UNIVERSIDADE FEDERAL DA PARAIBA – UFPB
Centro de Ciências Sociais Aplicadas – CCSA
Graduação em Administração – GADM

ALGUNS IMPACTOS DA INTELIGÊNCIA ARTIFICIAL NA COMUNICAÇÃO ORGANIZACIONAL: CASO DA MOTOROLA SOLUTIONS

LUCAS MACÊDO DE OLIVEIRA LIMA

João Pessoa
Setembro,
2025

LUCAS MACÊDO DE OLIVEIRA LIMA

ALGUNS IMPACTOS DA INTELIGÊNCIA ARTIFICIAL NA COMUNICAÇÃO ORGANIZACIONAL: CASO DA MOTOROLA SOLUTIONS

Trabalho de Curso apresentado como parte dos requisitos necessários à obtenção do título de Bacharel em Administração, pelo Centro de Ciências Sociais Aplicadas, da Universidade Federal da Paraíba / UFPB.

Professora Orientadora:
Maria Camerina Maroja Limeira

João Pessoa
Setembro,
2025

Catalogação na publicação
Seção de Catalogação e Classificação

L732a Lima, Lucas Macedo de Oliveira.
Alguns impactos da inteligência artificial na comunicação organizacional: caso da Motorola Solutions / Lucas Macedo de Oliveira Lima. - João Pessoa, 2025.
28 f.

Orientação: Maria Camerina Maroja Limeira.
TCC (Graduação) - UFPB/CCSA.

1. Inteligência Artificial. 2. Comunicação organizacional. 3. Governança multidisciplinar. I. Limeira, Maria Camerina Maroja. II. Título.

UFPB/CCSA CDU 005(043)

Elaborado por ANDRE DOMINGOS DA SILVA FERNANDES - CRB-15/00730

Folha de aprovação

Trabalho apresentado à banca examinadora como requisito parcial para a Conclusão de Curso do Bacharelado em Administração

Aluno: Lucas Macêdo de Oliveira Lima

Trabalho: ALGUNS IMPACTOS DA INTELIGÊNCIA ARTIFICIAL NA COMUNICAÇÃO ORGANIZACIONAL: CASO DA MOTOROLA SOLUTIONS

Área de pesquisa: Tecnologia da Informação e Comunicação Organizacional

Data de aprovação: 23/09/2025

Banca examinadora

Profa Dra. Maria Camerina Maroja Limeira
Orientadora

Prof. Ms. Arturo Rodrigues Felinto
Avaliador

Profa. Dra. Sandra Leandro Pereira
Avaliadora

Dedico este trabalho ao meu pai (*in memoriam),* a pessoa que é a minha eterna inspiração e o meu maior exemplo de força.

AGRADECIMENTOS

Ao lembrar do garoto que entrou no curso de administração em maio de 2019, ansioso para adentrar em meio a uma jornada que daria início à sua vida no meio dos negócios e o comparo com a pessoa que sou hoje, vejo que fiz a escolha certa e sinto um orgulho interior imenso. Além disso, sinto gratidão por ter me permitido sonhar e começar a trilhar meu caminho com minhas próprias pernas, gratidão também a todos aqueles que cruzaram meu caminho direta ou indiretamente por todo o curso e me ensinaram muito sobre a administração e também sobre a vida, permitindo não somente que eu crescesse, mas também que eu aprendesse com cada um que cruzou meu caminho e com suas experiências.

Agradeço, primeiramente, ao meu pai, aquele que sempre foi minha maior inspiração e exemplo, um empreendedor nato, mas não só isso, um pai presente, um homem que dedicava sua vida à família, aquele que me ensinou a entender o valor das coisas na vida e a projetar os meus caminhos sem medo, sonhando, mas com os pés no chão. Ele é o dono da minha maior saudade e mesmo não estando mais aqui, me inspira e está comigo em todos os momentos, sejam difíceis ou de comemorações, de lutas ou de glória. Se cheguei até aqui, devo a ele, que nunca deixou de me incentivar e a desafiar meus próprios limites. Agradeço também à minha família, minha mãe e minha irmã, que estão comigo a todo tempo, pelo apoio incondicional e pelo incentivo, que jamais faltaram e foram combustível para a minha caminhada. E a Izabella, minha parceira de vida e confidente, que está comigo quase que desde o início do curso, sendo minha energia e porto seguro a todo tempo, aquela que sempre acreditou no meu potencial e me incentivou, nos momentos bons e nos ruins, inclusive no desenvolvimento deste trabalho.

Aos meus colegas de curso e amigos, que partilharam e trilharam esse caminho ao meu lado, de desafios e vitórias, minha eterna gratidão.

À OLM e a todos que fazem parte dessa empresa, essa que foi meu ponto de partida na jornada profissional, onde pude alinhar os conhecimentos obtidos no curso à vida empresarial na prática. Em especial quero agradecer ao meu tio Lula, a Fábio e a Bruno, que além de companheiros de trabalho, são família para mim, por estarem comigo no meu dia a dia, vivenciando desafios, aprendizados e vitórias.

E, claro, agradeço a todos os professores que estiveram comigo do início do curso até o TCC, com os quais pude aprender diariamente e que contribuíram demasiadamente para a minha formação. Em especial, agradeço à professora Maria Camerina, por todas as orientações dadas, dos estágios ao TCC. À professora Meiry, por todas as trocas que tivemos em sala de aula, as quais me instigaram a buscar ser melhor como homem e empreendedor. Ao professor Arturo, que sempre acreditou em mim e me ensinou bastante sobre a administração estratégica e sobre o empreendedorismo, que é o que eu amo fazer. Ao professor Fábio, pelas aulas sobre a administração da produção e em especial por me apresentar o livro “A Meta”, ajudando-me a entender com clareza a importância do trabalho em equipe e a necessidade da constante busca por vitórias, pessoais ou profissionais. Ao professor Vitor, pelas trocas nas aulas de filosofia, área que gosto bastante e que é essencial para o entendimento do ser humano e suas ações. Ao professor Jorge, que me ensinou no curso sobre tecnologia, área que atuo profissionalmente, permitindo-me fazer conexões entre o meio acadêmico e o meio profissional.

A todos, meu muito obrigado!

RESUMO

Este artigo tecnológico investiga alguns impactos da Inteligência Artificial (IA) na comunicação organizacional, tendo a Motorola Solutions como estudo de caso ilustrativo. O objetivo é compreender como a IA reconfigura fluxos de comunicação, tomada de decisão e gestão de segurança nas organizações, identificando ganhos, riscos e condições de sucesso. A pesquisa é de natureza aplicada, com abordagem descritivo-analítica, baseada em revisão de literatura e análise documental de relatórios corporativos, white papers e normativos recentes sobre IA. O contexto analisado evidencia a transição da Motorola Solutions de fornecedora de rádios de missão crítica para um ecossistema integrado de "segurança inteligente", combinando comunicações, vídeo-analytics, sensores e plataformas de comando com IA. O diagnóstico aponta quatro frentes de desafios: (i) técnico-operacionais (integração de dados e sistemas legados, qualidade/viés de dados, latência e resiliência); (ii) humanos e organizacionais (resistência à mudança, novas competências digitais, risco de desumanização da comunicação); (iii) ético-legais (privacidade, transparência, prestação de contas e conformidade regulatória); e (iv) de segurança digital e ciberameaças. A análise mostra soluções e boas práticas: plataformas unificadas com IA assistiva e humano no laço; computação de borda para reduzir latência; treinamento e gestão da mudança; e uma governança de IA "by design", com princípios claros, comitês multidisciplinares, métricas de qualidade/equidade, rotinas de auditoria e transparência para usuários (rótulos de IA e SOPs). Portanto, a IA eleva a eficácia comunicacional e a capacidade de resposta quando sustentada por governança robusta, segurança da informação e protagonismo humano. O estudo oferece um guia prático para gestores estruturarem a adoção responsável da IA na comunicação organizacional, equilibrando eficiência, ética e confiança.

Palavras-chave: Inteligência Artificial; Comunicação Organizacional; Governança Multidisciplinar.

LISTA DE SIGLAS

CNET	Computer Network
CONAR	Conselho Nacional de Autorregulamentação Publicitária
LAAD	Feira Latino-Americana de Defesa e Segurança
LGPD	Lei Geral de Proteção de Dados

SUMÁRIO

1 INTRODUÇÃO 7

2 CONTEXTO E REALIDADE INVESTIGADA 7

2.1 A IA na comunicação organizacional e segurança: panorama atual 7

2.2 Motorola Solutions e a era da IA em comunicações e segurança 9

3 DIAGNÓSTICO DA SITUAÇÃO-PROBLEMA E/OU OPORTUNIDADE 10

4 ANÁLISE DA SITUAÇÃO-PROBLEMA E PROPOSTAS DE INOVAÇÃO/INTERVENÇÃO/RECOMENDAÇÃO 12

4.1 Impactos da IA na comunicação organizacional interna e externa 12

4.2 Impactos da IA na vigilância inteligente e na privacidade 15

4.3 Impactos da IA na segurança digital e cibersegurança organizacional 18

4.4 Desafios éticos e de governança no uso organizacional de IA 21

5 CONCLUSÕES E CONTRIBUIÇÃO TECNOLÓGICA/SOCIAL 24

REFERÊNCIAS BIBLIOGRÁFICAS 25

1 INTRODUÇÃO

A ascensão da inteligência artificial (IA) nas últimas décadas tem provocado transformações profundas nos processos de comunicação das organizações. Comunicação organizacional, entendida como o conjunto das práticas de comunicação interna e externa de uma instituição, está passando por uma fase de reconfiguração impulsionada pelas novas tecnologias de IA (França & Oliveira, 2024). Ferramentas de IA estão sendo incorporadas para automatizar tarefas, analisar grandes volumes de dados e mesmo gerar conteúdo, alterando a maneira como empresas se comunicam com seus públicos e gerenciam informações (Barbosa & Portes, 2023). Ao mesmo tempo, aplicações de IA em vigilância inteligente e segurança digital trazem novas capacidades e desafios para a proteção de dados, pessoas e ativos, áreas cruciais em ambientes organizacionais contemporâneos.

