modelos clássicos de infrações civis e administrativas. Ao mesmo

tempo, esse cenário exige uma reconfiguração das próprias funções de advocacia, regulamentação e jurisprudência.

Do ponto de vista constitucional da Constituição Federal de 1988, a proteção de dados pessoais é sustentada diretamente, particularmente pelo Artigo 5º, incisos X e XII, que garantem a inviolabilidade da intimidade, da vida privada e da confidencialidade das comunicações, e pelo inciso LXXIX, inserido pela Emenda Constitucional nº 115/2022, que declarou explicitamente que a proteção de dados é um direito fundamental autônomo.

Esse reforço normativo solidificou o princípio da autodeterminação informacional como um elemento central dos direitos da personalidade. Esse reconhecimento, no entanto, será prático, mas não pode ser tomado em sua totalidade, pois o efeito prático desse reconhecimento dependerá de instrumentos legais e institucionais capazes de traduzir esses princípios em mecanismos adequados de responsabilidade e reparação (o que não é totalmente verificado).

Como marco regulatório, a LGPD é essencial, pois impõe deveres de transparência, proporcionalidade, segurança e não discriminação. O Artigo 42 confere ao controlador e operador uma responsabilidade civil objetiva, o que é um avanço, pois não exige que se prove culpa em muitos casos.

Quanto a lei, no entanto, enfrenta exceções em casos que apresentam resultados erráticos, e até que ponto algoritmos que desenvolvem modelos de aprendizado contínuo podem ser processados por decisões tomadas por agentes que os agentes ou mesmo os desenvolvedores não conseguem apreciar.

Além disso, não existem regras precisas sobre "dados inferidos", os tipos, perfis e probabilidades gerados por informações originais, o que leva a uma área cinzenta, na qual tais dados poderiam ser usados para determinar as trajetórias de vida do titular, deixando-o com pouco controle direto sobre a coleta e utilização desses dados.

A prevenção, prevista na LGPD com ferramentas como Relatórios de Impacto à Proteção de Dados Pessoais (Art. 38), privacidade por design e privacidade por padrão, permanece ineficaz no Brasil. Esses instrumentos requerem regulamentação e supervisão rigorosa para funcionar.

A ANPD, embora seja a mais influente, também está sujeita a restrições significativas de estrutura e pessoal, o que prejudica sua capacidade de garantir o monitoramento dos padrões de mercado, administrar penalidades administrativas e

cultivar um ambiente de conformidade.

Na ausência de plataformas comuns que permitam a certificação e auditoria algorítmica, empresas e órgãos públicos tendem a se restringir a políticas formais de proteção, sem melhorar significativamente os riscos fundamentais associados aos sistemas de IA.

A reparação de danos em aplicações algorítmicas também é altamente problemática. O sistema jurídico brasileiro prevê tanto danos materiais quanto morais, incluindo aqueles para indivíduos e grupos. Entretanto, medir o dano é difícil em casos de danos graves ou intangíveis, como preconceitos algorítmicos ou oportunidades perdidas de decisões automatizadas. Instâncias proeminentes, como o vazamento de dados pelo Banco Inter (2018) e a exposição de dados de milhões de consumidores pela Serasa (2021), demonstram que a redenção individual não pode corresponder à escala do dano coletivo.

Em tais circunstâncias, a ação civil pública emerge como um dispositivo chave, mas não necessariamente um usado mais amplamente em casos de proteção de dados do que ainda é frequentemente negligenciado, subfinanciado e subinvestido nessa ferramenta que corroe grande parte da resposta sistêmica da lei.

Outra coisa importante é a prova contundente. A opacidade dos algoritmos torna quase impossível para um titular demonstrar como seus dados foram usados ou que sustentaram qualquer decisão dada. Como Mendes e Doneda (2021) defendem um regime mais protetor, permitindo que o ônus da prova seja invertido, com o controlador sendo obrigado a mostrar que seus processos estão em conformidade.

A referida proposta é semelhante ao modelo de responsabilidade do Código de Defesa do Consumidor e visa reconciliar as relações entre os vulneráveis e as grandes corporações digitais. No entanto, como isso é implementado depende de uma construção judicial progressiva ou de uma positivação legislativa específica, nenhuma das quais ainda aconteceu. Lições da perspectiva comparativa.

