Centro de Documentação e Pesquisa | OABRJ

Direito e Inteligência Artificial: Desafios Jurídicos do Processamento de Linguagem Natural no Uso de Dados Pessoais

Angela Dias Mendes
Pós-doutorado/Universidade de Coimbra

Gabriel Fortuna Rodrigues
Graduação/Universidade do Estado do Rio de Janeiro

Resumo

O avanço da Inteligência Artificial (IA) tem promovido transformações em diferentes campos do conhecimento, impulsionando a convergência entre áreas científicas e o surgimento de soluções inovadoras voltadas à melhoria da vida humana e social. Nesse cenário, o Processamento de Linguagem Natural (PLN) destaca-se como uma das subáreas mais relevantes da IA, ao possibilitar que máquinas realizem tarefas complexas de compreensão, análise e produção de linguagem, com sofisticação. No campo jurídico, sua adoção vem se expandindo em tribunais, escritórios de advocacia e órgãos públicos, intensificando o uso de dados em larga escala. Contudo, esse processo também suscita importantes desafios éticos e jurídicos, sobretudo quanto ao tratamento de dados pessoais sensíveis utilizados no treinamento desses modelos. À luz da Lei Geral de Proteção de Dados (LGPD), torna-se essencial refletir sobre os riscos que o uso indiscriminado dessas informações pode representar à privacidade, à liberdade e à dignidade da pessoa humana. Assim, o presente artigo propõe uma análise geral dos principais desafios jurídicos relacionados ao uso de dados pessoais no treinamento de modelos de PLN.

Palavras-chave: Inteligência Artificial; Processamento de Linguagem Natural; Proteção de dados pessoais; LGPD; Ética; Direito e tecnologia.

ABSTRACT

The advancement of Artificial Intelligence (AI) has promoted transformations in different fields of knowledge, driving convergence between scientific areas and the emergence of innovative solutions aimed at improving human and social life. In this scenario, Natural

Language Processing (NLP) stands out as one of the most relevant sub-areas of AI, enabling machines to perform complex tasks of understanding, analyzing, and producing language with sophistication. In the legal field, its adoption has been expanding in courts, law firms, and public bodies, intensifying the use of data on a large scale. However, this process also raises important ethical and legal challenges, especially regarding the treatment of sensitive personal data used in the training of these models. Given the General Data Protection Law (LGPD), this is crucial to consider how the uncontrolled use of such information could pose risks to individual privacy, freedom, and human dignity. Thus, this article proposes a general analysis of the main legal challenges related to the use of personal data in the training of NLP models.

Keywords: Artificial Intelligence; Natural Language Processing; LGPD; ethics; law and technologies.

1. Introdução

O avanço exponencial da Inteligência Artificial (IA), especialmente nas últimas duas décadas, vem provocando mudanças significativas em diversas áreas do conhecimento.[1] As ciências convergem seus conhecimentos, transformando mutuamente os conhecimentos já solidificados no tempo e fazendo surgir inovações jamais imaginadas. Mão biônica devolve o sonho daqueles que outrora perderam o movimento das mãos, exoesqueletos permitem pessoas voltem a andar. Hoje, é possível entrelaçar saberes como a engenharia genética com a biologia e a robótica, entre outras, criando um mundo de sonhos e esperanças para a melhoria da qualidade de vida humana e social.

Nesse sentido, dentre as subáreas da IA, em especial o Processamento de Linguagem Natural (PLN) ganhou destaque ao proporcionar que as máquinas imitem o comportamento humano. Assim, elas passam a compreender a forma de pensar e de fazer humana e, ultimamente, apresentam um nível alto de sofisticação nessa tarefa. Não é difícil ver análises de uma grande massa de dados para gerar textos e decisões.

No contexto jurídico, o PLN, progressivamente, vem sendo adotado por diversas áreas, destacando-se, no Brasil, pelos Tribunais Superiores. Além deles, escritórios de

[1] BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (coord.). *Regulação Digital:* Perspectivas Jurídicas sobre Tecnologia e Sociedade. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024. 363p.

advocacia, procuradorias e outros setores seguem o caminho da automação, sinalizando um futuro com uma única certeza, por enquanto, que é o uso cada vez maior de dados.