A Motorola Solutions é uma empresa multinacional líder em comunicação de missão crítica e segurança. Com um histórico de 90 anos em soluções de rádio e, mais recentemente, investimentos em tecnologias de IA – como sistemas de vigilância por vídeo, análise de dados e assistentes virtuais, a empresa ilustra como a IA pode melhorar a eficiência da comunicação e a segurança, mas também evidencia preocupações éticas e organizacionais. A Motorola Solutions integrou IA em diversos produtos e processos, desde chatbots e assistentes para comunicação e comando, até câmeras de vigilância com analytics avançado e ferramentas de cibersegurança para proteção de redes (Sriram, 2025). Essas iniciativas buscam potencializar a tomada de decisão humana e antecipar riscos (Motorola Solutions, 2025a), refletindo uma tendência ampla nas organizações: usar a IA para fazer melho*r* o que já se faz, de forma mais rápida, integrada e inteligente (Motorola Solutions, 2019).

Por outro lado, a adoção acelerada da IA traz questões problemáticas que exigem reflexão. Como balancear ganhos de produtividade e qualidade na comunicação organizacional com a manutenção da ética e transparência? (Rego, 2024). Como aproveitar sistemas de vigilância inteligentes sem ferir a privacidade e os direitos civis? (Deloitte, 2021). E de que modo a segurança digital pode se fortalecer com IA, ao mesmo tempo em que novas ameaças impulsionadas por IA também emergem? O presente artigo investiga esses pontos de forma abrangente e crítica. Apresenta-se inicialmente o contexto e realidade investigada, situando a Motorola Solutions e o panorama da IA nas comunicações organizacionais. Em seguida, diagnostica-se a situação-problema e, na sequência, realiza-se uma análise detalhada dos impactos observados, subdividindo a discussão em Comunicação Organizacional, Vigilância Inteligente e Segurança Digital, além de considerar aspectos éticos transversais. Por fim, são apresentadas as conclusões e a contribuição tecnológica social deste estudo, ressaltando a importância de uma adoção responsável da IA para que seus benefícios à comunicação e à segurança sejam maximizados em prol da sociedade.

2 CONTEXTO E REALIDADE INVESTIGADA

2.1 A IA na comunicação organizacional e segurança: panorama atual

A incorporação de IA pelas organizações é uma realidade consolidada em escala global e nacional. Em 2022, uma pesquisa da IBM indicou que 41% das empresas brasileiras já utilizavam IA de alguma forma em seus processos de negócios (França & Oliveira, 2024). No campo específico da comunicação corporativa, a tendência também se confirma: um estudo da Associação Brasileira de Comunicação Empresarial (Aberje) revelou que 54% das organizações pretendiam utilizar algum tipo de IA em 2024, sendo que 36% já o faziam e 18% planejam começar (Aberje, 2024). As aplicações mais comuns concentram-se na produção de textos e

geração de insights para comunicação – por exemplo, 77% das empresas que adotam IA na comunicação usam ferramentas de IA generativa como o ChatGPT para redigir conteúdos ou apoiar na criatividade (Aberje, 2024). Além disso, ferramentas de apoio à escrita e revisão (como Grammarly, usada por 19% das empresas) têm ganhado espaço, assim como plataformas de automação de posts e análise de dados (Aberje, 2024).

Esse panorama reflete um movimento maior de digitalização da comunicação organizacional, apontado por estudiosos como parte de um novo paradigma (Saad, 2023). As tecnologias digitais conectadas – redes sociais, intranets, sistemas de colaboração – já haviam tornado a comunicação mais ágil e distribuída. A IA vem somar-se a esse contexto, introduzindo capacidades de automação e análise antes inimagináveis, ampliando a eficiência e o alcance das ações comunicativas (Kunsch, 2018). Em síntese, vivemos um momento em que a IA deixa de ser ideia futurista e se torna elemento tangível da gestão da comunicação e da segurança nas organizações (Borgonovo, 2024). Ferramentas como chatbots, assistentes virtuais, motores de recomendação e algoritmos preditivos vêm sendo implementadas gradualmente, abrindo um novo capítulo de "comunicação aumentada por máquinas" e segurança preditiva (Borgonovo, 2024). Entretanto, essa incorporação da IA traz consigo desafios significativos. Profissionais da área relatam preocupações quanto à falta de competências e clareza de responsabilidades para lidar com IA (Sebastião, 2020). Segundo o *European Communication Monitor 2019*, a maioria dos comunicadores europeus não teme tanto a perda de empregos pela automação, mas sim a necessidade de adaptação às novas habilidades exigidas e a definição de quem responde pelo que em um cenário com IA (Sebastião, 2020). Além disso, questões de ética e transparência são cada vez mais centrais: modelos de IA podem introduzir vieses ou erros que afetem a reputação e a confiança nas mensagens (Buolamwini & Gebru, 2018; Gonçalves, 2024). Casos concretos ilustram riscos – como a iniciativa do portal Computer Network (CNET), que publicou dezenas de artigos escritos por IA e teve que corrigir mais da metade deles por imprecisões e até trechos plagiados (Sato & Roth, 2023). Tal experimento mal conduzido gerou repercussão negativa e demonstrou que a comunicação organizacional não pode abrir mão da curadoria humana qualificada, sob pena de comprometer a credibilidade (Sato & Roth, 2023).

Paralelamente, no campo da segurança pública e corporativa, a IA vem sendo aplicada em sistemas de vigilância por vídeo, análise preditiva de crime e cibersegurança, levando ao conceito de "vigilância inteligente". Um levantamento de 2019 mostrou que 56 de 176 países já utilizavam algum sistema de IA para vigilância urbana (Deloitte, 2021). Cidades em todo o mundo adotaram câmeras inteligentes com reconhecimento facial e detecção de padrões suspeitos, bem como softwares de *predictive policing* (policiamento preditivo) para prever áreas e horários de maior probabilidade de crimes (Deloitte, 2021; Borgonovo, 2024). Na América Latina, por exemplo, grandes metrópoles como Rio de Janeiro, Buenos Aires e Cidade do México empregam IA para identificar veículos procurados e monitorar aglomerações em tempo real, otimizando a alocação de efetivo policial (Borgonovo, 2024). Empresas privadas também têm interesse nessas tecnologias para proteger instalações, controlar acessos e prevenir perdas.

Nesse domínio da segurança, os benefícios prometidos pela IA são uma reação mais rápida e até antecipação de incidentes. Sistemas modernos conseguem reduzir uma busca em imagens de vídeo de dias para poucos minutos, graças à identificação automática de pessoas ou objetos de interesse (Borgonovo, 2024). Alertas em tempo real podem ser enviados a autoridades quando uma câmera detecta comportamento anômalo, por exemplo alguém cruzando uma área restrita ou um pacote deixado sem dono (Borgonovo, 2024). Porém, aqui novamente emergem dilemas éticos e legais: o uso de reconhecimento facial pela polícia, por exemplo, tem sido criticado por vieses raciais que podem levar a falsas acusações contra minorias (Buolamwini & Gebru, 2018). Em regiões onde privacidade é valorizada, há resistência social e até proibição de certas tecnologias – como ocorreu em cidades dos EUA que baniram softwares de reconhecimento facial ou ferramentas preditivas por considerá-los uma ameaça às liberdades civis (Deloitte,

2021). Regulamentações começam a ser discutidas ou implementadas para equilibrar segurança e direitos: na Europa, a proposta de Lei de IA caminha nesse sentido, enquanto no Brasil a Lei Geral de Proteção de Dados (LGPD) e futuras leis específicas de IA buscam dar contornos legais ao uso dessas tecnologias.

2.2 Motorola Solutions e a era da IA em comunicações e segurança

A empresa a ser analisada neste trabalho será a Motorola Solutions Inc., por ser uma empresa parceira de uma empresa prestadora de serviços no Estado da Paraíba, de modo a ser realizado um diagnóstico de uma situação-problema desenvolvido no item 3, a seguir, deste trabalho.

A Motorola Solutions Inc., empresa originada da divisão da Motorola em 2011, é hoje uma das protagonistas globais em soluções de comunicação crítica, segurança pública e empresarial, tendo abraçado a IA como parte central de sua estratégia tecnológica. Com sede nos EUA e presença marcante no Brasil e América Latina, a Motorola Solutions atua fornecendo desde redes de rádio digitais, centrais de despacho de emergências (911/190), até sistemas de videomonitoramento e softwares de gerenciamento de evidências. Ao longo dos últimos anos, a empresa investiu em aquisições e inovações para incorporar IA a esse portfólio. Em 2018, adquiriu a Avigilon, especialista em câmeras de segurança e análise de vídeo por IA, e posteriormente empresas como a canadense Ava Security e a Openpath, focadas em soluções de vigilância e controle de acesso baseadas em nuvem e inteligência (Motorola Solutions, 2019; Revista Digital Security, 2021).