A experiência comparativa fornece lições importantes. Além do Regulamento Geral de Proteção de Dados (GDPR), o ato de IA dentro da União Europeia está desenvolvendo classificações de risco e estabelece requisitos para explicabilidade, auditabilidade, certificação e regulamentação na classe acima de sistemas e os mecanismos de controle sobre esses sistemas.

Nesse sentido é uma estratégia que visa não apenas corrigir essas falhas, mas

também evitá-las de acontecer em primeiro lugar, proporcionando o tipo certo e um grau adequado de regulamentação sobre o progresso tecnológico e da melhor maneira possível para reter a segurança dos direitos básicos do país.

Embora não haja uma lei federal específica nos EUA, leis estaduais como a CCPA na Califórnia já criam obrigações legais relevantes (proteção de dados), bem como o direito do consumidor de saber quais dados estão sendo coletados e o direito de exigir que sejam excluídos. Embora seja fragmentada, essa experiência reforça a importância da responsabilidade ex-ante e da liberdade dos titulares de escolher quais dados são mantidos.

As perspectivas futuras dos aparatos legais no Brasil dependem de uma combinação de três fatores; fortalecimento institucional da ANPD, consolidação da legislação anterior relacionada a questões de IA e proteção de dados e legislação específica relacionada à governança algorítmica sendo aprovada como parte de um quadro coerente. Até que esses avanços aconteçam, a advocacia é de fato um ator básico.

Em território propenso a conflitos, é exigido pelo advogado invocar princípios constitucionais e de consumo para exigir pagamento e corresponsabilidade pelas cadeias de processamento de dados. Um advogado de prática profissional no campo preventivo atua como parceiro organizacional, projetando programas de conformidade e cláusulas de proteção contratual, auditorias de algoritmos e conduzindo due diligence.

Além disso, a profissão jurídica atua como árbitro e facilitador na tradução do conhecimento técnico para a linguagem jurídica, capacitando instituições e promovendo a cultura de governança digital.

Assim, a eficácia dos mecanismos legais existentes para casos algorítmicos não é tão forte quanto costumava ser, mas pelo menos não é zero. Um marco legal com fundamentos sólidos que pode impulsionar a defesa dos direitos é a LGPD, o Marco Civil da Internet e o Código de Defesa do Consumidor (CDC). Mas a falta de requisitos legais definidos para IA, o desafio da opacidade algorítmica e a natureza institucionalmente frágil da ANPD tornam essas ferramentas menos úteis na prática.

A combinação de uma profissão jurídica aprimorada, uso de melhores práticas internacionais e evolução legislativa serve como um guia prático para o Brasil na criação de um cenário legal capaz de enfrentar e responder adequadamente a tais

violações legais induzidas por sistemas algorítmicos.

Nesse viés, a verdadeira tarefa é garantir que a inovação tecnológica não prejudique os direitos fundamentais e, ao mesmo tempo, faça isso por meio do diálogo, garantindo que possamos construir um futuro digital ético, transparente e baseado na dignidade humana.

2.3 O IMPACTO DOS VAZAMENTOS DE DADOS NO SETOR PÚBLICO BRASILEIRO E SUAS IMPLICAÇÕES LEGAIS À LUZ DO PAPEL DA PROFISSÃO JURÍDICA NA ERA DIGITAL

A gestão de dados pessoais no setor público brasileiro apresenta uma das ameaças mais urgentes no campo da proteção da privacidade e segurança da informação. À medida que as instituições públicas aceleram a digitalização dos serviços e a integração de sistemas, a quantidade de dados sensíveis sob sua custódia torna-se cada vez mais massiva, o que, por sua vez, aumenta o risco de incidentes de segurança.

Este contexto revela uma tensão constante entre dois princípios igualmente legítimos e aplicáveis: a visibilidade e transparência exigidas para a administração pública e a proteção dos dados pessoais dos cidadãos. Agora, com a promulgação da LGPD, o Brasil implementou uma lei de proteção de dados que se aplica a organizações do setor público e privado.