Tal cenário, naturalmente indefinido, gera incertezas quanto ao uso desses dados. Essa transformação traz consigo inúmeros desafios de ordem ética e jurídica relevantes, sobretudo no que se refere à privacidade dos dados utilizados para o treinamento desses modelos. A maior parte dos modelos atuais de PLN exige grandes volumes de dados, sendo que estes são formados por dados sensíveis. Esses dados, quando são utilizados de forma ampla e sem transparência, limites éticos e critérios bem definidos, podem colocar em risco a dignidade da pessoa humana.

A Lei Geral de Proteção de Dados (LGPD), em seu artigo 5º, II, traduz o conceito de dado pessoal sensível como aquele relacionado à

> [...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.[2]

Desse modo, tem a Lei "[...] o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.", como estipulado em seu artigo 1º.[3]

Nesse contexto, o uso do PLN redesenha o fato jurídico e desafia esse profissional a buscar conhecimentos que vão além do Direito para que possam exercer a correta assistência no mundo dos negócios. Desta forma, o presente texto, não tem a intenção de cansar o leitor com aprofundamentos jurídicos ou matemáticos que vão além da sua necessidade. Pelo contrário, ele apresenta uma análise mais geral, trazendo à baila alguns dos principais desafios jurídicos associados ao uso de dados pessoais no treinamento de modelos de PLN, à luz da legislação vigente e das limitações técnicas da tecnologia. E propõe alguns caminhos jurídicos e técnicos para mitigar os riscos identificados.

2. Processamento de Linguagem Natural: arquiteturas, desafios regulatórios e a práxis na era da Inteligência Artificial

---

[2] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 22 mar. 2026.

[3] _____ idem.

O Processamento de Linguagem Natural é uma subárea da IA que busca capacitar máquinas a compreender e gerar linguagem humana de forma significativa. Os modelos de PLN mais avançados atualmente utilizam arquiteturas de redes neurais profundas, como os transformadores, para representar palavras e frases em vetores multidimensionais. A transição de sistemas baseados em regras para modelos probabilísticos e, mais recentemente, para arquiteturas de aprendizado profundo, conhecido como *deep learning*, redefiniu os limites da interação entre o humano e a máquina. Contudo, essa evolução técnica trouxe junto inúmeros dilemas éticos, jurídicos e epistemológicos que exigem uma nova governança, muito mais sofisticada para atender com eficácia as novas exigências atuais de proteção e segurança. Além disso, ela passou a exigir uma abordagem sistêmica e multidisciplinar do tratamento desses dilemas.

Esses modelos são treinados frequentemente com grandes volumes de textos oriundos da internet e ajustam bilhões de parâmetros por meio de técnicas de aprendizado supervisionado ou auto supervisionado. A performance desses modelos está diretamente relacionada à qualidade e à quantidade dos dados utilizados em sua fase de treinamento. Dados são a matéria-prima essencial para o desenvolvimento de modelos de PLN.[4] Sem eles, é impossível capturar padrões linguísticos e semânticos necessários para que os modelos operem com precisão. Porém, essa dependência de dados levanta preocupações, sobretudo quando se consideram os dados pessoais incluídos nesses conjuntos.

Nessa arquitetura, que não é meramente semântica, as palavras e as frases não são apenas símbolos. Elas são convertidas em *embeddings*[5]*, os* vetores multidimensionais citados acima, que mapeiam as relações semânticas das frases, em um espaço matemático contínuo. Palavras com significados ou usos contextuais semelhantes são posicionadas próximas nesse espaço vetorial. Desta forma, a representação permite que os Modelos de Linguagem de Grande Porte (LLMs — *Large Language Models*) realizem inferências estatísticas complexas pela qual uma palavra deve seguir a outra.