Esses movimentos posicionaram a Motorola Solutions na vanguarda da segurança inteligente conectada. Na Feira Latino-Americana de Defesa e Segurança (LAAD) 2019, no Rio de Janeiro, a empresa apresentou um sistema integrado de defesa e segurança que combinava sensores, câmeras fixas e corporais, rádios comunicadores, nuvem e softwares de análise com IA para criar "cidades mais seguras" (Motorola Solutions, 2019). Dentre as capacidades demonstradas estavam: software de análise baseado em IA capaz de localizar rapidamente veículos ou pessoas e emitir alertas de movimentações incomuns, usando *machine learning* para identificar padrões de comportamento suspeitos (Motorola Solutions, 2019). Também foi exibida a tecnologia Avigilon Appearance Search, um mecanismo de busca por imagens com IA que permite vasculhar horas de filmagens de vídeo e encontrar indivíduos ou veículos específicos em minutos (Motorola Solutions, 2019). Essas soluções mostraram na prática o potencial da IA em acelerar investigações e fornecer "consciência situacional" aprimorada para comandantes e agentes de campo (Motorola Solutions, 2019).

Mais recentemente, na Feira Latino-Americana de Defesa e Segurança (LAAD) 2025, a Motorola Solutions reforçou essa direção ao lançar um ecossistema de segurança potenciado por IA (Motorola Solutions, 2025a). Esse conjunto inclui câmeras de longo alcance com detecção térmica a 30 km (para vigilância de fronteiras), drones autônomos para mapeamento de áreas de risco, body cams com transmissão ao vivo e – crucial no contexto – serviços avançados de cibersegurança para proteger toda essa infraestrutura conectada (Motorola Solutions, 2025a). A empresa destacou que investe em IA tanto para proteger a linha de frente e melhorar a comunicação em missões críticas, quanto para reforçar a segurança cibernética de bases e redes, evitando acessos não autorizados ou interrupções em sistemas vitais (Motorola Solutions, 2025a). Essa visão integrada exemplifica como uma organização pode aplicar IA em várias camadas: dos dispositivos físicos (câmeras, rádios) às plataformas de software e nuvem, sempre com o objetivo de aumentar a eficácia, rapidez e resiliência das operações de comunicação e segurança.

Internamente, a Motorola Solutions também procura adotar IA de forma inovadora em seus processos. Em 2023, a empresa anunciou a *Assist*, sua IA de assistência para segurança pública, incorporada a diversos produtos (Motorola Solutions, 2023). E em maio de 2025, durante

sua conferência Summit, divulgou o Assist Chat, um chatbot de IA generativa desenvolvido para que profissionais de agências de segurança consultem dados da própria organização de modo conversacional (Motorola Solutions, 2025b). Essa ferramenta, oferecida sem custo a órgãos públicos dos EUA, conecta-se às bases de dados institucionais (registros de ocorrências, históricos de casos, vídeos etc.) e permite que despachantes, analistas ou policiais façam perguntas em linguagem natural e obtenham respostas rápidas, transcrições e insights, tudo em ambiente seguro e com conformidade a normas de sigilo (Motorola Solutions, 2025b). O Assist Chat ilustra como a IA pode auxiliar na comunicação interna de organizações de segurança: um fluxo de informação mais ágil entre sistemas e pessoas, reduzindo o tempo de busca e interpretação de dados. As expectativas são de melhora na tomada de decisão e ganho de tempo, já que o assistente automatiza tarefas repetitivas (como transcrever áudios ou compor relatórios) e libera os profissionais para focarem nas ações críticas e estratégicas (Motorola Solutions, 2025b). Ao mesmo tempo em que inova, a Motorola Solutions parece ciente das responsabilidades envolvidas. A empresa tem enfatizado publicamente princípios de IA responsável, declarando uma filosofia de *"human-in-the-loop"* (humano no circuito) para quaisquer decisões consequentes e buscando transparência nas aplicações de IA (Motorola Solutions, 2023). Em julho de 2025, anunciou a introdução de "rótulos nutricionais de IA" – os *AI Labels* – em todos os seus produtos de segurança que utilizam inteligência artificial, de modo a informar claramente o tipo de IA envolvida, sua finalidade, os dados que acessa e o grau de supervisão humana presente (Sriram, 2025; Medeiros, 2025). Essa iniciativa inédita no setor de segurança pública visa demistificar o papel da IA e construir confiança junto aos clientes e à sociedade, num momento em que a ética em IA está sob escrutínio global (Sriram, 2025). Os rótulos serão aplicados em itens como câmeras corporais, softwares de comando e controle e plataformas de análise de vídeo, tornando transparente "os ingredientes" de IA em cada produto (Medeiros, 2025). Trata-se de um exemplo claro de comunicação organizacional proativa da empresa: ao adotar voluntariamente uma medida de transparência, a Motorola Solutions não só atende às preocupações éticas, como também reforça sua imagem institucional de confiança e liderança responsável (Medeiros, 2025).

Esse conjunto de contextos – alta adoção de IA na comunicação corporativa em geral, e o caso específico da Motorola Solutions que incorpora IA em comunicação, vigilância e segurança – configura a realidade investigada deste artigo. O cenário é fértil em oportunidades, mas também carregado de tensões que precisam ser diagnosticadas e analisadas, conforme se detalha a seguir.

3 DIAGNÓSTICO DA SITUAÇÃO-PROBLEMA E/OU OPORTUNIDADE

Diante do contexto apresentado da empresa Motorola aqui estudada, pode-se delinear a situação-problema em torno de uma questão central: como integrar a inteligência artificial aos processos de comunicação organizacional e às práticas de segurança de forma eficiente e ética, garantindo benefícios sem comprometer valores fundamentais? Essa problemática desdobra-se em quatro eixos específicos, a seguir:

1 • Otimização vs. Substituição na comunicação: As organizações buscam otimizar suas comunicações internas e externas com IA, automatizando tarefas e ganhando velocidade nas interações. Chatbots, por exemplo, já atendem clientes e funcionários em diversas empresas 24 horas por dia, fornecendo informações imediatas (Aberje, 2024). O Banco do Brasil, desde 2018, utiliza chatbot para responder cerca de 70% dos atendimentos em suas redes sociais, agilizando o suporte ao cliente (França & Oliveira, 2024). Contudo, surge o desafio de até que ponto essa automação pode substituir ou degradar o contato humano. Há receios de despersonalização das mensagens, ou mesmo da perda de empregos em comunicação, ainda que estudos indiquem que o maior desafio é requalificar profissionais para trabalhar com as novas ferramentas (Sebastião, 2020). Assim, o problema aqui é equilibrar

a eficiência trazida pela IA (respostas mais rápidas, produção de conteúdo em escala) com a manutenção da qualidade relacional e humana na comunicação, algo essencial para engajamento e confiança dos públicos.

2 • Segurança aprimorada vs. Privacidade e liberdades: No âmbito da vigilância inteligente, a IA promete cidades e instalações mais seguras, mas coloca em questão direitos individuais. A Motorola Solutions exemplifica a dualidade: oferece câmeras e algoritmos que identificam suspeitos e padrões criminosos com rapidez inédita (Motorola Solutions, 2019; Borgonovo, 2024), contribuindo para prevenir incidentes – o que é claramente desejável do ponto de vista social. Porém, os mesmos sistemas podem ser percebidos como intrusivos ou discriminatórios. Sistemas de reconhecimento facial já erraram desproporcionalmente com pessoas negras, por exemplo, devido a vieses nos dados de treinamento, levando a reconhecimentos equivocados (Buolamwini & Gebru, 2018). Outro caso preocupante é o uso de IA para "reviver" digitalmente pessoas falecidas em campanhas, como a propaganda da Volkswagen que recriou a voz e imagem da cantora Elis Regina; a ação gerou polêmica ética e foi objeto de processo pelo Conselho de Autorregulamentação Publicitária (CONAR) após queixas do público (BBC News Brasil, 2023). Essas situações demonstram o dilema: até onde usar IA para segurança ou comunicação sem violar limites éticos e legais? A situação-problema aqui envolve criar mecanismos de controle, regulação e transparência para que os ganhos em segurança não signifiquem vigilância abusiva ou uso indevido da imagem/dados das pessoas.

3 • Confiabilidade e qualidade das decisões automatizadas: Com IA integrando-se na comunicação e segurança, cresce a dependência das organizações nas saídas geradas pelos algoritmos. Isso levanta questões sobre a confiabilidade dessas decisões/recomendações. Por exemplo, se um assistente de IA resumir um relatório de ocorrência para um gestor, ele confiará cegamente nesse resumo? Se uma câmera inteligente der um alerta de intrusão, a equipe de segurança agirá imediatamente com base nele – e se for um falso positivo? O problema identificado é que sistemas de IA, apesar de poderosíssimos, não são infalíveis: podem apresentar erros, vieses ou limitações contextuais (O'Neil, 2016). Logo, as organizações precisam evitar tanto a superconfiança ingênua na IA (risco de decisões erradas sem revisão humana) quanto a subutilização por desconfiança excessiva. Encontrar esse ponto de equilíbrio requer políticas claras: manter sempre um humano validando decisões críticas (Motorola Solutions, 2023), estabelecer critérios de qualidade e treinamento dos modelos, e prover forma de auditoria nas ações da IA (Rego, 2024). A Motorola Solutions, ao adotar rótulos informativos sobre a IA nos produtos, está justamente tentando aumentar essa confiabilidade via transparência – usuários sabendo o que a IA faz e sob quais condições (Sriram, 2025).