A LGPD esclarece em seu artigo 46 que os agentes de tratamento de dados devem implementar medidas de segurança técnicas e administrativas para proteger os dados pessoais de acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou disseminação.

Em comparação, o Artigo 48 prevê que o controlador deve alertar a ANPD e o titular dos dados que incidentes de segurança podem ocorrer, representando risco ou dano significativo (Brasil, 2018). Certamente, na prática, essas disposições tiveram suas falhas, principalmente no setor público.

Nos últimos quatro anos, os vazamentos de dados governamentais aumentaram mais de vinte vezes, de acordo com uma pesquisa realizada pela Revista Veja (2024), e a administração pública tornou-se agora o setor mais afetado por incidentes de segurança no país.

O problema é agravado pela ausência de uma cultura organizacional

relacionada à proteção de dados, falta de infraestrutura para mecanismos estruturados de governança digital e ausência de recursos técnicos para estabelecer medidas de segurança à altura, considerando o volume de informações processadas e a sensibilidade.

Um exemplo de destaque é o evento de vazamento de dados em que cerca de 220 milhões de brasileiros foram afetados, documentado em 2021, e no qual a ANPD continua uma investigação. O caso revelou bancos de dados massivos, incluindo CPF, informações de registro e também dados sensíveis (renda, localização etc.), conforme relatado em comunicado oficial (ANPD, 2021).

Dito isso, embora o vazamento tenha ocorrido de forma privada, teve consequências públicas porque eram dados públicos de todos os brasileiros que agora se aplicavam a toda a população brasileira e incluíam informações fornecidas originalmente a agências estaduais.

Tornou-se uma questão nacional e mundial e demonstrou a importante necessidade de aprimorar a colaboração entre o setor público e privado na proteção das informações pessoais. Mas também há incidentes envolvendo a administração pública. Então, um incidente de segurança que impactou cerca de 300.000 titulares de dados foi descoberto, por exemplo, em 2024, a Secretaria de Estado da Saúde de Santa Catarina (SES-SC) foi subsequentemente sancionada pela Autoridade Nacional de Proteção de Dados.

A agência foi considerada responsável por não comunicar efetivamente o incidente aos titulares dos dados e à própria ANPD, violando os artigos 38 e 49 da LGPD relacionados ao relatório de impacto de proteção de dados no contexto das responsabilidades específicas dos agentes públicos.

Conforme declarado no relatório da autoridade, houve negligência na adoção de medidas preventivas e falta de transparência no tratamento dos riscos envolvidos (ANPD, 2024). As penalidades incluíram a publicação de um aviso público por 90 dias, comunicação individual aos cidadãos que foram afetados e o estabelecimento de um cronograma para corrigir falhas.

O caso de Santa Catarina é ilustrativo porque mostra que mesmo serviços públicos que desempenham funções críticas para a cidadania podem ser seriamente prejudicados no controle e salvaguarda de dados pessoais.

A fraqueza dos sistemas estaduais é exposta, juntamente com a ausência de

procedimentos de segurança da informação bem definidos para a confidencialidade dos cidadãos, com consequências negativas não apenas para a privacidade dos cidadãos, mas também para a confiança social na administração pública.

Além disso, o aumento da inter-relação de bancos de dados governamentais e sistemas automatizados habilitados por inteligência artificial exacerba os riscos, pois decisões administrativas correm o risco de serem tomadas com base em dados errados, corrompidos ou não acreditados.

Esta análise legal desses incidentes mostra que, no contexto de dados pessoais, o Estado atua como controlador, o que significa que a responsabilidade é atribuída também aos agentes privados. Nesses casos, a responsabilidade civil do setor público é objetiva, conforme definido pelo artigo 37, § 6 da Constituição Federal, exigindo apenas prova de dano e nexo causal para que surja o dever de indenizar.

Além disso, em uma decisão recente, o Tribunal de Justiça do Distrito Federal e Territórios (TJDFT) reconheceu a responsabilidade do Estado no caso de vazamento de dados pessoais e afirmou que se tornou responsabilidade da administração pública garantir a integridade das informações que armazena e processa (TJDFT, 2025).

