

Proteção de dados e Large Language Models

05.10.2023 4 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Blockchain e Inovação

Assuntos

Inteligência Artificial

Quando se pensa em sistemas de inteligência artificial, mais especificamente em grandes modelos de linguagem (*Large Language Models* ou *LLMs*), o nome que vem inicialmente à cabeça é quase sempre o mesmo: ChatGPT.

O queridinho da vez, que bateu o recorde de crescimento de número de usuários de aplicações voltadas ao consumidor, chegando a 100 milhões de usuários ativos em menos de 2 meses desde o seu lançamento, não tem chamado atenção somente de pessoas interessadas em testar as habilidades de resposta da ferramenta: autoridades de proteção de dados ao redor do mundo também têm acompanhado de perto as suas práticas de proteção de dados.

Analisar as condutas adotadas por respectivos órgãos reguladores, bem como as alegações das práticas potencialmente violadoras da legislação de proteção de dados, tende a ser útil para outros provedores de serviços similares, ou mesmo de soluções de inteligência artificial com propósitos distintos, mas com tratamentos de dados pessoais comparáveis aos realizados pelo ChatGPT.

No dia 30 de março de 2023, o Garante, autoridade de proteção de dados da Itália, emitiu uma decisão emergencial determinando a imediata suspensão do tratamento de dados pessoais de usuários localizados na Itália pelo ChatGPT. Na ordem, o Garante indicava que os titulares de dados não possuíam informações apropriadas sobre os tratamentos realizados pela OpenAI, e que possivelmente não existiria uma base legal para a coleta e processamento massivo de informações para fins de treinamento dos algoritmos.

A ordem de suspensão foi revista pelo Garante em 28 de abril de 2023, depois de a OpenAI ter realizado diversas melhorias em aspectos de sua conformidade com o GDPR, incluindo a disponibilização de informações adicionais a respeito dos tratamentos de dados pessoais conduzidos, a adoção de medidas para permitir aos usuários exercerem direitos de oposição e de exclusão, e a inclusão de verificações prévias sobre a idade dos usuários, no intuito de restringir a utilização do serviço por menores de 13 anos, embora a investigação conduzida pela autoridade Italiana continue em curso.

Depois de autoridades de proteção de dados da Alemanha e da Espanha também manifestarem que investigariam as práticas do ChatGPT, o *European Data Protection Board*, órgão responsável por garantir a aplicação consistente no GDPR, anunciou, no dia 13 de abril de 2023, a criação de uma força-tarefa dedicada a avaliar as práticas da OpenAI e compartilhar informações sobre possíveis ações de fiscalização e imposição de sanções.

Em maio de 2023, o professor Luca Belli divulgou um artigo no qual apontava

diversas violações à LGPD por parte do ChatGPT, que o levaram a protocolar uma petição perante a ANPD contra a OpenAI. Dentre as infrações indicadas estão a ausência de informações adequadas, de bases legais para o tratamento, o desrespeito aos direitos dos titulares previstos na legislação e a falta de nomeação de um Encarregado. Embora alguns meios de comunicação tenham divulgado que a ANPD teria aberto processo de fiscalização para apurar denúncias contra a OpenAI, no sítio eletrônico da Autoridade ainda não constam informações oficiais nesse sentido.

Mais recentemente, em agosto de 2023, um pesquisador polonês fez uma reclamação à autoridade de proteção de dados local, na qual alega que a OpenAI viola sistematicamente as disposições do GDPR, ignorando por completo solicitações de exercício de direitos do titular e infringindo frontalmente suas obrigações de transparência.

Os casos mencionados acima são somente a ponta do iceberg. Até o momento, nenhuma autoridade de proteção de dados se manifestou de forma terminativa a respeito das práticas de tratamento de dados pessoais realizadas pelo ChatGPT, mas fica evidente que existem profundos questionamentos sobre a licitude dessas condutas.

Em especial, é possível extrair desses casos recentes 3 aspectos que merecem atenção de desenvolvedores de sistemas de inteligência artificial: (i) transparência é fundamental e deve ser levada em consideração em todos os momentos; (ii) direitos do titular devem ser observados, mormente no que tange às solicitações de correção e de exclusão; e (iii) proteção de dados deve estar no radar de qualquer fornecedor desde a concepção de qualquer novo produto ou serviço, em respeito ao princípio de *privacy by design*.

>>> Este conteúdo faz parte do e-book "*Inteligência artificial: visões jurídicas dos dilemas do futuro*". Leia mais artigos aqui.

Profissionais que aliam visão jurídica e visão de mercado



Felipe Palhares