4 • Segurança digital e ciberameaças: A crescente digitalização e inteligência nos sistemas também amplifica a superfície de ataque cibernético. Ironicamente, a IA que protege também pode ser explorada por atacantes habilidosos. Hackers podem usar ferramentas de IA generativa para automatizar criação de *malware*, *phishing* e outras ameaças em escala (Malwarebytes, 2023). Portanto, as organizações enfrentam a situação de ter que adotar IA para se defender de IA: uma corrida onde quem não investe em segurança com IA fica vulnerável às investidas de criminosos que usam IA para encontrar brechas (Ponemon Institute, 2024). No diagnóstico, identifica-se que muitas empresas ainda estão amadurecendo na adoção de IA para cibersegurança – apenas 18% no estudo do Ponemon de 2024 disseram ter implantações de IA de segurança totalmente operacionais e metrificadas (Ponemon Institute, 2024). Ou seja, há um caminho a percorrer para as organizações aprenderem a gerir riscos de IA (como proteger seus algoritmos contra manipulação de dados ou roubo de modelos) e a usar IA como aliada na detecção de ameaças. A Motorola Solutions, por exemplo, incluiu serviços de cibersegurança em seu

portfólio e destaca a necessidade de resiliência digital em seu ecossistema (Motorola Solutions, 2025a). O problema é que a evolução das ameaças é muito dinâmica, exigindo atualizações constantes e pessoal capacitado para supervisionar os sistemas de IA de defesa (Ponemon Institute, 2024).

Em resumo, o diagnóstico evidencia que o potencial transformador da IA vem acompanhado de riscos e desafios que não podem ser ignorados. A situação atual nas organizações – e explicitamente no caso da Motorola Solutions – mostra avanços promissores em eficiência comunicacional, capacidade de vigilância e robustez de segurança. Contudo, emergem pontos problemáticos: a necessidade de competências humanas atualizadas, o imperativo de ética e transparência, a importância da governança de IA para evitar abusos, e a urgência de proteções cibernéticas à altura das novas ameaças. Esta análise situacional aponta, assim, para a exigência de uma abordagem equilibrada e responsável na integração da IA, tema que será aprofundado a seguir na análise dos impactos concretos em cada esfera (comunicação, vigilância e segurança digital).

4 ANÁLISE DA SITUAÇÃO-PROBLEMA E PROPOSTAS DE INOVAÇÃO/INTERVENÇÃO/RECOMENDAÇÃO

Com base no contexto e nos desafios diagnosticados no item anterior, esta seção aprofunda os impactos da IA na comunicação organizacional e nas áreas correlatas de vigilância inteligente e segurança digital, utilizando a Motorola Solutions como fio condutor. A análise está estruturada em subitens, refletindo os principais tipos de impactos observados e as devidas recomendações.

4.1 Impactos da IA na comunicação organizacional interna e externa

A introdução de ferramentas de IA na comunicação organizacional tem impactos multifacetados: ao mesmo tempo em que potencializa a eficiência e a personalização, também exige adaptações culturais e cuidados éticos. Do lado positivo, um dos impactos mais notáveis é a automação de processos comunicacionais repetitivos, liberando os profissionais para atividades mais estratégicas. Chatbots e assistentes virtuais ilustram esse ganho: eles conseguem atender funcionários e clientes em tempo real, respondendo dúvidas frequentes ou fornecendo informações padronizadas sem intervenção humana (Screencorp, 2024). Isso agiliza o fluxo de comunicação. Por exemplo, um colaborador pode perguntar a um chatbot interno sobre política de férias ou benefícios e obter resposta imediata, ao invés de aguardar retorno do RH. Esse uso de IA melhora a agilidade comunicacional interna e reduz a sobrecarga de equipes de atendimento (Screencorp, 2024). Como benefício adicional, chatbots funcionam 24/7, aumentando a disponibilidade de suporte (França & Oliveira, 2024). A Motorola Solutions ainda não divulgou uso de chatbots corporativos específicos, mas sua iniciativa Assist Chat em órgãos de segurança é análoga: trata-se de um *bot* que permite aos membros da organização consultarem informações rapidamente, mostrando como a lógica vale também em ambientes institucionais (Motorola Solutions, 2025b).

Outro impacto importante está na qualidade e consistência das mensagens. Ferramentas de IA de apoio à redação (como corretores e geradores de texto) contribuem para padronizar comunicados e evitar erros. Empresas têm utilizado IA para revisar textos de newsletters, e-mails ou relatórios internos, garantindo uma comunicação escrita mais clara e livre de deslizes gramaticais (Screencorp, 2024). Isso profissionaliza a comunicação e economiza tempo das equipes. A IA também consegue sugerir melhorias estilísticas ou adequação de tom, adaptando a mensagem ao público-alvo com base em aprendizado prévio. Em comunicações externas, *softwares* de inteligência artificial ajudam a analisar grandes volumes de dados de consumidores (redes sociais, feedbacks) e gerar insights sobre tendências e preferências,

permitindo que a empresa ajuste seu conteúdo para maior relevância (Girardi & Pase, 2024). Ferramentas de análise de sentimento, por exemplo, vasculham milhares de menções à marca nas redes e indicam aos comunicadores se a percepção é positiva ou negativa, orientando campanhas de relações públicas de forma mais embasada.

A personalização em escala é outro impacto fundamental: algoritmos de IA permitem enviar mensagens adaptadas a diferentes perfis de empregados ou clientes. No contexto interno, já existem aplicações que determinam o melhor horário para enviar determinados comunicados a cada área, ou que segmentam o conteúdo conforme o cargo, localização ou interesses do colaborador (Screencorp, 2024). Isso aumenta o engajamento, pois cada funcionário recebe informações mais pertinentes (Screencorp, 2024). Externamente, empresas como a Starbucks exemplificam o uso de IA para personalizar ofertas: através de aplicativos que coletam preferências de compra e horários de consumo, a Starbucks empregou algoritmos para enviar promoções sob medida aos clientes, aumentando a satisfação e as vendas (Marr, 2018). Esse caso ilustra como a IA contribui para novas formas de relacionamento com o público – no caso, o marketing one-to-one – o que se enquadra na comunicação organizacional mercadológica (França & Oliveira, 2024). Outro exemplo notável de personalização é a *Lu do Magalu*, influenciadora virtual criada pela Magazine Luiza usando tecnologias de IA e computação gráfica. Ela interage de forma "humanizada" com consumidores nas redes sociais, tornou-se um ícone da marca e ajudou a construir uma imagem corporativa moderna e positiva (França & Oliveira, 2024). Isso mostra que a IA também impacta a comunicação institucional e de marca, oferecendo novos personagens e narrativas para engajar o público.

Porém, juntamente com essas melhorias, emergem impactos desafiadores. Um deles é o risco de desinformação e erros na comunicação quando confiada cegamente à IA. Modelos de linguagem avançados (como os usados para gerar textos) podem produzir informações incorretas com aparência de verdade – o fenômeno das "alucinações" do modelo. Se uma empresa usar IA generativa para redigir um comunicado de imprensa, por exemplo, precisa revisar cuidadosamente os fatos. O incidente do Computer Network (CNET) citado (Sato & Roth, 2023) alerta que a implantação descuidada de IA na produção de conteúdo pode minar a confiabilidade da comunicação organizacional. Erros factuais e até plágios passaram despercebidos inicialmente, exigindo correções posteriores e dano reputacional. Portanto, as organizações devem estabelecer processos de revisão humana e validação de tudo que a IA produzir antes de divulgar publicamente (Sato & Roth, 2023). A Motorola Solutions, atenta a isso, adota o princípio de que usuários devem se manter informados das decisões da IA e manter controle– ou seja, nenhuma saída de IA substitui o juízo humano em decisões consequentes (Motorola Solutions, 2023). Esse alinhamento com a ideia de IA como apoio, não substituição, é crucial para evitar comunicações enganosas ou inadequadas.

Outro impacto delicado se relaciona à ética e privacidade na comunicação com IA. Ferramentas de análise de perfil e monitoramento interno alimentadas por IA podem gerar preocupações entre funcionários. Se a empresa começa a analisar todas as mensagens internas, e-mails ou chats com IA para medir "engajamento" ou "humor" dos colaboradores, isso pode ser percebido como invasão de privacidade e vigilância indevida (Magnolo & Whitaker, 2024). Há relato de organizações usando IA para acompanhar produtividade em mensagens, ou até para prever comportamentos de empregados, o que pode minar a confiança e criar um ambiente de trabalho tenso (Magnolo & Whitaker, 2024). Portanto, o impacto da IA interna precisa ser moderado por políticas claras de proteção de dados dos colaboradores e transparência sobre o que está sendo monitorado. A Screencorp (2024) recomenda exatamente isso: garantir privacidade e promover diálogo transparente sobre como a IA é usada na comunicação interna, de modo que os funcionários compreendam os objetivos (por exemplo, melhorar fluxos, não punir indivíduos). Além disso, sugerem-se treinamento e adaptação cultural, preparando líderes e equipes para colaborarem com ferramentas de IA, sem medo, mas com consciência dos limites e melhores

práticas (Screencorp, 2024). Em suma, a inserção da IA deve vir acompanhada de governança: códigos de conduta para uso de IA, diretrizes de quando se requer aprovação humana, e esforços de aculturamento digital.