---

[4] SAMPAIO, Aline Bessa. *Judiciário*: análise do risco de vieses algorítmicos em decisões judiciais. 2025. Dissertação (Pós-graduação em Direito) - Programa de Pós-Graduação em Direito, Universidade Federal do Ceará. Fortaleza, 2025. Disponível em: https://repositorio.ufc.br/bitstream/riufc/80882/1/2025_dis_absampaio.pdf. Acesso em: 10 dez. 2025.

[5] VASWANI, A. *et al. Attention is All You Need*. [*S. l.*]: 2017.

Como mencionado acima, muitos modelos de PLN são treinados com dados absorvidos do mundo online (*web scraping)*. Redes sociais, fóruns públicos, transcrições jurídicas e bases de dados documentais são utilizados no tratamento[6] desses dados. Ocorre que o conjunto desses dados pode conter informações pessoais, identificáveis e sensíveis. Mesmo quando há esforços para anonimização, estudos indicam que a reidentificação é possível com técnicas de *cross-referencing* e inferência estatística.[7]

A principal controvérsia jurídica relacionada ao treinamento de modelos de PLN diz respeito justamente à utilização de dados pessoais absorvidos no processo indiscriminado de tratamento. Vale dizer que, de acordo com a Lei Geral de Proteção de Dados Pessoais, que regulamenta o uso de dados pessoais no Brasil[8] e com o Regulamento Geral de Proteção de Dados da União Europeia (GDPR)[9], dado pessoal é qualquer informação relacionada a uma pessoa natural identificada ou identificável.[10]

O uso de dados sensíveis, como convicções religiosas, opiniões políticas ou informações sobre saúde, intensifica o problema, pois requer bases legais mais rígidas e cuidados especiais, conforme definido nos artigos 11 a 13 da LGPD. O tratamento dessas informações exige salvaguardas rigorosas, e sua inclusão inadvertida em modelos de PLN pode gerar danos irreparáveis aos direitos da pessoa, assim como, à imagem das instituições. Desta forma, é essencial uma governança que adote mecanismos de controle e de auditoria dos dados utilizados nesses modelos, para minimizar possíveis danos à dignidade humana e não comprometer a imagem das empresas ou das instituições envolvidas no tratamento.

---

[6] A palavra tratamento é utilizada no texto como sinônimo de qualquer ação relacionada ao dado pessoal, nela incluída, coleta, guarda, transferência etc.
[7] NARAYANAN, A et all. *Robust De-anonymization of Large Sparse Datasets.* [*S. l.*]: 2008.
[8] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 22 mar. 2026.
[9] UNIÃO EUROPEIA. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.* General Data Protection Regulation (GDPR). Bruxelas, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680. Acesso em: 22 mar. 2026.
[10] MARQUES, Daniel Silva. *Reconhecimento facial e segurança pública*: Lawethics by design como novo paradigma regulatório. Rio de Janeiro, 2025. Disponível em: https://www.bdtd.uerj.br:8443/bitstream/1/24762/2/Tese - Daniel da Silva Marques - 2025 - Completa.pdf. Acesso em: 02 dez. 2025.

Além das questões relativas à privacidade, outro desafio crítico é a limitação dos modelos de PLN na compreensão do conteúdo jurídico ou normativo. A linguagem jurídica é notoriamente densa, ambígua e contextual. Palavras e expressões têm significados que variam conforme o ramo do Direito, a época, o local e o entendimento jurisprudencial dominante.

Modelos de PLN, embora avançados, funcionam com base em padrões estatísticos, e não em raciocínio jurídico estruturado. Isso pode levar a falhas graves na interpretação de normas podendo confundir expressões ignorar o sistema legal e a ordem jurídica vigente. Utilizar esses modelos para sugerir decisões judiciais, elaborar minutas ou filtrar precedentes requer extrema cautela. Os vieses podem estar presentes, a discriminação algorítmica e erros interpretativos também, especialmente quando os modelos são tratados como infalíveis.

