Fé Pública e Algoritmos: O Desafio de Regular a Inteligência Artificial nos Serviços Notariais e Registrais Nas entrelinhas das IAs e LLMs, esconde-se o verdadeiro dilema entre efi...

Article · May 2025

CITATIONS
0

READS
26

3 authors, including:

Douglas Resende Maciel
Federal University of Uberlândia
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

Alexandre Cardoso
Federal University of Uberlândia
298 PUBLICATIONS **1,005** CITATIONS
SEE PROFILE

Fé Pública e Algoritmos: O Desafio de Regular a Inteligência Artificial nos Serviços Notariais e Registrais

Nas entrelinhas das IAs e LLMs, esconde-se o verdadeiro dilema entre eficiência e responsabilidade

Douglas Resende Maciel[1], Jovino Mustafa Cheik[2], Alexandre Cardoso[3]

[1] Faculdade de Engenharia Elétrica – Universidade Federal de Uberlândia - MG – Brasil – Diretor executivo e responsável por inteligência artificial na empresa NoCartorio.com
[2] Tabelião e Registrador no Estado de Minas Gerais – Estudioso e entusiasta da aplicação de tecnologia na área do direito.
[3] Faculdade de Engenharia Elétrica – Universidade Federal de Uberlândia - MG – Brasil – Professor Associado - Coordenador do Programa de Pós-graduação em Engenharia Elétrica

Resumo

O presente artigo explora os riscos associados ao emprego de inteligência artificial (IA), em especial modelos de linguagem de larga escala (Large Language Models – LLMs), nos serviços extrajudiciais brasileiros (cartórios de registros e notariais). Inicialmente, discute-se o valor estratégico dos dados mantidos por essas serventias e os perigos de vazamentos, à luz de incidentes notórios como o escândalo Cambridge Analytica, a brecha de dados do Google+ e o megavazamento brasileiro de 2021. Em seguida, explica-se o funcionamento dos LLMs e porque sua adoção indiscriminada pode expor padrões sensíveis não previstos explicitamente pelos programadores, gerando potenciais violações de privacidade e segurança. São examinados riscos específicos aos cartórios, incluindo o uso de LLMs comerciais de terceiros e a centralização de dados em plataformas nacionais como o ONR, ON-RCPN e outras centrais nacionais. Apresentam-se dois cenários ilustrativos – um hipotético, envolvendo a utilização de IA em um cartório de registro de imóveis, e um real, de espionagem internacional com uso indevido de dados do registro civil (caso revelado pela BBC News). Por fim, são propostas recomendações para um uso seguro, ético e **soberano** da IA nos serviços extrajudiciais, tais como adoção de LLMs locais, aprendizado federado, auditorias técnicas e regulamentação específica pelo Conselho Nacional de Justiça (CNJ). As conclusões reforçam a necessidade de modernização responsável, garantindo que a IA seja aliada e não uma ameaça à integridade dos sistemas registrais e notariais brasileiros.

Introdução

A inteligência artificial tem avançado rapidamente, tornando-se parte integral de múltiplos setores da sociedade. Modelos de linguagem de larga escala (LLMs), como o GPT-4, DeepSeek e outros, destacam-se por sua capacidade de gerar textos coesos e responder perguntas complexas, o que tem impulsionado seu uso em aplicações cotidianas e profissionais. No contexto jurídico e administrativo, já se observa o interesse em utilizar IA para otimizar fluxos de trabalho, realizar análises de documentos e até auxiliar na redação de peças ou pareceres. Não é diferente nos **serviços extrajudiciais** – os cartórios de notas e registros públicos – que lidam diariamente com grande volume de informações textuais e poderiam, em tese, se beneficiar de assistentes automatizados para aumentar a eficiência.

Entretanto, os cartórios exercem uma função delicada e estratégica. Por força de lei, os serviços notariais e de registro destinam-se a garantir a publicidade, autenticidade, segurança e eficácia dos atos jurídicos praticados. Isso significa que a confiança pública nos cartórios depende da absoluta integridade e confidencialidade dos dados manuseados. Qualquer tecnologia adotada nesse âmbito deve respeitar os rígidos padrões éticos e legais da atividade notarial e registral, sob pena de comprometer direitos fundamentais dos cidadãos, abalando a fé pública jurisdicional, na fiscalização dos cartórios (art. 92 e seguintes, da CF), fé pública notarial e registral (art. 236, da CF), a fé nos documentos, e minando a

primeira colocação nos quesitos confiança, importância e qualidade dos serviços que os cartórios ocupam, para a população brasileira.

Diante da ubiquidade das IAs e de seu potencial transformador, impõe-se uma análise aprofundada de riscos: **Quais seriam as consequências de utilizar LLMs nos cartórios brasileiros?** Como garantir que essas ferramentas não violem a privacidade dos dados sigilosos armazenados, nem a soberania informacional do país? O objetivo deste artigo é responder a essas questões, examinando riscos concretos e propondo diretrizes para que a incorporação da IA seja feita de forma segura, legal e alinhada ao interesse público.

A importância dos dados como ativo estratégico

Em plena era da informação, os dados emergem como um dos ativos mais valiosos e estratégicos que organizações – públicas ou privadas – podem deter. Acesso massivo a dados permite desde melhorias de serviços até vantagens econômicas e geopolíticas. Por outro lado, **vazamentos de dados podem ter consequências catastróficas**, expondo informações pessoais, segredos comerciais ou mesmo segredos de Estado. Exemplos recentes ilustram o potencial danoso do uso indevido de dados em larga escala:

- **Caso Cambridge Analytica (2018)**: A consultoria política Cambridge Analytica obteve, sem consentimento adequado, dados pessoais de até **87 milhões de usuários do Facebook**. Essas informações foram usadas para traçar perfis comportamentais e influenciar eleitores em campanhas como a da eleição presidencial norte-americana e do referendo do *Brexit*. O episódio, amplamente divulgado, revelou como a exploração não autorizada de dados pode manipular processos democráticos e gerou intenso debate regulatório sobre privacidade e proteção de dados.