Um impacto psicológico e organizacional, por fim, merece menção: a IA traz uma mudança de paradigma profissional na comunicação. Profissionais de RP, jornalismo corporativo, marketing interno – todos precisam evoluir seu papel. Em vez de redatores ou distribuidores de informação, passam a atuar como curadores, estrategistas e treinadores da IA. Girardi & Pase (2024) observaram em estudo que a adoção de ferramentas como ChatGPT na área exige que os comunicadores forneçam contexto e orientações muito claras para obter resultados úteis, o que demanda novas habilidades. Além disso, notaram que o uso eficaz desses sistemas demanda uma mudança de mentalidade profissional, abrindo-se à colaboração com a máquina e aprendendo a avaliar criticamente o que ela produz (Girardi & Pase, 2024). Ou seja, a IA não elimina a profissão de comunicador, mas transforma as competências-chave – a chamada "mudança de paradigma". A Motorola Solutions e outras empresas de tecnologia têm investido em centros de inovação e treinamento exatamente para capacitar seus times em IA. A empresa inclusive criou um comitê interno (MTAC) para alinhar o desenvolvimento de IA com valores e propósitos organizacionais (Motorola Solutions, 2023). Isso indica que, do ponto de vista do impacto organizacional interno, a IA leva as empresas a instituir novos fóruns de discussão ética, novos papéis (como cientistas de dados atuando junto com comunicadores) e novas rotinas de aprovação de conteúdo gerado automaticamente.

Em síntese, na comunicação organizacional a IA traz impactos positivos expressivos em agilidade, alcance e personalização das mensagens, bem como na eficiência operacional ao automatizar tarefas. Entretanto, esses ganhos acompanham responsabilidades e riscos: a necessidade de manter a comunicação confiável e humanizada, de resguardar a privacidade de todos os envolvidos e de capacitar os profissionais para trabalharem lado a lado com as inteligências artificiais. Empresas como a Motorola Solutions, que usam a IA inclusive para se comunicar sobre seus produtos de IA (vide os rótulos nutricionais), demonstram que a transparência e a ética na comunicação potencializada por IA não são obstáculos, mas sim condições essenciais para o sucesso sustentável dessa integração. Em última instância, a IA na comunicação organizacional deve ser empregada como uma ferramenta para empoderar a comunicação humana, não para silenciá-la ou substituí-la (Rego, 2024). Com essa premissa, as organizações podem colher os frutos tecnológicos sem perder de vista sua identidade e responsabilidade social.

Perante a integração de IA na comunicação, recomenda-se que a Motorola implemente programas contínuos de educação digital voltados ao "como usar, quando usar e quando não usar" essas ferramentas. Esses programas devem combinar prática (workshops curtos, simulações e guias de bolso) com reflexão crítica sobre ética, transparência, vieses e possíveis efeitos psicológicos das mensagens automatizadas. A mensagem central precisa ser explícita: a IA é parceira estratégica que apoia o trabalho humano — não o substitui.

Recomenda-se, ainda, estabelecer trilhas de treinamento contínuas do básico ao avançado, cobrindo operação das ferramentas, leitura crítica de saídas (detecção de vieses e erros factuais) e proteção de dados. Para tornar o processo consistente e auditável, recomenda-se adotar checklists de revisão humana antes de publicar, protocolos de resposta a incidentes e métricas simples de acompanhamento (por exemplo: retrabalho por erro da IA e tempo de resposta a correções).

Para preservar autenticidade e confiança, recomenda-se adotar uma estratégia híbrida: automatizar o operacional (triagem, rascunhos, sínteses) e reservar às pessoas o que exige nuance — mensagens estratégicas, temas sensíveis e comunicações que pedem empatia. Recomenda-se também rotular claramente conteúdos "assistidos por IA" e definir pontos obrigatórios de intervenção humana ao longo do fluxo de comunicação.

Por fim, recomenda-se alinhar essas práticas a valores institucionais por meio de políticas internas claras e comunicações periódicas sobre limites e boas práticas. Com esse conjunto — educação contínua, revisão humana, métricas e transparência — a Motorola amplia inovação sem abrir mão de seus princípios, reforçando a confiança de públicos interno e externo.

4.2 Impactos da IA na vigilância inteligente e na privacidade

No domínio da vigilância inteligente, que engloba a utilização de IA em sistemas de monitoramento, segurança física e policiamento, os impactos são profundos e dualísticos. A tecnologia tem aprimorado consideravelmente a capacidade de prevenir incidentes e responder a emergências, mas simultaneamente levanta preocupações sobre privacidade, equidade e direitos civis. Os impactos positivos mais evidentes residem na ampliação do alcance e da precisão do monitoramento. Câmeras dotadas de algoritmos de visão computacional podem analisar em tempo real dezenas ou centenas de fluxos de vídeo, algo humanamente impossível. Isso significa que em uma cidade ou instalação vigiada, a IA consegue "assistir" a todos os cantos simultaneamente, detectando eventos relevantes automaticamente – por exemplo, identificar uma pessoa portando arma em local público, reconhecer uma placa de veículo roubado que passa por uma rodovia monitorada, ou perceber comportamentos atípicos como alguém deixando um pacote em área sensível (Borgonovo, 2024). A Motorola Solutions, via sua linha Avigilon, implementou exatamente essas capacidades: suas câmeras inteligentes diferenciam objetos (pessoas, veículos etc.) e emitem alertas instantâneos para operadores ao notar ocorrências potencialmente críticas (Motorola Solutions, 2019; 2025a). O impacto disso na segurança é enorme: redução do tempo de resposta e, muitas vezes, prevenção proativa. Se uma plataforma analítica sinaliza uma aglomeração fora do normal se formando num evento, a polícia pode intervir antes que vire tumulto. Se um suspeito for flagrado por câmeras ao entrar num prédio corporativo, a segurança pode contê-lo antes de qualquer dano. Esse tipo de inteligência preditiva representou um salto de paradigma – do modelo reativo (ver o crime depois de ocorrer, nas filmagens) para um modelo proativo (acionar recursos durante ou até antes do incidente). Em experimentos em cidades latino-americanas, a IA apontou regiões e horários quentes de crimes permitindo planejar policiamento preventivo, resultando na diminuição de ocorrências em algumas localidades (Borgonovo, 2024).

Além da rapidez, outro impacto positivo é a objetividade dos registros e análises. Diferentemente de um vigia humano que pode se distrair ou se cansar, a IA "não pisca" nem perde foco – analisando dados continuamente (Motorola Solutions, 2019). Isso aumenta a probabilidade de flagrantes e reduz a falha humana. Tecnologias como sensores acoplados a armas (que acionam câmeras automaticamente ao sacar, por exemplo) garantem registro auditável de eventos críticos (Motorola Solutions, 2019). Esse monitoramento automatizado pode proteger tanto cidadãos quanto agentes, fornecendo evidências confiáveis (vídeos, áudio) que servem para esclarecer fatos e aumentar a transparência das operações de segurança. Por exemplo, com câmeras corporais inteligentes (bodycams) que iniciam gravação diante de certas condições definidas por IA (como detecção de briga ou corrida), constrói-se uma "caixa-preta" da ação policial, coibindo abusos e também defendendo os policiais de falsas acusações (Motorola Solutions, 2019). Nesse sentido, a vigilância inteligente, se bem implementada dentro de protocolos éticos, pode inclusive fortalecer a confiança pública nas instituições de segurança, por demonstrar compromisso com responsabilidade.

No ambiente corporativo, a vigilância inteligente com IA auxilia na proteção patrimonial e na segurança do trabalho. Câmeras de fábricas ou escritórios podem, por exemplo, detectar intrusão fora do horário de expediente, identificar falta de uso de EPI (equipamento de proteção) por funcionários em áreas perigosas, ou reconhecer faces para controle de acesso sem contato. A IA permite diferenciar condições – uma pessoa desconhecida pulando um muro acionará alarme,

mas um funcionário autorizado passando normalmente não (depois do devido treinamento do modelo e integração com sistemas de identidade). Isso reduz falsos alarmes e foca a atenção dos seguranças no que realmente importa. Empresas que lidam com infraestrutura crítica (usinas, data centers) já adotam vigilância inteligente para antever riscos de sabotagem ou acidentes, integrando dados de câmeras, sensores e clima para, por exemplo, detectar princípio de incêndio pela combinação de imagem (fumaça) e elevação de temperatura, antes mesmo do alarme tradicional disparar. Esse monitoramento ampliado por IA protege vidas e bens, constituindo um impacto claramente benéfico.