A mitigação dos riscos associados ao uso de dados pessoais no PLN exige uma abordagem integrada entre Direito e tecnologia. Por um lado, é imprescindível o respeito aos princípios da proteção de dados desde a concepção dos sistemas, com a chamada *privacy by design e,* por outro lado*,* a *privacy by default*, conforme estabelecido no artigo 46 da LGPD.

Do ponto de vista técnico, é necessário empregar métodos robustos para garantir a privacidade dos cidadãos, entre elas, anonimização, limite na coleta de dados ao mínimo necessário. Além disso, implementar a prática de auditorias independentes sobre os modelos utilizados, documentando de forma transparente suas fontes de dados, informações sobre a arquiteturas são práticas que demonstram a boa governança do processo.

Também é urgente criar marcos regulatórios específicos que tratem do uso de IA no Direito. A sociedade necessita de normas que, por exemplo, estabeleçam os requisitos mínimos de explicabilidade, transparência, supervisão humana e responsabilização, como proposto por Vale e Edwards[11], na análise das diretrizes europeias para decisões automatizadas.

2.1 Entre a Inovação e a Privacidade

[11] Disponível em: https://arxiv.org/abs/1803.07540.

A principal controvérsia jurídica subjacente ao treinamento de modelos de PLN de fronteira diz respeito à absorção indiscriminada de dados pessoais. Sob a égide do Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e da Lei Geral de Proteção de Dados Pessoais no Brasil (LGPD), o conceito de dado pessoal é expansivo, abarcando qualquer informação relacionada a uma pessoa natural identificada ou identificável.

Outro fato relevante que devemos destacar refere-se à base de treinamento de *datasets*. Ela geralmente é formada por dados oriundos da *web* e isso colide frontalmente com princípios gerais da proteção de dados pessoais. Quando ocorre a publicação de um documento para atender à determinações legais como a transparência, não houve a ciência, nem muito menos o consentimento para terceiros treinarem algoritmos. Os dados que ali estão não foram autorizados por seus titulares para serem parte de qualquer experimento, por isso, não há legítimo interesse das instituições nesse tratamento.

Treinamento de algoritmos de IA são revestidos de grande opacidade, o que representa um desafio para a proteção de dados na fase de treinamento. Há perigos reais de ocorrem o que alguns chamam de alucinações jurídicas reveladas no resultado do processo, embora, a IA generativa já consiga sugerir decisões judiciais, elaborar minutas complexas ou realizar jurimetria preditiva com alto nível de acerto. A automação no STF demonstra esse grau de assertividade e eficiência, por exemplo, com ferramentas que agrupam cerca de 5 mil processos em 2 minutos[12].

2.2 Governança algorítmica e algumas estratégias de mitigação de riscos

A mitigação dos riscos associados ao PLN exige uma arquitetura de governança que consiga entrelaçar soluções tecnológicas avançadas e um *compliance* regulatório estrito. Uma boa premissa pode ser adotar a *Privacy by Design* e *Privacy by Default* que garante a proteção de dados, por padrão, desde a concepção da arquitetura de rede neural e posteriormente em ajustes no sistema, conforme já explicamos em sessão anterior.

---

[12] As informações estão disponíveis no portal https://portal.STF.jus.br. Citado por MENDES, Angela et all. Inovação tecnológica no Judiciário após a Pandemia de Covid-19. In As inovações tecnológicas no Direito – O impacto nos diferentes ramos. Luiz Fux, Marco Aurélio Bezerra de Melo, Humberto Dalla Bernardina de Pinho (coords), Londrina, PR: Thoth, 2024.

Do ponto de vista técnico, as melhores práticas internacionais apontam para a superação da anonimização simples em favor de técnicas matemáticas mais recentes que possam contribuir para o aprimoramento dessa formulação. Não vamos nos ater a elas por uma questão metodológica.

No âmbito jurídico e regulatório é imperativa a consolidação de marcos normativos específicos para a IA, alinhados à abordagem baseada em risco, como o *AI Act* europeu. Tais normas devem exigir auditorias algorítmicas independentes, documentação exaustiva sobre a proveniência dos dados e a garantia de explicabilidade.

