Relatório Comparativo: Read.ai e Microsoft 365 Copilot – Privacidade, Segurança da Informação e LGPD

1. Introdução

Ferramentas baseadas em inteligência artificial têm se tornado cada vez mais presentes no dia a dia das empresas. Entre elas, destacam-se o Read.ai e o Microsoft 365 Copilot, que atuam na automação e análise de dados de reuniões e documentos. Contudo, junto com os benefícios vêm também responsabilidades: proteger os dados pessoais tratados por essas soluções e estar em conformidade com a LGPD é fundamental.

Além da legislação brasileira LGPD, normas internacionais como a ISO/IEC 42001:2023, voltada à governança de sistemas de IA, passam a ganhar importância no cenário corporativo global.

2. Read.ai

Segurança da Informação

O Read.ai armazena transcrições e análises de reuniões em servidores protegidos. A empresa afirma que os dados dos usuários não são usados no treinamento de seus modelos de IA, a menos que o usuário permita explicitamente.

Alguns pontos devem ser levantados em consideração:

- Utiliza criptografia em trânsito (TLS) e em repouso (AES-256).
- Parte dos recursos de segurança (ex: controle granular de acesso, logs de auditoria, retenção customizada) está disponível apenas em planos pagos (Enterprise+).
- O Read.ai **opera a partir dos EUA**, com transferência de dados internacionais, sem garantia clara de conformidade com requisitos da LGPD nesse ponto

Privacidade e LGPD

Apesar de apresentar uma política de privacidade e afirmar seguir normas como a GDPR (europeu), alguns relatos de usuários apontam falhas na prática, como dificuldades em excluir dados ou controlar acessos. O controle de compartilhamento dos relatórios é oferecido, mas faltam informações públicas mais claras sobre como os dados são gerenciados sob a ótica da legislação brasileira.

Alguns pontos devem ser levantados em consideração:

- Coleta extensiva de **dados pessoais e sensíveis**, incluindo voz, imagem, cargo, nome de usuário, comportamento e sentimentos dos participantes das reuniões.
- A ferramenta depende da **configuração do usuário para limitar ou controlar o compartilhamento**, mas **não exige consentimento ativo e estruturado dos participantes** das reuniões.
- Declara possibilidade de compartilhamento com terceiros, como prestadores de serviços, consultores e plataformas integradas (ex: Teams, Slack).
- A política de privacidade não assegura plena adequação à LGPD, especialmente quanto à retenção, exclusão e uso para melhoria de modelos de IA.
- Não há comprovação de anonimização/pseudonimização de dados.

Outras observações críticas

A ferramenta se integra ao Microsoft Teams como um aplicativo externo que acessa a infraestrutura do Office 365, **ampliando a superfície de ataque cibernético.**

A presença de um **"ouvinte artificial"** pode afetar a percepção psicológica e o comportamento dos colaboradores.

A ausência de controle centralizado pela organização permite que **dados confidenciais sejam processados sem supervisão adequada**, o que caracteriza **shadow IT** (uso de tecnologia sem governança).

Certificações

Até a data deste relatório, não foram encontradas evidências de que a plataforma possua a certificação ISO/IEC 42001:2023, voltada para sistemas de gestão de inteligência artificial.

3. Outras ferramentas similares ao Read.ai

Outras soluções que oferecem geração automática de atas de reuniões que apresentam a mesma fragilidade do Read.ai.

- Otter.ai;
- Fireflies.ai;
- Avoma;
- Fathom.

Crítica comum a todas essas ferramentas:

- Operam majoritariamente fora do Brasil, com servidores nos EUA ou outros países.
- Coletam áudio, transcrições, e metadados com práticas de segurança variadas.
- Raramente apresentam conformidade explícita com a LGPD.
- Têm termos de uso semelhantes ao Read.ai, com foco em treinamento de modelos e uso de dados para melhorias algorítmicas.

Portanto, são ainda menos recomendadas que o Read.ai, que ao menos declara certos controles básicos como criptografia e consentimento.

4. Microsoft 365 Copilot

Segurança da Informação

Por operar dentro do ecossistema Microsoft 365, o Copilot herda as práticas já consolidadas da empresa em termos de segurança e compliance. Os dados são acessados apenas conforme as permissões já definidas no Microsoft Graph, e não são utilizados para treinar os modelos de linguagem.

Alguns pontos devem ser levantados em consideração:

- Integrado ao ecossistema Microsoft 365, herda os controles de segurança avançados da plataforma, como criptografia nativa, autenticação multifator e conformidade com as políticas de dados corporativas via Microsoft Graph.
- Os dados utilizados não são empregados para treinar os modelos de IA.
- Residência e segregação de dados possível conforme região e regulação vigente.

Privacidade e LGPD

A Microsoft oferece recursos específicos para organizações que desejam se adequar à LGPD, como o Microsoft Priva, que permite monitorar e gerenciar dados pessoais. Há também formas automatizadas de atender aos direitos dos titulares, como acesso, correção e exclusão de dados.

Alguns pontos devem ser levantados em consideração:

- A Microsoft disponibiliza ferramentas como o **Microsoft Priva**, voltadas à gestão de dados pessoais, com suporte ao exercício dos direitos dos titulares.
- Possui fluxos automatizados para **acesso, correção, exclusão e rastreabilidade de dados**.