Contudo, os impactos adversos e os riscos inerentes à vigilância inteligente também são significativos. O primeiro e talvez mais debatido é o potencial atentado à privacidade e à liberdade individual. Uma rede de câmeras com reconhecimento facial em toda uma cidade pode significar que cidadãos são continuamente identificados e rastreados em seus deslocamentos cotidianos, mesmo sem estarem cometendo delito algum. Isso configura uma vigilância massiva que muitos consideram incompatível com sociedades livres (Deloitte, 2021). Há temores de que, sem controles rigorosos, governos ou corporações utilizem esses sistemas para fins indevidos, como perseguir opositores, discriminar grupos ou simplesmente lucrar com dados pessoais (Couldry & Yu, 2018). No contexto organizacional, um empregador que instale câmeras com IA para monitorar constantemente cada movimento de seus colaboradores pode gerar um clima de opressão e desconfiança, além de esbarrar em limites legais trabalhistas e de privacidade (Magnolo & Whitaker, 2024). Assim, a linha tênue entre segurança e vigilância excessiva precisa ser gerenciada. O impacto negativo aqui seria a erosão de direitos e a possibilidade de efeito inibidor: pessoas mudando seu comportamento (deixando de exercer liberdades como manifestar-se publicamente ou mesmo ser criativas no trabalho) pelo medo de estarem sendo constantemente vigiadas – a chamada "espiral do silêncio tecnológica" (Karhawi et al., 2024).

Outro impacto problemático é a possibilidade de viés e injustiça algorítmica na vigilância. Se os algoritmos de detecção de suspeitos são treinados com bases de dados tendenciosas, podem focar desproporcionalmente em certos perfis (Buolamwini & Gebru, 2018). Há evidências de sistemas de reconhecimento facial comerciais que apresentaram taxas de erro 35% maiores para mulheres negras em comparação a homens brancos, devido à sub-representação de faces negras no treinamento (Buolamwini & Gebru, 2018). Isso implica que comunidades já marginalizadas poderiam ser alvo mais frequente de abordagens policiais por falsos positivos da IA – intensificando preconceitos sistêmicos em vez de mitigá-los (Lum & Isaac, 2016). Também, algoritmos preditivos treinados em dados históricos de crime tendem a "prever o passado", apontando sempre os mesmos bairros (geralmente pobres e de maioria étnica minoritária) como focos de crime, simplesmente porque no passado a polícia incidiu mais lá e gerou mais registros (Lum & Isaac, 2016; O'Neil, 2016). Isso pode gerar um ciclo vicioso de superpoliciamento de certos grupos e regiões, aumentando desigualdades e tensões sociais. Portanto, um impacto adverso da vigilância inteligente mal calibrada é a perpetuação de vieses e injustiças, minando a legitimidade dos esforços de segurança. No caso da Motorola Solutions, a empresa tenta abordar esse risco enfatizando governança e supervisão humana – por exemplo, em seu guia de IA afirma que sistemas de reconhecimento facial e outras decisões críticas mantêm um "humano no circuito" antes de qualquer ação (Motorola Solutions, 2023). Ainda assim, a simples presença da funcionalidade gera debates públicos, e muitos defendem restrições ao uso dessa tecnologia até que se garanta acurácia e ausência de discriminação (Deloitte, 2021).

Há também preocupações quanto ao armazenamento seguro dos dados de vigilância. Com mais sensores e vídeos gravando tudo, cria-se um enorme volume de dados sensíveis. Se esses dados caem em mãos erradas por falha de segurança digital, podem ser usados maliciosamente (Malwarebytes, 2023). Imagens de pessoas podem ser vazadas, registros de movimentação expostos etc. Assim, a vigilância inteligente requer concomitantemente um investimento forte em cibersegurança, senão os mesmos recursos que protegem podem se converter em vetores de

ataque ou abuso (Ponemon Institute, 2024). O impacto negativo aqui seria a sensação de vulnerabilidade: cidadãos e funcionários passam a se preocupar não só em estar sendo filmados, mas também com quem poderia acessar essas filmagens sem autorização. A Motorola Solutions busca mitigar isso oferecendo soluções de armazenamento seguro e criptografia para seus sistemas de evidências digitais (Motorola Solutions, 2019), mas incidentes como o vazamento de conversas do próprio ChatGPT em 2023 (quando uma falha permitiu usuários verem histórico de outros) mostram que mesmo grandes provedores estão sujeitos a falhas (OpenAI, 2023 apud França & Oliveira, 2024). Logo, a confiança do público nos sistemas de vigilância inteligente está condicionada à capacidade das organizações de garantir a segurança e uso responsável dos dados coletados.

Por fim, há um impacto social e psicológico mais amplo: a normalização da vigilância. Se as pessoas se acostumam a ser vigiadas o tempo inteiro, pode ocorrer uma mudança cultural de menor valorização da privacidade, ou uma apatia em relação a isso ("não tenho nada a esconder, então tanto faz"). Tal normalização pode abrir caminho para menos resistência a medidas autoritárias e um enfraquecimento do controle democrático sobre quem observa quem (Zuboff, 2019). Esse é um efeito difuso, mas potencialmente pernicioso a longo prazo. Por isso, muitos especialistas insistem na necessidade de debates éticos e regulamentação transparente sempre que se introduz IA em vigilância (Deloitte, 2021; Rego, 2024). Cidades como Nova York exigem por lei que a polícia divulgue publicamente quais tecnologias de vigilância utiliza e suas finalidades (Deloitte, 2021). No Brasil, o uso de câmeras com reconhecimento facial em locais públicos está sob análise de órgãos como o Ministério Público em diversos estados, buscando avaliar sua proporcionalidade e legalidade. O Conselho Nacional de Autorregulamentação Publicitária (CONAR), mencionado antes, é outro exemplo de instância reguladora reagindo a usos de IA: embora focado em publicidade, ao questionar o anúncio com IA da Volkswagen, tocou em um ponto ético essencial sobre o consentimento e os limites do uso de imagens de pessoas (BBC News Brasil, 2023). Isso demonstra que a sociedade está atenta e cobrando freios e contrapesos.

Em conclusão, os impactos da IA na vigilância inteligente delineiam um quadro de ganhos substanciais em segurança e eficiência, representados pelo caso Motorola Solutions com suas soluções integradas, mas também de riscos significativos à privacidade e à equidade. A situação-problema aqui se resolve – ou ao menos se mitiga – com governança responsável da tecnologia: incluindo transparência (como os AI Labels de Motorola Solutions), auditorias independentes para detecção de vieses, envolvimento da comunidade e respeito às leis de proteção de dados. Se bem administrada, a vigilância inteligente pode cumprir sua promessa de cidades e empresas mais seguras sem suprimir direitos. Do contrário, os impactos negativos podem eclipsar os positivos, gerando resistências que inviabilizem a adoção dessa tecnologia. (Zerfass et al., 2019) mencionam que sem aceitação pública, até o melhor sistema de comunicação falha. A balança entre segurança e liberdade, portanto, precisa ser continuamente calibrada pelos gestores organizacionais e poderes públicos, na era da IA.

A Motorola pode criar espaços realmente participativos para decidir sobre o uso de vigilância inteligente com IA. Em vez de decisões tomadas apenas por áreas técnicas, conselhos consultivos poderiam se reunir periodicamente com gente da sociedade civil, especialistas e reguladores, olhando casos concretos, avaliando riscos e benefícios e registrando o que for decidido em atas públicas. Esse arranjo aproxima a decisão de quem sente os efeitos da tecnologia no dia a dia e dá previsibilidade: fica claro o que a IA pode ou não fazer, por quê e com base em quais salvaguardas. Na prática, a vigilância deixa de ser só "mais segurança" e passa a ser um bem coletivo, em que proteção e privacidade são discutidas e equilibradas de forma democrática.

Para sustentar esse processo, programas robustos de compliance digital fazem diferença. O caminho inclui mapear fluxos de dados, auditar algoritmos com regularidade, publicar relatórios de impacto (em linguagem acessível) e adotar protocolos claros para dados sensíveis — quem acessa, por quanto tempo, com qual finalidade e como revoga consentimentos quando

couber. Transparência não é um apêndice: ela reduz o medo de abuso, qualifica o debate público e consolida a percepção da tecnologia como instrumento legítimo de segurança, e não como ameaça às liberdades civis.

Outro pilar é a formação. Não basta treinar o operador do sistema; gestores e lideranças precisam entender ética algorítmica, privacidade e vieses nos dados para tomar boas decisões sob pressão. Treinamentos curtos e recorrentes, estudos de caso ajudam a transformar princípio em prática: quando parar uma análise automatizada, quando escalar para revisão humana, como justificar uma decisão a um cidadão. Equipes assim ganham autonomia e responsabilidade — e a cultura absorve o tema, em vez de tratá-lo como obrigação externa.

Por fim, comunicação e engajamento contínuos evitam a sensação de vigilância opressiva. Projetos devem explicar, de forma simples, objetivos, limites e funcionamento dos sistemas; sinalizar quando e onde há coleta ou análise; abrir canais para dúvidas e contestação; e fechar o ciclo com devolutivas sobre ajustes feitos a partir do feedback das comunidades. Quando a sociedade vê que pode perguntar, ser ouvida e influenciar, a tecnologia deixa de parecer imposição unilateral e passa a ser um esforço compartilhado por segurança com respeito à privacidade.