- **Vazamento do Google+ (2018)**: A extinta rede social Google+ sofreu duas brechas de segurança graves. A primeira, divulgada em outubro de 2018, **expos informações de cerca de 500 mil perfis** de usuários; a segunda, revelada posteriormente, **atingiu mais de 50 milhões de contas**. Esses incidentes minaram a credibilidade da plataforma e levaram o Google a antecipar o encerramento definitivo do Google+ em 2019. Embora menos debatido que outros casos, o episódio demonstra que mesmo gigantes da tecnologia não estão imunes a falhas que comprometem dados pessoais de milhões de pessoas.

- **Megavazamento de dados no Brasil (2021)**: No início de 2021, descobriu-se aquele que é possivelmente **o maior vazamento de dados pessoais da história brasileira**, atingindo **223 milhões de CPFs** – número que supera a população do país, indicando inclusão de registros antigos ou de pessoas falecidas. Foram expostos nomes completos, datas de nascimento, CPF, e possivelmente outras informações sensíveis, em uma base de dados que circulou livremente na internet. Esse megavazamento evidenciou fragilidades graves nos sistemas de segurança de entidades públicas e privadas no Brasil, bem como a **dificuldade de conter a disseminação** das informações uma vez que caem na internet (à época, cópias dos dados foram encontradas em fóruns da dark web e servidores abertos). O caso serviu de alerta sobre a urgência da implementação efetiva da Lei Geral de Proteção de Dados (LGPD) e de melhores práticas de governança da informação.

Nos cartórios brasileiros, os dados tratados têm caráter sensível e sigiloso: registros de nascimento, casamento e óbito, escrituras de imóveis, procurações, atas notariais, declarações, testamentos, entre outros, que podem conter informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato, dados sobre saúde e vida sexual, dados genéticos e biométricos. . Esses registros **são a prova legal de direitos e fatos da vida civil e patrimonial** de cada cidadão. Seu valor estratégico é imenso – tanto para garantir direitos individuais (por exemplo, comprovar a propriedade de um bem ou a

existência de um vínculo familiar) quanto em perspectiva coletiva (por exemplo, estatísticas populacionais ou imobiliárias que orientam políticas públicas). Dessa forma, **a proteção desses dados é crucial**. Um vazamento de informações de cartório não representaria apenas violação de privacidade, mas poderia gerar **fraudes patrimoniais, usurpação de identidade e outros crimes** com consequências para a segurança jurídica do país.

Importante lembrar que os cartórios brasileiros operam sob um regime legal que impõe deveres rigorosos de guarda e sigilo. A Lei n.º 8.935/1994 (Lei dos Notários e Registradores) estabelece ser obrigação dos titulares **"guardar sigilo sobre a documentação e os assuntos de natureza reservada"** de que tenham conhecimento em função da atividade. Ou seja, a confidencialidade não é apenas uma questão de ética profissional, mas um imperativo legal no âmbito registral e notarial. Qualquer ferramenta tecnológica que manipule os dados dos usuários dessas serventias deve, portanto, respeitar os mesmos níveis de segurança e confidencialidade esperados de um oficial de registro.

Como funcionam os LLMs e por que representam risco

Modelos de linguagem de larga escala (LLMs) são algoritmos de IA treinados com bases massivas de textos, capazes de produzir respostas coerentes e realizar tarefas complexas de processamento de linguagem natural. Esses modelos não seguem instruções pré-programadas linha a linha; em vez disso, **eles "aprendem" padrões estatísticos** a partir dos dados de treinamento. Por exemplo, ao treinar um LLM com bilhões de frases em português, ele captará as regularidades do idioma e a frequência de determinadas sequências de palavras, desenvolvendo a habilidade de prever a próxima palavra ou frase dada uma entrada inicial (*prompt*).

O poder dos LLMs reside nessa capacidade de generalização: eles podem responder de forma útil a perguntas nunca antes vistas, combinando conhecimentos diversos adquiridos nos dados de treinamento. Contudo, o mesmo mecanismo de aprendizado estatístico traz **desafios e riscos peculiares**:

- **Extração inadvertida de padrões sensíveis**: Os LLMs podem acabar memorizando fragmentos do conjunto de treinamento, especialmente se certos dados aparecem com frequência ou possuem um padrão único. Assim, **um LLM pode revelar dados confidenciais nas respostas sem intenção aparente**. Por exemplo, se um modelo foi treinado em milhões de e-mails corporativos, é possível que informações privadas contidas em alguns desses e-mails sejam reproduzidas em suas respostas a usuários externos – fenômeno conhecido como **"vazamento de dados do modelo"**. Esse risco é particularmente preocupante se o modelo foi exposto a documentos sigilosos (como contratos, registros pessoais, senhas, etc.), já que bastaria uma pergunta com intenção de induzir a erro , ou um contexto específico, para ele regurgitar partes desses conteúdos.

- **Inferências não programadas**: Diferentemente de um software tradicional, que faz apenas o que foi explicitamente codificado, um LLM pode fazer inferências complexas não previstas por seus desenvolvedores. Se um padrão implícito existe nos dados, o modelo pode descobri-lo. Por exemplo, se em uma base de contratos houver correlação entre certos nomes e valores financeiros, o LLM pode captar essa associação. Isso significa que **modelos de IA podem revelar correlações sensíveis ou deduzir informações reservadas combinando diferentes dados**, mesmo sem acesso direto a um dado específico. Em um contexto de registros públicos, isso pode levar a descobertas involuntárias – imagine um LLM deduzindo a renda de indivíduos apenas analisando padrões em registros imobiliários ou identificando relacionamentos pessoais sigilosos a partir de coincidências em registros civis.