O papel da profissão jurídica (do advogado) nesses episódios torna-se exponencialmente mais significativo. Do ponto de vista da prevenção, o advogado deve aconselhar as instituições públicas sobre como realizar iniciativas de conformidade em relação à proteção de dados; elaborar relatórios de impacto e implementar políticas internas de segurança da informação.

Dessa forma, espera-se também garantir a conformidade com os requisitos legais na LGPD, incluindo a comunicação de incidentes e a transparência do processamento de informações.

Na esfera contenciosa, o advogado tem um papel crucial na promoção dos direitos dos titulares de dados preocupados, seja individualmente ou em grupo, na busca de indenizações por danos morais e materiais e na execução de processos administrativos que a ANPD inicia.

Além disso, a profissão jurídica pode usar a aplicação estratégica de litígios para reforçar a jurisprudência protetora em casos de proteção de dados para integrar a responsabilidade do Estado e a obrigação de prevenção.

Quanto a ação legal, ela não deve apenas visar a reparação, apontam Mendes

e Doneda (2021); deve esforçar-se para construir uma cultura institucional que se preocupe mais com a manutenção dos direitos informacionais; deve também tentar construir novos tipos de estruturas para proteger informações sobre direitos informacionais.

Assim destaca a necessidade de advogados sugerirem governança digital no setor público por meio do uso de sistemas de governança digital projetados para apoiar a auditoria de sistemas de agências públicas, treinar servidores públicos e mecanismos para rastrear dados processados por tecnologias de IA.

Outra consideração em torno do vazamento de dados no setor público é o potencial para mudança legislativa. Projetos como o Projeto de Lei nº 1876/2023, em um momento em que estão sendo discutidos na Câmara dos Deputados, preveem a necessidade de tornar a divulgação pública geral de incidentes de segurança em que ocorreu o uso de informações pessoais um requisito fundamental sob a lei, como meio de aumentar a transparência e fornecer uma camada extra de responsabilidade aos atores estatais (Câmara dos Deputados, 2023).

Entende-se que esta é uma medida que precisa ser complementada por políticas de prevenção bem-sucedidas, para que a divulgação não sirva apenas para encontrar erros administrativos, mas também para desempenhar um papel como ferramenta pedagógica que educa e melhora as instituições.

O problema também está intimamente ligado à influência da inteligência artificial na administração pública. Numerosos sistemas automatizados dependem de enormes bases de dados para suas operações e sua qualidade e segurança são essenciais para a geração confiável de dados.

Algoritmos podem reproduzir distorções, introduzir discriminação e violar direitos fundamentais quando ocorre um vazamento ou alteração de dados. Portanto, o advogado mediará o progresso tecnológico e a proteção legal, permitindo o uso de IA pelo Estado, de forma ética, transparente e em conformidade com os princípios da LGPD.

Com base nessas constatações, não podemos esconder o fato de que vazamentos de dados no setor público brasileiro não são simplesmente o resultado de erros tecnológicos, mas o resultado de um sistema que ainda não está totalmente desenvolvido em termos de instituições e capacidades técnicas.

Os atos proativos da profissão jurídica podem contribuir significativamente para

o estabelecimento de práticas de governança pública que aderem aos princípios de proteção de dados e proteção da sociedade contra as falhas do estado.

Como resultado, a administração pública precisa investir em infraestruturas de segurança, credenciais de funcionários e melhorar a cultura de privacidade além do ambiente legal existente que precisa se adaptar às complexidades em evolução da era digital.

Assim, o estudo dos vazamentos de dados no setor público brasileiro mostra que o efeito da LGPD não é apenas uma questão de dispositivos normativos, mas também que requer uma ação integrada entre o Estado, a profissão jurídica e os órgãos reguladores.

A exposição das instituições públicas a incidentes de segurança destaca a necessidade de uma profissão jurídica especializada e ética para supervisionar, defender e litigar em linha com os direitos informacionais.

Manter a evolução tecnológica e a gestão de dados públicos em equilíbrio com a salvaguarda da dignidade humana para que todos os seres humanos possam existir em segurança, transparência e confiabilidade juntos no mundo digital é o desafio que enfrentamos hoje.