Como argumentam alguns autores, como Valle[13], para alcançar a transparência algorítmica não podemos nos limitar a abrir o código-fonte o que, aliás, pode ser ininteligível até mesmo para os especialistas devido à natureza profunda dessa elaboração neural. Segundo eles, a transparência deve ser identificada na justificativa das decisões e na manutenção do humano revendo essa decisão. Assim, é possível assegurar que a responsabilidade final pelas ações da máquina seja identificada de forma inequívoca nas instituições e indivíduos que operam o processo.

3. Considerações Finais

O uso de modelos de PLN na área jurídica representa uma inovação de grande potencial, capaz de ampliar o acesso à informação, reduzir custos e otimizar o funcionamento do sistema judicial. No entanto, os desafios jurídicos associados a essa tecnologia são igualmente significativos, principalmente no que se refere à utilização de dados pessoais no treinamento de modelos.

A análise apresentada neste trabalho destacou que, sem o devido cuidado com a privacidade dos titulares de dados, os sistemas de PLN podem reproduzir ou até mesmo ampliar violações de direitos fundamentais. A dificuldade dos modelos em interpretar corretamente a linguagem jurídica reforça a necessidade de limites claros para seu uso em atividades decisórias.

---

[13] VEALE, Michael et all. *Enslaving the algorithm: from a "Right to an Explanation" to a "Right to Better Decisions"?* Disponível em: https://arxi.org/ab/1803.07540, 2018. Acesso em: 06 jan 2026.

Como recomendação, deixamos algumas sugestões que podem contribuir para reduzir os riscos aqui apresentados: o investimento em modelos treinados com dados sintéticos, a adoção de protocolos de consentimento informado e o fortalecimento da governança algorítmica. Além disso, é essencial promover a colaboração entre juristas, engenheiros e cientistas de dados na formulação de políticas públicas e normas técnicas que orientem o uso responsável da IA no Direito com vistas a ampliar a proteção da dignidade humana guardada pela privacidade dos dados pessoais sensíveis.

Referências

BRANCO, Sérgio; TEFFÉ, Chiara Spadaccini de (coord.). *Regulação Digital:* Perspectivas Jurídicas sobre Tecnologia e Sociedade. Rio de Janeiro: Instituto de Tecnologia e Sociedade do Rio, 2024. 363p.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil. Presidência da República. Casa Civil. 1988.

BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 22 mar. 2026.

MARQUES, Daniel Silva. *Reconhecimento facial e segurança pública*: Lawethics by design como novo paradigma regulatório. Rio de Janeiro, 2025. Disponível em: https://www.bdtd.uerj.br:8443/bitstream/1/24762/2/Tese - Daniel da Silva Marques - 2025 - Completa.pdf. Acesso em: 02 dez. 2025.

MENDES, Angela Dias. *As Inovações Tecnológicas no Direito*. STF. Coord. Luiz Fux, Marco Aurélio Bezerra de Mello, Humberto Dalla de Pinho. [*S. l.*]: Ed. Thoth, p. 478, 2024.

NARAYANAN, Arvind et all. *Robust De-anonymization of Large Sparse Datasets.* [*S. l.*]: 2008.

SAMPAIO, Aline Bessa. *Judiciário*: *análise do risco de vieses algorítmicos em decisões judiciais.* 2025. Dissertação (Pós-graduação em Direito) - Programa de Pós-Graduação em Direito, Universidade Federal do Ceará. Fortaleza, 2025. Disponível em: https://repositorio.ufc.br/bitstream/riufc/80882/1/2025_dis_absampaio.pdf. Acesso em: 10 dez. 2025.

UNIÃO EUROPEIA. *Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016.* General Data Protection Regulation (GDPR). Bruxelas, 2016.

Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L0680. Acesso em: 22 mar. 2026.

VEALE, Michael et all. *Enslaving the algorithm: from a "Right to an Explanation" to a "Right to Better Decisions"?* Disponível em: https://arxi.org/ab/1803.07540, 2018.