- **Alucinações e erros**: Embora poderosos, LLMs não têm compreensão perfeita nem garantias de veracidade. Eles frequentemente sofrem do problema de *hallucination*, isto é, **podem gerar**

informações incorretas ou mesmo completamente inventadas com ar de plausibilidade. No ambiente de um cartório, um erro desses pode significar a sugestão de um dado errado em uma escritura ou a citação de uma lei inexistente em um parecer, colocando em risco a segurança jurídica do ato praticado. Como os modelos tendem a "preencher lacunas" quando a informação precisa não está disponível, **qualquer utilização de LLMs para auxiliar em documentos oficiais requer verificação humana criteriosa**.

- **Falta de transparência (caixa-preta)**: Os LLMs de ponta, com milhões ou bilhões de parâmetros, são em grande medida caixas-pretas – suas tomadas de decisão não são facilmente explicáveis. Isso dificulta auditorias e a **identificação exata da fonte de cada informação gerada**. No caso de um vazamento de dado sigiloso por um modelo, por exemplo, seria complexo rastrear qual parte do treinamento originou aquele vazamento. Essa opacidade conflita com a necessidade de **responsabilização e controle** nas atividades notariais e registrais, onde cada ato é registrado, chancelado e pode ser posteriormente auditado pelas corregedorias de justiça.

Em suma, os LLMs representam uma tecnologia disruptiva, mas que carrega riscos substanciais de **quebra de confidencialidade e confiabilidade**. Quando se considera integrá-los a sistemas que lidam com dados sensíveis – a exemplo dos serviços extrajudiciais – é preciso ter ciência de que, sem devidas salvaguardas, **o modelo tem possibilidade "vazar" informações protegidas e agir de maneiras não inteiramente previsíveis**, expondo as serventias e os cidadãos a situações indesejadas. Adicionalmente, o uso de LLMs fornecidos por terceiros, como ChatGPT, DeepSeek etc. implica em **transmitir dados para fora da infraestrutura atual**, o que traz um conjunto adicional de preocupações abordadas a seguir.

Riscos específicos às serventias extrajudiciais

Os cartórios de notas e de registro – também chamados de **serventias extrajudiciais** – ocupam uma posição singular no que tange à custódia de informações. Ao mesmo tempo em que devem dar publicidade a muitos de seus atos (por exemplo, qualquer pessoa pode solicitar certidões de registro público), também lidam com **documentos cuja divulgação irrestrita seria danosa ou proibida**, mantendo-os sob sigilo quando necessário (como testamentos cerrados, livros de notas com negócios ainda em andamento, ou dados pessoais sensíveis). A seguir, detalhamos riscos particulares da introdução de LLMs nesse ambiente tão peculiar:

(a) Violação do dever legal de sigilo e da LGPD: Conforme mencionado, a Lei nº 8.935/94 impõe aos notários e registradores o dever de sigilo profissional. Inserir dados de cartório em modelos de linguagem comercial baseados em nuvem (como ChatGPT, Microsoft Azure OpenAI, Google Gemini, DeepSeek, entre outros) pode, na prática, significar o **compartilhamento de informações protegidas com servidores de terceiros**. Isso fere diretamente o dever de confidencialidade e pode também representar uma infração à Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018), que impõe regras rigorosas para o tratamento e a **transferência de dados pessoais**, especialmente quando se trata de envio para fora do país. Nesses casos, a LGPD exige uma base legal válida, consentimento expresso dos titulares ou garantias adequadas de proteção. Assim, ao alimentar um LLM na nuvem com dados sensíveis constantes de uma escritura — como nomes das partes, CPFs, descrição do imóvel e valores do negócio —, o cartório pode estar promovendo, inadvertidamente, uma transferência internacional de dados pessoais sem autorização dos titulares, muitas vezes sem sequer compreender plenamente os termos de uso da plataforma contratada. Além disso, uma vez enviados, **esses dados podem ficar armazenados nos servidores do provedor de IA**, fora do controle do cartório. Empresas como a Samsung já identificaram esse perigo: em 2023, a Samsung **baniu o uso do ChatGPT por funcionários após descobrir que engenheiros vazaram acidentalmente código-fonte confidencial ao inseri-lo na ferramenta**. O receio, conforme comunicado interno da empresa, era de que informações enviadas a plataformas de IA ficariam guardadas externamente e poderiam ser acessadas indevidamente por terceiros. Por analogia, um cartório que envia dados ao ChatGPT, por exemplo, corre o risco de que esses

dados fiquem retidos nos logs da OpenAI (empresa responsável) e, pior, possam ser expostos a outros usuários mediante alguma falha ou utilização maliciosa.

(b) Risco à integridade e autenticidade dos atos: Os cartórios têm a missão de assegurar a autenticidade e eficácia dos atos jurídicos. Se um LLM for utilizado, por exemplo, para **redigir minutas de documentos ou responder consultas técnicas** dentro da serventia, há o perigo de que ele introduza informações incorretas (*alucinações*) ou formate o texto de forma inadequada juridicamente. Um modelo de IA poderia sugerir cláusulas inválidas, citar erroneamente uma lei ou jurisprudência, ou até confundir dados de casos diferentes. Caso o tabelião ou registrador confie cegamente na sugestão da IA, um erro pode acabar incorporado ao registro ou escritura. Imagine-se a **inclusão de um número de matrícula de imóvel errado** em uma escritura por sugestão da IA – isso poderia transferir a propriedade do bem incorretamente, gerando uma disputa judicial complexa para desfazer o equívoco. Em última instância, **o uso irresponsável da IA pode minar a confiança nos documentos notariais e registrais**, que sempre gozaram de alta presunção de veracidade. Ressalte-se que, legalmente, os oficiais continuam responsáveis pelos atos que praticam, ainda que tenham sido auxiliados por uma ferramenta; portanto, responderiam disciplinarmente e civilmente por danos causados por eventuais deslizes da IA.