4.3 Impactos da IA na segurança digital e cibersegurança organizacional

À medida que as organizações incorporam IA em seus sistemas e operações, elas se deparam também com impactos expressivos da IA no domínio da segurança digital – isto é, na proteção contra ameaças cibernéticas, na integridade de dados e na continuidade dos serviços de TI. Aqui novamente observa-se dois lados: a IA surge como uma ferramenta poderosa para defesa cibernética, mas simultaneamente viabiliza ofensivas cibernéticas mais sofisticadas, configurando uma espécie de corrida armamentista digital. Do ponto de vista da defesa, o impacto da IA em cibersegurança tem sido elevar a capacidade de detecção e resposta a ataques a patamares inéditos. Em redes corporativas modernas, trafegam milhões de eventos e logs diariamente – é humanamente inviável analisar tudo em busca de anomalias. Algoritmos de *machine learning* aplicados a sistemas de monitoramento, porém, conseguem aprender o padrão "normal" de operação de uma rede e identificar em tempo real desvios suspeitos, como tráfego incomum, tentativas de acesso atípicas ou padrões que indiquem malware (Ponemon Institute, 2024). Com IA, ferramentas de *IDS/IPS* (sistemas de detecção e prevenção de intrusões) tornaram-se mais eficazes, detectando até ameaças *zero-day* (desconhecidas) por similaridade de comportamento, onde métodos tradicionais baseados em assinatura falhariam. Segundo pesquisa do Ponemon Institute, 70% dos profissionais de segurança acreditam que a IA é altamente efetiva em detectar ataques antes não detectáveis por meios convencionais (Ponemon Institute, 2024). Além disso, a IA ajuda a reduzir o ruído em centros de operação de segurança: organizações recebem em média 22 mil alertas de segurança por semana, e mais da metade pode ser triada e tratada automaticamente por IA, sem intervenção humana (Ponemon Institute, 2024). Isso diminui drasticamente a sobrecarga das equipes e o tempo de resposta. Aliás, 66% dos profissionais consultados esperam que a implantação de tecnologias de segurança com IA aumente a produtividade do pessoal de TI (Ponemon Institute, 2024) – o que faz diferença num cenário de escassez de mão de obra em cibersegurança.

No caso da Motorola Solutions, a empresa enfatiza a oferta de serviços gerenciados de cibersegurança com IA para seus clientes de segurança pública e empresarial, justamente porque reconhece que a comunicação crítica e sistemas de vigilância conectados precisam estar protegidos contra ataques (Motorola Solutions, 2025a). Eles empregam IA em soluções como o *Shielded* (programa de proteção de rede) para prevenir acessos não autorizados ou interrupções em redes de missão crítica (Motorola Solutions, 2025a). Em seu site, destacam que seus sistemas de vídeo são projetados com *analytics* de IA responsáveis e incluem defesas contra ameaças cibernéticas emergentes (Motorola Solutions, 2023). Ao integrar IA nas camadas de

segurança, obtém-se um efeito de resposta em velocidade de máquina: por exemplo, se uma câmera IP conectada começar a se comportar de modo anômalo (possível sinal de comprometimento), o sistema pode automaticamente isolá-la da rede antes que um invasor use-a como ponto de entrada. Esse tipo de automação defensiva é crucial para neutralizar ataques em seus primórdios, evitando escalada. Outro impacto positivo da IA é melhorar a identificação de vulnerabilidades e priorização de correções. Em vez de depender apenas de scans manuais ou da experiência dos analistas, algoritmos podem correlacionar informações de diversas fontes (boletins de segurança, atividade na rede, configurações) e apontar quais vulnerabilidades no ambiente apresentam maior risco efetivo de exploração (Ponemon Institute, 2024). Essa priorização inteligente se traduz em melhor alocação de recursos: equipes focam nas brechas que realmente importam, economizando tempo. Além disso, IA pode ajudar a testar defesas via *red-teaming* automatizado – simulando ataques para identificar pontos fracos. Grandes empresas vêm usando aprendizado de máquina para gerar tráfego de teste sofisticado, identificando se seus sistemas de monitoramento detectariam ou não certos padrões maliciosos. Esse uso "do bem" da IA em segurança digital resulta em sistemas mais robustos e auditados.

No entanto, assim como nos outros domínios, há um lado desafiador: os agentes mal-intencionados também aproveitam a IA, criando um cenário de ameaças mais complexo. Um dos impactos negativos mais preocupantes é a otimização de ataques cibernéticos por IA. Atores de ameaça podem usar IA generativa para automatizar a produção de *phishing* altamente convincente, personalizado para cada alvo – e em larga escala (Malwarebytes, 2023). Antes, criar e enviar milhões de e-mails de phishing distintos exigiria muito esforço, agora um modelo de linguagem treinado pode gerar infinitas variações de mensagens persuasivas (em múltiplos idiomas, inclusive), dificultando a filtragem e aumentando as chances de sucesso dos ataques. Além disso, IAs podem encontrar vulnerabilidades em softwares de forma automatizada, vasculhando código-fonte em busca de padrões de falha ou testando combinações. Já se demonstrou que uma IA pode até escrever código malicioso funcional – pesquisadores induziram um modelo a criar um *malware* de roubo de dados praticamente indetectável por antivírus tradicionais (Malwarebytes, 2023). Assim, a barreira de entrada para hackers inexperientes cai, pois podem se valer de ferramentas inteligentes para criar ataques complexos que antes só especialistas conseguiriam.

Esse contexto alimenta o aumento no volume e na sofisticação das ameaças digitais – um impacto direto da difusão da IA. Organizações reportam crescimento de ataques automatizados e mais elaborados. Por exemplo, campanhas de *spear phishing* (phishing direcionado) usando IA para coletar informações de rede social e criar mensagens customizadas a executivos tornaram-se mais comuns e difíceis de distinguir de comunicações reais. Também há relatos de criminosos utilizando deepfakes de voz (gerados por IA) para enganar funcionários a fazerem transferências bancárias, imitando a voz de um diretor ao telefone. Esse tipo de golpe evidencia que a segurança digital agora precisa englobar até a verificação de autenticidade de mídias, outro desafio trazido pela IA generativa (Malwarebytes, 2023). A Motorola Solutions, inclusive, tem um núcleo de inovação que pesquisa como identificar *deepfakes* em contexto de segurança pública, ciente de que falsificações de áudio/vídeo podem ser usadas tanto para cibercrime quanto para enganar sistemas de vigilância (Motorola Solutions Blog, 2023).

Outro impacto da IA no campo digital é a necessidade de novas habilidades e funções especializadas para operá-la de forma eficaz. As organizações precisam não apenas de analistas de segurança, mas de cientistas de dados aplicados à segurança. A Ponemon (2024) indica que cerca de metade das empresas já conta com profissionais dedicados à supervisão de ferramentas de IA na segurança. Isso envolve entender como o algoritmo toma decisões, ajustar limitações, investigar alertas produzidos pela IA (que às vezes podem ser falsos positivos sofisticados). Essa demanda por talento especializado é um desafio, pois há escassez tanto de profissionais de segurança quanto de IA, e a intersecção dos dois é ainda mais rara. Assim, um impacto

organizacional é a pressão por formação e contratação nessas áreas, algo que empresas como Motorola Solutions têm endereçado via parcerias com universidades e instalação de centros de desenvolvimento de software (Revista Digital Security, 2023). Para manter seu ecossistema seguro, a empresa anunciou a criação de um centro de design de software no Brasil focado em inovar com IA – isso não apenas para criar produtos, mas também para reforçar segurança e talento local (Revista Digital Security, 2023).

Ainda no contexto organizacional, a complexidade das ferramentas de IA pode introduzir um problema: a dependência e compreensão limitada dos processos decisórios da IA. Muitos algoritmos de detecção de ameaças são caixas-pretas (redes neurais profundas) que podem dar um alerta sem que o analista saiba exatamente qual padrão gerou aquilo. Isso dificulta a confiança e a explicação para gestores ("por que precisamos desligar esse servidor? Porque a IA apontou anomalia X – mas como ela chegou a X?"). A Motorola Solutions aborda essa questão em seu *Trust Center*, apontando que foca em IA interpretável e com feedback do usuário, de forma que mantenha a confiabilidade (Motorola Solutions, 2023). Ainda assim, no mercado em geral, a falta de interpretabilidade dos modelos de IA é um ponto de atenção: decisões automáticas sem clareza de critérios contrariam princípios de normas como a GDPR europeia, que dá direito à explicação ao titular dos dados. Portanto, o impacto aqui é uma tensão entre utilizar modelos mais poderosos versus modelos mais transparentes, que as organizações precisam equilibrar. Em termos de ciber-risco, um impacto a considerar é que a incorporação de IA em tudo também abre novas superfícies de ataque: atacantes podem tentar corromper a IA em si, num processo chamado *data poisoning* (envenenamento de dados) – inserindo dados maliciosos no treino ou operando nos sensores para enganar o algoritmo. Por exemplo, pesquisadores já mostraram ser possível enganar um sistema de visão de veículo autônomo colando adesivos específicos numa placa de trânsito para a IA "pensar" que é outra coisa. Trazendo ao contexto: um criminoso cibernético poderia tentar manipular os modelos de detecção de intrusão de uma empresa, para que ignorem justamente a atividade que ele planeja fazer, injetando falsos negativos. Isso nos alerta que as IAs de segurança também precisam ser defendidas, e esse é um impacto novo – sair de proteger apenas infraestrutura e passar a proteger também a integridade dos algoritmos e de seus dados de treinamento (Malwarebytes, 2023).