Certificações

Em 2024, o Copilot conquistou a certificação ISO/IEC 42001:2023, tornando-se uma das primeiras soluções no mundo a demonstrar conformidade com boas práticas internacionais para IA responsável.

5. Comparativo

Tabela comparativa com alguns dos critérios para a segurança dos dados em ferramentas com IA.

Critério	Read.ai	Microsoft 365 Copilot	Otter.ai	Fireflies.ai	Avoma	Fathom
Armazenamento de Dados	EUA, com criptografia	**Na nuvem do 365, pode ser regional**	EUA, com criptografia	EUA, com criptografia	EUA, com criptografia	EUA, com criptografia
Uso no Treinamento de IA	Apenas com consentimento explícito	**Não são usados para treinar modelos**	Sim, salvo indicação contrária do usuário	Sim, salvo ajustes na conta	Sim – dados usados para melhorar modelos	Sim – com termos amplos sobre uso para "melhorias"
Exercício de direitos LGPD	Relatos de dificuldades	**Ferramentas específicas para LGPD**	Limitado, foco na CCPA/GDPR	Não adaptado à LGPD	Requer contato manual, sem interface específica	Ausência de suporte claro à LGPD
Controle de Acesso	Definido pelo usuário	**Regido pelas permissões do Microsoft 365**	Controles por usuário e equipe, mas sem RBAC granular	Simples, sem integração com SSO corporativo	Controles administrativos disponíveis	Simples, não integrado ao controle de identidade corporativa
Certificação ISO 42.001	Não possui	**Certificada (2024)**	Não possui	Não possui	Não possui	Não possui
Residência de dados	Não informado	**Conformidade com regiões e soberania de dados**	Estados Unidos (sem opção de residência local)	Estados Unidos (sem opção de residência local)	Estados Unidos	Estados Unidos
Nível de Adequação à LGPD	Parcial, com diversos pontos críticos	**Alta adequação**	Inadequada – ausência de garantias específicas	Inadequada, ausência de cláusulas contratuais específicas	Inadequada, foco em mercado norte-americano	Inadequada, política genérica e permissiva
Governança de dados	Opaca e permissiva	**Alta – com documentação clara e controles internos**	Limitada, sem detalhamento sobre exclusão e auditoria	Superficial, foco em produtividade	Limitada a configurações básicas	Não possui

6. Conclusão

Tanto o Read.ai quanto o Copilot se propõem a oferecer recursos com foco em produtividade e segurança. No entanto, quando avaliados sob a ótica da LGPD e das boas práticas internacionais, o Copilot sai na frente. Além da robustez das ferramentas da Microsoft, há maior transparência quanto à gestão de dados e uma certificação internacional que válida a abordagem ética e responsável da empresa no uso de IA.

Já o Read.ai mostra boas intenções, mas peca na execução. A ausência de uma certificação como a ISO 42001 e a falta de informações claras sobre governança de dados reduzem a confiança para organizações que precisam de alto grau de conformidade.

Em suma: *para empresas brasileiras que buscam reduzir riscos legais e alinhar-se às exigências da LGPD, o Microsoft 365 Copilot representa, atualmente, uma escolha mais segura e estratégica.*

7. Crédito ao autor

Documento produzido por André Gouveia, Consultor de segurança da informação.

Mais de 15 anos de experiência em TI (Infraestrutura), Segurança da Informação e Governança de TI e em GRC.

Membro do Comitê Idcyber da ABNT, com trajetória no fortalecimento da maturidade em segurança da informação e na mitigação de riscos em ambientes complexos como setor bancário e de saúde.

Certificações de Destaque:
Certified AI Lead Implementer (IA Governança & Segurança); ISO/IEC 27001 Profissional (Segurança da Informação); ISO/IEC 27001 Lead Auditor; +2 anos de experiência em implementação de Sistemas de Gestão de Segurança da Informação (SGSI).

Compromisso com o Código de Ética:
Certified Information Security Officer (CISO) v2; Certified Data Protection Officer (DPO); ISO/IEC 27005 Risk Management; LGPD & GDPR Foundation; ISO/IEC 29100 Data Privacy Foundation.

8. Referências Bibliográficas

Brasil. Lei nº 13.709, de 14 de agosto de 2018 (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm .

ISO. ISO/IEC 42001:2023 – Artificial Intelligence Management Systems. https://www.iso.org/standard/81230.html

Microsoft. “Microsoft 365 Copilot Achieves ISO/IEC 42001 Certification.” Microsoft Tech Community, 2024. https://techcommunity.microsoft.com/blog/microsoft365copilotblog/microsoft-365-copilot-achieves-isoiec-420012023-certification/4397144

Microsoft. Documentação de privacidade e proteção de dados do Copilot. https://learn.microsoft.com

Read.ai. Política de Privacidade. https://www.read.ai/pt/privacidade

Read.ai. Visão geral de segurança. https://support.read.ai

Reddit. “Usuários relatam falhas de privacidade no Read.ai.” https://www.reddit.com/r/privacy/comments/1bjpz3q/warning_ai_company_readai_violates_privacy_rights/?tl=pt-br

Otter.ai – Privacy Policy https://otter.ai/privacy-policy

Fireflies.ai – Privacy Policy https://fireflies.ai/privacy

Avoma – Privacy Policy https://www.avoma.com/privacy

Avoma – Security Practices https://www.avoma.com/security

Fathom – Privacy Policy https://fathom.video/privacy

Fathom – Security Overview https://fathom.video/security