(c) Perigos na centralização de dados (SERP, ONR, ON-RCPN e demais centrais): Nos últimos anos, o Brasil avançou na criação de sistemas centralizados para integrar os cartórios em nível nacional. O Sistema Eletrônico dos Registros Públicos (Serp) instituído pela Lei nº 14.382/2022 visa orientar esta transformação, sendo assim o **Operador Nacional do Registro de Imóveis (ONR)**, por exemplo, foi criado pela Lei nº 13.465/2017 para implementar o Sistema de Registro Eletrônico de Imóveis, integrando todos os cartórios de imóveis do país. De modo análogo, o **Operador Nacional do Registro Civil de Pessoas Naturais (ON-RCPN)**, instituído pela Lei nº 14.382/2022, visa coordenar a digitalização e unificação dos registros civis (nascimentos, casamentos, óbitos) em âmbito nacional. Esses sistemas prometem **maior eficiência, acessibilidade e padronização** dos serviços. Contudo, também representam uma mudança de paradigma: em vez de dados fragmentados em milhares de cartórios locais, passaremos a ter **grandes bases de dados nacionais** concentrando informações de todos os brasileiros.

Do ponto de vista de segurança, a centralização cria um alvo mais valioso para ataques. **Uma brecha de segurança em um sistema central pode expor dados de milhões de pessoas simultaneamente**, amplificando o impacto de um incidente. Se tal central usar IA de forma imprudente, as consequências seriam proporcionais à escala nacional dos dados. Por exemplo, se o ONR integrasse um assistente de IA conectado à internet para agilizar buscas registrais, e esse assistente fosse comprometido, **poder-se-ia extrair maciçamente informações de proprietários, valores de imóveis, localização de bens, etc., de todo o território nacional**. No caso do ON-RCPN, um vazamento amplo poderia expor dados pessoais básicos (nome, filiação, data de nascimento, etc.) de praticamente toda a população – informações que, cruzadas com outras bases, facilitariam fraudes de identidade em larga escala.

Além disso, **dados centrais do registro civil podem ter interesse estratégico para inteligências estrangeiras**. Uma base completa de nascimentos, por exemplo, permite mapear perfis demográficos e até identificar alvos para espionagem. Nos cenários de espionagem que discutiremos, ficou evidente como agentes estrangeiros se beneficiaram da obtenção de certidões brasileiras. Ou seja, a centralização precisa vir acompanhada de investimentos robustos em cibersegurança e de limites claros ao uso dessas informações, incluindo o uso de IA. Ferramentas de IA empregadas nesses sistemas centrais **deveriam, idealmente, operar de forma isolada (offline) ou sob rígido controle, evitando qualquer comunicação inadvertida com serviços externos**.

(d) Aspectos éticos e de viés: Por fim, cabe lembrar que LLMs carregam vieses presentes nos dados com que foram treinados. Se um modelo não for devidamente ajustado, **pode reproduzir preconceitos ou tratamentos discriminatórios**. Nos serviços extrajudiciais, isso seria inaceitável – por exemplo, um assistente que auxilia na triagem de pedidos de certidões não pode, em hipótese alguma, dar preferência a solicitações com base em nome, origem ou qualquer atributo sensível. Garantir a **imparcialidade e equidade** das IAs em cartórios é obrigatório, mas alcançá-la requer um trabalho cuidadoso de filtragem e treinamento adicional desses modelos, o que nem sempre está ao alcance de pequenas serventias.

Diante de todos esses pontos, evidencia-se que **a utilização de IA nos cartórios brasileiros envolve riscos multidimensionais**: legais, de segurança da informação, operacionais e éticos. Não se trata de desaconselhar totalmente o uso da tecnologia – os benefícios potenciais existem –, mas de ressaltar que, nesse setor, qualquer inovação precisa ser implementada com redobrada cautela, sob pena de ferir os fundamentos de confiança e segurança nos quais o sistema registral/notarial se apoia.

Cenários hipotéticos e casos reais

Para ilustrar de forma mais concreta os perigos discutidos, apresentamos dois cenários. O primeiro é hipotético, mas perfeitamente plausível dado o estado atual da tecnologia e práticas de alguns usuários; já o segundo baseia-se em fatos reais divulgados na imprensa, evidenciando como informações de registros podem ser exploradas em geopolítica e espionagem.

Cenário 1 (hipotético) – Uso de LLM em um cartório de registro de imóveis e/ou tabelionado de notas: Imagine um cartório de **registro de imóveis** e/ou um **tabelionato de notas** de médio porte em uma capital brasileira que decide adotar soluções tecnológicas para **agilizar seus procedimentos internos** e melhorar o atendimento ao público. A equipe, buscando eficiência, começa a utilizar informalmente uma **IA comercial**, como o ChatGPT ou Gemini por exemplo, para **auxiliar na lavratura de escrituras públicas, confecção de minutas de registros e conferência de dados**.

Inicialmente, os resultados são positivos: escreventes conseguem **redigir atos notariais e registrais com mais rapidez**, transcrever descrições antigas com apoio da IA, revisar cláusulas complexas com sugestões automáticas e até realizar **buscas em lote sobre ônus reais, certidões e impedimentos**. Para isso, a equipe insere nos prompts **dados reais das partes e dos atos jurídicos**, como:

- Nome completo, CPF, RG, endereço e estado civil das partes;
- Valor da compra e venda, doação, permuta etc.;
- Informações sobre o imóvel, tipo de garantia (hipoteca, alienação fiduciária etc.) e existência de procurações ou substabelecimentos;
- Relações familiares ou societárias, forma de pagamento e condições contratuais específicas.

Com o tempo, milhares de interações similares são realizadas. Embora a plataforma afirme **não armazenar os dados**, a IA — por seu funcionamento estatístico — **absorve padrões recorrentes**, e isso permite que usuários externos, via **engenharia de prompt**, consigam **reconstruir tendências regionais e dados sensíveis**, como:

- “Quais os valores médios de imóveis doados com reserva de usufruto no bairro Y?”
- “Qual a forma de garantia mais comum usada em escrituras lavradas em Minas Gerais?”

A situação se agravaria com um **vazamento de logs ou de backups** da IA, que acabam expondo minutas de escrituras públicas, dados patrimoniais e informações pessoais sensíveis, violando não só a LGPD, mas também os princípios de fé pública e sigilo funcional.