3 CONSIDERAÇÕES FINAIS

Este estudo teve como objetivo examinar os desafios apresentados pelas inteligências artificiais (IA) à proteção de dados no Brasil com base no arcabouço legal e na posição da profissão jurídica.

As conclusões validam o argumento original: apesar das conquistas da LGPD, na sociedade brasileira o arcabouço normativo é muito fraco para lidar com as peculiaridades da IA em geral e a opacidade algorítmica e a complexidade na responsabilização em particular.

O estudo mostrou que o papel do trabalho jurídico na era digital precisa de uma reconfiguração de habilidades. Onde o advogado em exercício de sua função, deve estar ciente sobre o uso e exercício de ferramentas algorítmicas e ter condições de compreender o funcionamento e as consequências que o uso indevido das IAs pode trazer tanto para os seus clientes quanto para a sociedade como um todo. Sendo um pilar essencial na proteção de dados e da sociedade brasileira contemporânea.

Através de conhecimento técnico multidisciplinar, o profissional jurídico precisa confrontar a "caixa preta algorítmica" com prevenção por meio de conformidade digital, bem como repressão, buscando compensação por danos e reversão do ônus da prova em tribunal.

Porém a eficácia limitada das ferramentas legais para responsabilização, prevenção e reparação (o terceiro tópico) é prejudicada por problemas probatórios e pela ausência de critérios claros na LGPD para governar algoritmos de alto risco.

Além disso, o exame dos vazamentos de dados do setor público (o quarto) destacou a necessidade de uma governança estatal ainda mais forte, revelando que a suscetibilidade do Estado a violações traz consigo implicações legais e sociais graves, exigindo ação legal contundente em nome dos direitos críticos.

No geral, responder às questões de preservação de dados nas circunstâncias da IA requer cooperação. A reforma legislativa é importante na regulamentação e transparência do risco algorítmico, no empoderamento institucional da ANPD e no treinamento contínuo de uma força de trabalho jurídica especializada, ética e proativa.

Portanto, somente depois disso será possível não permitir que a inovação tecnológica tenha precedência sobre os direitos fundamentais e a dignidade humana no espaço digital.

REFERÊNCIAS

AGÊNCIA NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Portal institucional**. Brasília, DF, [2025]. Disponível em: <https://www.gov.br/anpd>. Acesso em: 12 mai. 2025

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União: seção 1**, Brasília, DF, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011- . Acesso em: 12 mai. 2025

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Lei Geral de Proteção de Dados – LGPD). **Diário Oficial da União: seção 1**, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 12 de mai. 2025

ANEXO A – COMPROVANTE DE SUBMISSÃO

01/11/2025, 17:10

Gmail - [RDU] Agradecimento pela submissão



Lucas Delmondes <ldelmondes03@gmail.com>

[RDU] Agradecimento pela submissão

1 mensagem

ALEXANDRE AUGUSTO BATISTA DE LIMA via Portal de Revistas <pen-bounces@emnuvens.com.br> 1 de novembro de 2025 às 13:40
Responder a: ALEXANDRE AUGUSTO BATISTA DE LIMA <alexandre.lima@uninovafapi.edu.br>
Para: Lucas Delmondes Martins Lima <ldelmondes03@gmail.com>

Lucas Delmondes Martins Lima,

Agradecemos a submissão do trabalho "DESAFIOS DA PROTEÇÃO DE DADOS PESSOAIS NA ERA DAS INTELIGÊNCIAS ARTIFICIAIS: limites do ordenamento jurídico e da atuação da advocacia" para a revista Revista de Direito UNINOVAFAPI.

Acompanhe o progresso da sua submissão por meio da interface de administração do sistema, disponível em:

URL da submissão: <https://uninovafapi.emnuvens.com.br/revinterdireito/authorDashboard/submission/2286>

Login: lucasdelmondes03

Em caso de dúvidas, entre em contato via e-mail.

Agradecemos mais uma vez considerar nossa revista como meio de compartilhar seu trabalho.

ALEXANDRE AUGUSTO BATISTA DE LIMA

UNINOVAFAPI <http://revistainterdisciplinar.uninovafapi.edu.br/index.php/revinterdireito> Revista de Direito