Em outro episódio, o modelo **alucina a existência de uma restrição ambiental** sobre um imóvel rural, levando o oficial a **averbar indevidamente** uma informação no registro, o que trava uma venda futura e **gera perdas financeiras e judicialização**. Em lavraturas notariais, a IA passa a **confundir termos jurídicos**, como "comunhão parcial de bens" e "separação obrigatória", gerando minutas incorretas e impactando a **segurança dos atos**.

As consequências concretas são severas:

- Violação da confidencialidade de dados pessoais e patrimoniais, com potencial de responsabilização administrativa, civil e até penal;
- Abalo da fé pública, pilar central dos serviços notariais e registrais;
- Sanções ao delegatário, incluindo processos administrativos pelo CNJ, indenizações a terceiros prejudicados e multas por infrações à LGPD;
- Exploração indevida das informações por agentes externos, que se valem dos dados para direcionar investimentos imobiliários, mapear ativos estratégicos ou influenciar artificialmente o mercado local.

Esse cenário demonstra de forma clara que a adoção de **IA comercial** sem controles técnicos e jurídicos adequados por serventias extrajudiciais **coloca em risco a privacidade dos cidadãos**, a confiabilidade dos atos jurídicos e a própria **legitimidade institucional dos cartórios**.

Cenário 2 (caso real)– Espionagem internacional com uso de dados do registro civil: Em um contexto mais dramático, considere que **agentes de inteligência estrangeiros** consigam acesso indevido a bancos de dados de registro civil brasileiros. De posse de informações de nascimentos e identidades, eles passam a **fabricar identidades "reais" para espiões**, combinando dados verídicos de diferentes pessoas. Infelizmente, esse cenário não é mera ficção – investigações recentes revelaram casos de espiões russos que adotaram identidades brasileiras para atuar em países ocidentais sem levantar suspeitas.

Conforme reportado pela BBC News Brasil, documentos do FBI e da Polícia Federal brasileira mostraram **como o Brasil se tornou um "berçário" de espiões russos**, dada a facilidade de obter documentos autênticos ou quase autênticos no Brasil. Um exemplo notório é o de **Sergey Cherkasov**, agente russo do GRU, que viveu anos no Brasil sob a identidade falsa de Victor Muller Ferreira e quase ingressou como estagiário na Corte Penal Internacional, antes de ser detido. Outro caso é o de **Mikhail Mikushin**, apontado espião que se estabeleceu na Noruega como pesquisador; ele usava a identidade de *José Assis Giammaria*, supostamente nascido em Goiás. Uma **certidão de nascimento emitida em Padre Bernardo (GO)** foi parar nas mãos de Mikushin, permitindo-lhe obter passaporte brasileiro e atuar sob essa nacionalidade. Funcionários do cartório onde o documento se originou afirmaram não saber como a certidão chegou ao espião, indicando que pode ter havido fraude ou interceptação de dados do registro civil.

Esses incidentes verídicos demonstram que **dados do registro civil brasileiro têm grande valor para finalidades ilícitas transnacionais**, incluindo espionagem. Seja pela emissão fraudulenta de certidões autênticas, seja pela obtenção de informações de pessoas reais para criação de identidades falsas, há interesse de agentes estrangeiros em explorar brechas no nosso sistema registral. A Polícia Federal suspeita que a **confecção de certidões autênticas por meio de fraude em cartórios** foi uma das táticas utilizadas para dar base documental a espiões. A atratividade está na **"boa reputação" internacional do passaporte brasileiro e na relativa facilidade histórica de se obter registros no país**.

Nesse panorama, imagina-se o que não poderia ocorrer caso **extensas bases de dados de registros civis fossem acessadas por meio de IA ou vazamentos**: informações de milhões de brasileiros poderiam ser cruzadas para selecionar identidades "perfeitas" (por exemplo, pessoas que morreram na infância e não tiveram seus documentos usados, ou indivíduos com nome comum e poucas conexões), construindo perfis falsos altamente críveis. Poderiam ainda usar LLMs para automatizar a busca de candidatos a identidade falsa ou para elaborar documentos falsificados de forma mais convincente, a partir de modelos aprendidos nos documentos reais. Em suma, **a exposição indevida dos dados civis poderia escancarar uma porta para ingerência estrangeira e ameaças à segurança nacional**. O caso dos espiões russos serve de alerta: um simples documento de cartório, caindo em mãos erradas, pode sustentar operações clandestinas de grande envergadura.

Os dois cenários, cada um a seu modo, reforçam a premissa central deste artigo: **os dados geridos pelos cartórios são por demais sensíveis para que possamos arriscar seu uso negligente em plataformas de IA**. Seja pelo prejuízo individual (exposição de patrimônio, violação de privacidade) ou coletivo (erosão da confiança institucional, uso malicioso por atores criminosos ou estatais), os riscos superam em muito quaisquer ganhos imediatos de conveniência. Portanto, é imperativo desenvolver estratégias mitigadoras e diretrizes claras – como discutiremos na próxima seção – antes de incorporar IAs nos procedimentos cartorários.

Recomendações para uso seguro e soberano da IA

Tendo mapeado os riscos, passa-se a propor caminhos para **mitigar perigos e viabilizar um uso da IA alinhado com a segurança jurídica e a soberania tecnológica** do Brasil nos serviços extrajudiciais. Eis algumas recomendações concretas:

- **Desenvolvimento de LLMs locais ou *on-premises***: Ao invés de utilizar diretamente serviços de IA na nuvem oferecidos por terceiros, os cartórios (ou os órgãos reguladores) devem investir em soluções que possam ser executadas localmente, mesmo em nuvem mas dentro de uma infraestrutura não compartilhada. Modelos próprios e especializados podem ser treinados ou ajustados com dados públicos relevantes, de modo a criar um **assistente virtual interno, cujo controle de dados permaneça no Brasil**. A execução local garante que nenhuma informação sensível saia para servidores externos, atendendo às exigências da LGPD e do dever de sigilo. Além disso, permite customizar o comportamento do modelo conforme as necessidades do setor notarial/registral, filtrando respostas inadequadas e inserindo limites específicos (por exemplo, impedir que forneça dados pessoais de terceiros). Embora isso exija recursos computacionais significativos, parcerias entre a Academia e empresas de tecnologia nacionais poderiam viabilizar um LLM soberano a serviço dos cartórios. **LLMs locais** evitam a dependência de fornecedores estrangeiros e reduzem drasticamente o vetor de vazamento de dados, já que todo o processamento fica intramuros.

- **Aprendizado federado e colaboração segura**: Para aproveitar os benefícios da IA sem comprometer dados sensíveis, pode-se adotar **aprendizado federado** entre serventias. Nesse modelo, cada cartório ou cada base regional de dados treina localmente um modelo com seus dados (que nunca saem de lá) e somente os parâmetros aprendidos (pesos do modelo) são enviados a um servidor central para agregação com os de outros locais. O resultado é um modelo global aprimorado, **sem que os dados brutos de nenhum cartório tenham sido centralizados**. Assim, se 100 cartórios colaborarem, obtém-se um LLM treinado no conhecimento conjunto de todos, mas nenhum registro individual precisou ser compartilhado. Essa abordagem, aliada a técnicas de criptografia (como agregação segura de parâmetros), pode criar IAs poderosas preservando a privacidade. No contexto brasileiro, a empresa NoCartorio.com está criando e coordenando esse esforço federado, garantindo padronização e **respeito às particularidades locais** (por exemplo, idiomas regionais, formas diferentes de lavrar atos, etc.).

- **Limitação e anonimização de dados de entrada**: Uma medida prática, enquanto soluções mais robustas não são implementadas, é **nunca inserir identificadores pessoais diretos nas consultas à IA**. Se um cartório for testar o uso de um LLM, deve **anonimizar** o máximo possível as informações – substituindo nomes por iniciais, ocultando documentos, endereços e outros dados sensíveis – de modo que, mesmo que haja interceptação ou armazenamento, as informações não estejam em formato utilizável. Da mesma forma, evitar usar dados reais em fase experimental: é preferível treinar e testar IAs com dados fictícios ou já públicos (por exemplo, usar registros e contratos que já sejam públicos em bases de jurisprudência ou editar minutas para retirar conteúdos privados). Só em ambiente controlado e após auditorias, pensar em usar dados reais, e ainda assim com parcimônia.

- **Auditorias técnicas e *compliance***: Antes de adotar uma solução de IA, deve-se realizar uma **auditoria de segurança e de aderência legal**. Especialistas em TI e em proteção de dados devem verificar como o modelo armazena informações, se possui logs, se há risco de *cache* de conteúdo sensível, quais conexões realiza, etc. Também é importante auditar os vieses – verificar se o modelo tem predisposições indevidas que precisam ser corrigidas. Ferramentas de IA devem passar por um crivo similar ao de qualquer software crítico utilizado em governo: testes de invasão, verificação de conformidade com a LGPD, e idealmente certificações independentes. O CNJ, em conjunto com a Autoridade Nacional de Proteção de Dados (ANPD), poderia criar um protocolo de certificação para sistemas de IA aptos ao uso em cartórios, contemplando requisitos de segurança da informação, privacidade e qualidade de output. Somente soluções certificadas (ou aprovadas em procedimento análogo) seriam utilizadas, reduzindo o improviso tecnológico que é fonte de tantos problemas.

- **Capacitação e conscientização dos profissionais**: A melhor política de segurança pode falhar se os usuários não estiverem conscientizados. Portanto, é crucial treinar tabeliães, registradores e escreventes sobre **boas práticas no uso de IA**. Isso inclui orientações claras: não inserir dados sigilosos em ferramentas online públicas; compreender as limitações do modelo (sabendo que ele pode errar ou alucinar); revisar sempre as respostas da IA; e reportar incidentes ou saídas estranhas do sistema. Criar manuais de uso responsável e promover workshops pode ajudar a criar uma cultura de **vigilância tecnológica** dentro das serventias. Vale lembrar que muitos riscos de vazamento decorrem de erro humano (como no caso Samsung, em que funcionários copiaram código confidencial para o ChatGPT sem malícia). A prevenção passa por educação.

- **Normatização pelo Conselho Nacional de Justiça (CNJ)**: O CNJ, que supervisiona a atividade extrajudicial, deve assumir um papel ativo na regulação do uso de IA nesse setor. Poderia ser editado um **Provimento** específico estabelecendo diretrizes: por exemplo, proibindo expressamente o uso de serviços de IA baseados no exterior para processar dados de atos notariais/Registrais; exigindo avaliação de impacto de proteção de dados (conforme a LGPD) antes de implementar IA em alguma serventia; e determinando padrões mínimos de segurança para quaisquer sistemas inteligentes adotados. O CNJ também poderia **estimular projetos pilotos controlados**, onde um pequeno número de cartórios utilize IA sob monitoramento, gerando relatórios de desempenho e segurança, de modo a aprender antes de expandir para todo o país. A normatização garantiria isonomia – todos os cartórios seguirão as mesmas regras – e daria **segurança jurídica** para os oficiais, que teriam clareza sobre o que é permitido ou vetado no uso dessas novas tecnologias.

- **Soluções complementares de segurança**: Além das específicas à IA, vale reforçar medidas tradicionais que ganham nova importância. **Criptografia robusta de bases de dados**, autenticação de dois fatores para acesso a sistemas centrais, trilhas de auditoria que registrem quem consultou dados e quando, tudo isso ajuda a impedir acessos indevidos – seja por hackers, seja por espiões infiltrados. Técnicas de *data masking* (mascaramento de dados) podem ser adotadas em ambientes de teste ou menos críticos, para que mesmo que um sistema de IA seja comprometido, não tenha à disposição dados reais em texto claro. A coordenação com órgãos de segurança (como a própria PF e ABIN) é recomendável para que vulnerabilidades no sistema de registros sejam tratadas também sob a ótica de contraespionagem e segurança nacional, dado o potencial de uso indevido demonstrado.

Em resumo, as recomendações visam permitir que a IA seja utilizada **nos termos do interesse público brasileiro**: preservando a confidencialidade dos dados dos cidadãos, garantindo a continuidade e fidelidade dos serviços cartorários, e evitando dependência tecnológica que comprometa a soberania. **É possível conciliar inovação e segurança**, mas isso demanda planejamento, investimento e prudência regulatória.

Conclusão

A incorporação da inteligência artificial nos serviços registrais e notariais do Brasil representa um verdadeiro dilema contemporâneo: de um lado, a promessa de modernização, eficiência e redução de erros humanos; de outro, o espectro de violações de privacidade, perda de confiança e até riscos à soberania nacional. Ao longo deste artigo, argumentamos que **qualquer adoção de IA nessas atividades essenciais deve ser cercada de cuidados excepcionais**, dada a natureza estratégica dos dados envolvidos e o papel fundamental que cartórios desempenham na estrutura legal do país.

Os casos e cenários apresentados serviram para demonstrar que os riscos não são meramente teóricos. Vazamentos massivos de dados já ocorreram no Brasil e no mundo, ensinando lições amargas sobre a fragilidade das defesas digitais frente a agentes mal-intencionados. No campo dos registros públicos, vimos que um descuido pode abrir brecha para fraudes e até espionagem internacional – um desdobramento que outrora pareceria enredo de ficção, mas hoje se revela uma preocupação concreta. Os LLMs, embora tecnicamente fascinantes, mostraram-se ferramentas de dois gumes: capazes de **gerar texto com proficiência quase humana**, mas também de **escapar ao controle dos programadores**, regurgitando informações indevidas ou incorporando vieses sutis.

Diante disso, a postura recomendada não é rejeitar sumariamente a IA, mas **abraçá-la com responsabilidade e sob nossos próprios termos**. Significa dizer que cartórios e órgãos reguladores devem apropriar-se da tecnologia, e não simplesmente consumir soluções prontas sem avaliação. É preferível demorar um pouco mais na implementação e fazê-la corretamente, do que adotar apressadamente uma novidade e enfrentar consequências desastrosas depois. A história da tecnologia é repleta de exemplos em que a falta de cautela gerou retrocessos – no contexto extrajudicial, um incidente grave poderia abalar a credibilidade de todo o sistema, algo que o Brasil não pode se permitir.

Em conclusão, a adoção de IA pelos cartórios deve ser guiada pelos princípios da **segurança, ética e soberania**. Segurança, para garantir que os dados dos cidadãos continuem protegidos e que os atos praticados mantenham sua integridade inquestionável. Ética, para assegurar que a tecnologia seja usada em benefício da sociedade, respeitando direitos fundamentais e evitando qualquer discriminação ou injustiça automatizada. Soberania, para que o país mantenha o controle sobre informações tão sensíveis, promovendo soluções alinhadas com nossas leis e valores, e não ficando à mercê de interesses ou infraestruturas estrangeiras. Somente com essa tríade de preocupações bem equacionadas poderemos transformar a inteligência artificial de uma potencial ameaça em uma poderosa aliada do aprimoramento dos serviços registrais e notariais, reforçando – e não corroendo – a confiança pública neles depositada.

Referências

- **Lei Geral de Proteção de Dados Pessoais (LGPD)** – Lei n.º 13.709/2018, marco legal brasileiro que regula a privacidade e o tratamento de dados pessoais. Estabelece princípios como a finalidade, adequação, necessidade e segurança no uso de dados, aplicáveis também aos cartórios extrajudiciais, e alterou disposições do Marco Civil da Internet para reforçar a proteção de dados no Brasil.
- **Lei dos Notários e Registradores** – Lei n.º 8.935/1994, que regulamenta o art. 236 da Constituição Federal, dispondo sobre a atividade notarial e de registro. Determina deveres dos oficiais, **inclusive o dever de sigilo sobre documentação e assuntos reservados** vinculados à função, bem como a finalidade de garantir publicidade, autenticidade, segurança e eficácia dos atos jurídicos.
- **Marco Civil da Internet** – Lei n.º 12.965/2014, estabelece princípios, garantias e direitos para o uso da internet no Brasil. Prevê, entre outros, a proteção da privacidade e dos dados pessoais nas

comunicações digitais. Foi complementado pela LGPD nos aspectos de tratamento de dados. Sua observância é relevante quando cartórios utilizam serviços em nuvem ou transmitem dados via internet.

- **Escândalo Facebook–Cambridge Analytica (2018)** – Caso internacional de uso indevido de dados de usuários de redes sociais. A empresa Cambridge Analytica coletou sem consentimento dados pessoais de até **87 milhões de usuários do Facebook** e os utilizou para fins de propaganda política dirigida (https://en.wikipedia.org/wiki/Facebook%E2%80%93Cambridge_Analytica_data_scandal). Levou a investigações nos EUA e Europa, multas ao Facebook e maior conscientização global sobre o valor dos dados e os riscos de sua exploração não autorizada.

- **Vazamentos de dados do Google+ (2018)** – Brechas de segurança na rede social Google+ expuseram perfis de usuários. **Cerca de 500 mil contas tiveram dados (nome, e-mail, etc.) vazados** inicialmente, e uma segunda falha afetou **mais 52 milhões de usuários** poucos meses depois (https://en.m.wikipedia.org/wiki/2018_Google_data_breach). O incidente precipitou o fim do Google+ e exemplificou fragilidades mesmo em empresas de tecnologia estabelecidas.

- **Megavazamento de 223 milhões de CPFs (2021)** – Incidente revelado pelo laboratório dfndr (PSafe) e reportado em janeiro de 2021. Uma base contendo dados pessoais de praticamente toda a população brasileira (incluindo nome, CPF, data de nascimento, e possivelmente informações como scores de crédito e fotos) foi **exposta e colocada à venda em fóruns online**, configurando o maior vazamento da história nacional (https://pt.wikipedia.org/wiki/Vazamento_de_dados_do_fim_do_mundo). O caso evidenciou deficiências na segurança de sistemas públicos/privados e impulsionou debates sobre aplicação da LGPD.

- **Reportagem BBC News Brasil – "Como o Brasil se tornou 'berçário' de espiões russos" (2022)** – Matéria investigativa da BBC News Brasil que revelou documentos do FBI e da PF indicando que agentes russos usaram o Brasil como base para criar identidades falsas. Cita o caso de **Sergey Cherkasov (alias Victor Muller Ferreira)** e outros, mostrando que **facilidades documentais brasileiras permitiram a espiões circular pela Europa e EUA com baixa suspeita** (https://www.bbc.com/portuguese/articles/ckk43wg6n31o). Alerta para vulnerabilidades no controle de registros civis e emissão de documentos.

- **Notícia UOL – "Espião russo que se passava por brasileiro é libertado em troca de prisioneiros" (2024)** – Reportagem do UOL Notícias sobre a troca de prisioneiros entre Rússia e Ocidente, mencionando **Mikhail Mikushin (alias José Assis Giammaria)**. Destaca que ele **usava certidão de nascimento brasileira falsa de Padre Bernardo (GO)**, segundo informações reveladas pela BBC Brasil, e que funcionários do cartório local não souberam explicar o acesso do russo a esse documento (https://noticias.uol.com.br/internacional/ultimas-noticias/2024/08/02/espiao-que-se-passava-por-brasileiro-e-libertado-em-troca-de-prisioneiros.htm). Ilustra um caso concreto de uso de dados de cartório em espionagem internacional.

- **Matéria Folha de S.Paulo – "Espiões da Rússia: Tribunal descarta fraude em cartório" (2023)** – Cobertura do jornal Folha de S.Paulo sobre as investigações referentes aos espiões russos com identidades brasileiras. Informa que a Corregedoria do TJ/RJ não identificou adulterações nos livros dos cartórios onde dois supostos espiões foram registrados, sugerindo que possivelmente **foram utilizadas identidades de brasileiros genuínos, nascidos nos anos 1980, cujos registros autênticos foram apropriados por terceiros**(https://www1.folha.uol.com.br/mundo/2023/04/tribunal-do-rj-descarta-fraude-em-registros-de-supostos-espioes-da-russia.shtml). O artigo discute a hipótese de que a vulnerabilidade residiu na obtenção posterior dos documentos, não na falsificação dentro do

cartório, mas reconhece a facilidade histórica de se obter registros no Brasil como fator explorado pelos agentes estrangeiros.

- **Política da Samsung sobre ChatGPT (2023)** – Após incidentes em que funcionários coreanos inseriram segredos corporativos no ChatGPT, a Samsung emitiu diretriz proibindo o uso de IA generativa no ambiente de trabalho. Conforme noticiado na Exame/Bloomberg, a empresa **teme que dados enviados a essas plataformas fiquem armazenados externamente e possam ser compartilhados com outros usuários** (https://exame.com/tecnologia/samsung-proibe-uso-de-ia-apos-vazamento-de-dados-com-chatgpt/). Esse caso é emblemático sobre riscos de confidencialidade ao usar LLMs de terceiros, levando grandes corporações a restringir seu uso para proteger propriedade intelectual e informações sensíveis.

Citações e referências bibliográficas:

Lei n.º 13.709/2018

https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

---

Lei n.º 8.935/1994

https://www.planalto.gov.br/ccivil_03/leis/l8935.htm

Constituição Federal de 1988 (CF)

https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

—---

Lei n.º 12.965/2014

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

---

Lei n.º 14.382/2022

https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/lei/L14382.htm

---

SERP

https://serp.org.br/

ONR

https://onr.org.br/

ON-RCPN

https://onrcpn.org.br/

PESQUISA IMAGEM DOS CARTÓRIOS.

https://www.anoreg.org.br/_site/_wp-content/uploads/_2022/_12/_Pesquisa-imagem-dos-cartorios.pdf. Acessado em . Acesso em: 03/05/2025.

—----------

Escândalo de dados Facebook–Cambridge Analytica – Wikipédia, a enciclopédia livre

https://pt.wikipedia.org/wiki/Esc%C3%A2ndalo_de_dados_Facebook%E2%80%93Cambridge_Analytica

---

Google+ chega ao fim após vazamentos de dados e baixa popularidade

https://www.techtudo.com.br/noticias/2019/04/google-chega-ao-fim-apos-vazamentos-de-dados-e-baixa-popularidade.ghtml

---

Dados de milhões de brasileiros vazados em 2021 continuam circulando, sugere site - TecMundo

https://www.tecmundo.com.br/seguranca/276809-dados-milhoes-brasileiros-vazados-2021-continuam-circulando-sugere-site.htm

---

OWASP Top 10 LLM: Os Principais Riscos para Aplicações de Inteligência Artificial | by Fernando Silva | Medium

https://fernando-silva.medium.com/owasp-top-10-llm-os-principais-riscos-para-aplica%C3%A7%C3%B5es-de-intelig%C3%AAncia-artificial-12837e7d4620

Lei Geral de Proteção de Dados Pessoais – Wikipédia, a enciclopédia livre

https://pt.wikipedia.org/wiki/Lei_Geral_de_Prote%C3%A7%C3%A3o_de_Dados_Pessoais

---

Samsung proíbe uso de IA após vazamento de dados com ChatGPT | Exame

https://exame.com/tecnologia/samsung-proibe-uso-de-ia-apos-vazamento-de-dados-com-chatgpt/

Espião russo que usava documento brasileiro é libertado em troca de prisioneiros

https://noticias.uol.com.br/internacional/ultimas-noticias/2024/08/02/espiao-que-se-passava-por-brasileiro-e-libertado-em-troca-de-prisioneiros.htm

---

Espiões da Rússia: Tribunal descarta fraude em cartório - 14/04/2023 - Mundo - Folha

https://www1.folha.uol.com.br/mundo/2023/04/tribunal-do-rj-descarta-fraude-em-registros-de-supostos-espioes-da-russia.shtml