Resumindo, na esfera da segurança digital, a IA age como uma espada de dois gumes. Os impactos positivos incluem: detecção mais rápida e precisa de ameaças, automação de respostas, produtividade das equipes de segurança, priorização eficaz de riscos e aprendizagem contínua, tornando a defesa cibernética mais proativa. Os impactos negativos envolvem: ataques potencializados por IA, novos vetores de ameaça (deepfakes, malware AI-driven), dificuldade de interpretação das decisões da IA e necessidade de expertise para operá-la, além de riscos de ataque aos próprios sistemas de IA. A Motorola Solutions e outras organizações em posição semelhante tratam isso investindo em IA defensiva e uma abordagem de segurança em múltiplas camadas, combinando soluções tradicionais e inteligentes (Motorola Solutions, 2025a).

Um dado encorajador é que a maioria das empresas já percebe valor na IA para segurança: 66% utilizam IA para detectar ataques em ambientes híbridos (cloud e local) e 70% relatam que a IA ajudou a identificar ameaças que passariam despercebidas (Ponemon Institute, 2024). Isso indica que, apesar dos novos riscos, a balança tende a ser favorável a quem emprega IA na defesa – desde que se tomem as precauções necessárias. Em suma, ignorar a IA na segurança digital não é opção, pois equivaleria a lutar contra atacantes equipados de IA com métodos obsoletos. Ao mesmo tempo, aderir à IA exige preparo: políticas de atualização de modelos, governança de dados rigorosa, treinamento da equipe e um forte componente ético (por exemplo, evitar coletar dados excessivos ou discriminatórios mesmo na defesa). Empresas como a Motorola Solutions, que tanto desenvolvem quanto usam IA em segurança, podem servir de modelo ao adotar posturas transparentes (como detalhar seu compromisso com IA imparcial e robusta no próprio site (Motorola Solutions, 2023) e colaborar com a comunidade para melhorar padrões de segurança

de IA. Assim, maximiza-se o impacto positivo: redes mais seguras, menos incidentes graves, continuidade de serviços – o que, no fim, protege não apenas a organização mas seus clientes, parceiros e a sociedade que depende do funcionamento confiável da infraestrutura digital.

A Motorola pode estruturar planos de resiliência digital que olhem diretamente para os riscos e as oportunidades do uso de IA em cibersegurança. Não basta instalar novas ferramentas: é preciso políticas de atualização contínua de modelos, auditorias periódicas para detectar vieses e fragilidades algorítmicas, testes de estresse e protocolos claros de resposta a incidentes — inclusive para ataques mediados por IA. Com essa postura preventiva e sistemática, a empresa fortalece suas defesas e, ao mesmo tempo, ganha credibilidade com clientes e parceiros ao mostrar equilíbrio entre inovação e responsabilidade na proteção de dados e de infraestruturas críticas.

Também é recomendável criar uma estrutura de governança específica para IA aplicada à segurança, com mecanismos de auditoria independentes e relatórios de conformidade acessíveis. Esses instrumentos permitem avaliar de forma contínua a eficácia dos modelos e explicitar como decisões automatizadas são tomadas. O resultado é mais confiança interna e externa — e menos risco de uma dependência acrítica de sistemas que, embora potentes, podem falhar ou ser manipulados.

Esse arranjo precisa vir acompanhado de investimento em formação de profissionais "híbridos", com base em segurança cibernética e ciência de dados. A demanda por especialistas capazes de supervisionar, ajustar e explicar modelos de IA já existe — e a falta desses perfis compromete a eficácia das soluções. Com equipes mais preparadas, a Motorola aumenta a eficiência de suas defesas e assegura que a tecnologia seja usada de modo ético, interpretável e alinhado aos objetivos institucionais.

Por fim, a adoção de IA em segurança deve caminhar junto com estratégias de cooperação com órgãos reguladores e centros de pesquisa. Compartilhar informações sobre novas ameaças, vulnerabilidades e padrões de ataque mediados por IA reduz a assimetria entre atacantes e defensores. Ao participar de redes colaborativas de defesa, a Motorola deixa de atuar isoladamente e passa a integrar um modelo mais resiliente de cibersegurança coletiva, capaz de responder com mais rapidez e eficiência às ameaças emergentes.

4.4 Desafios éticos e de governança no uso organizacional de IA

Transversalmente aos impactos discutidos nos subitens anteriores, emergem uma série de desafios éticos e de governança que as organizações precisam enfrentar ao adotar IA na comunicação, na vigilância e na segurança digital. São questões que, se não forem adequadamente tratadas, podem comprometer os benefícios da IA e gerar consequências sociais negativas. Dentre os desafios principais, destacam-se: garantir transparência e explicabilidade, evitar vieses e discriminações, proteger a privacidade e os dados sensíveis, assegurar responsabilidade e supervisão humana, e promover a aceitação e confiança junto aos stakeholders.

A transparência no uso da IA é vital para manter a confiança dos públicos interno e externo. Isso significa ser claro sobre onde e como a IA está sendo empregada, quais decisões ela influencia e com que objetivos. Uma comunicação organizacional ética sobre IA envolve não exagerar os méritos ("IA milagrosa") nem esconder os riscos. Por exemplo, se uma empresa usa IA para moderar comentários de clientes nas redes sociais, convém divulgar essa prática e, idealmente, explicar os critérios gerais que a IA utiliza. A Motorola Solutions, como já citado, deu um passo inédito ao criar rótulos informativos sobre a IA embutida em seus produtos de segurança (Medeiros, 2025). Ao listar o tipo de modelo, se é generativo ou não, o acesso que tem os dados e o grau de controle humano, a empresa fornece informações claras que qualquer interessado pode verificar. Essa medida atende a uma demanda ética crucial de explicabilidade: usuários têm o direito de saber que estão lidando com uma decisão algorítmica e quais são suas bases (Sriram, 2025). Esse tipo de iniciativa tende a ser cada vez mais requisitado – inclusive

regulado – ao redor do mundo. Na União Europeia, o *AI Act* em discussão exigirá transparência sobre sistemas de IA de alto risco. No Brasil, o Projeto de Lei de IA também discute obrigação de aviso quando conteúdo é automatizado. Portanto, as organizações devem se antecipar e incorporar transparência como parte de sua governança de IA, seja por meio de políticas internas, seja por práticas comunicacionais públicas.

Relacionado à transparência está o desafio da explicabilidade técnica – algumas decisões da IA precisam ser compreensíveis para auditoria e justificativa. Nem todos os modelos permitem isso facilmente (como uma rede neural profunda), mas há métodos (tais como LIME, SHAP e outros algoritmos de explicação) que podem ser empregados para extrair razões aproximadas. A governança de IA nas empresas modernas passa por incluir, nos requisitos de desenvolvimento ou compra de sistemas de IA, critérios de interpretabilidade. A Motorola Solutions, em sua diretriz de IA, afirma ter uma filosofia de design "human-centered" que enfatiza manter o usuário informado das decisões da IA e sob controle, garantindo que as soluções sejam "transparentes, compreensíveis e confiáveis" (Motorola Solutions, 2023). Essa postura reconhece que sem explicabilidade e controle, o usuário não confiará e não adotará plenamente a IA – ou poderá adotá-la de forma imprópria. Assim, do ponto de vista ético, transparência e explicação não são apenas questões morais, mas também funcionais para o sucesso da IA no ambiente organizacional (Gonçalves, 2024).

O viés algorítmico é outro desafio crítico. Conforme analisado, se a IA é treinada em dados históricos contendo desigualdades ou preconceitos, ela tende a reproduzí-los. Isso pode afetar a comunicação organizacional (por exemplo, um sistema de triagem de currículos que descarte sistematicamente minorias, gerando um problema de diversidade e reputação), a vigilância (reconhecimento facial menos preciso para certos grupos étnicos) e até a segurança digital (modelos que considerem certos países ou origens de IP inerentemente suspeitos, podendo bloquear usuários legítimos de regiões sub-representadas). A prevenção de viés requer cuidados desde a concepção: curadoria de dados, inclusão de diversidade nos conjuntos de treinamento, testes exaustivos de desempenho do modelo em diferentes subgrupos, e ajustes deliberados para corrigir disparidades (Buolamwini & Gebru, 2018). Requer também equipes diversas por trás do desenvolvimento e implementação da IA, pois pessoas de diferentes bagagens tendem a perceber vieses que outras não notam (Bourne, 2019). Do lado da governança, empresas líderes têm criado comitês de ética em IA – grupos multidisciplinares que avaliam os projetos de IA, suas implicações e aderência a princípios éticos. A Motorola Solutions formou um *Technology Advisory Committee* envolvendo várias áreas para garantir alinhamento da inovação com valores da empresa (Motorola Solutions, 2023). Tais comitês podem recomendar ajustes ou até veto a certas funcionalidades julgadas problemáticas eticamente. Por exemplo, poderiam determinar restrições ao uso do reconhecimento facial, como não usar para identificação de menores ou em locais específicos, enquanto as questões de viés não forem satisfatoriamente resolvidas. O desafio é tornar esses conselhos atuantes de fato, e não órgãos simbólicos.

A privacidade e a proteção de dados pessoais constituem outro pilar ético. Com IA vasculhando comunicações e vídeos, há grande coleta de dados pessoais (imagens de rostos, voz, textos que podem conter informações privadas). As organizações precisam seguir leis de privacidade (LGPD no Brasil, GDPR na UE etc.), o que implica adequação no tratamento desses dados: só coletar o necessário, base legal para processamento, garantir segurança e dispor de políticas de retenção e descarte. Além disso, eticamente, mesmo que algo não seja ilegal, convém perguntar: "é necessário e proporcional monitorar X com IA?". Por exemplo, monitorar e-mails internos com IA para medir engajamento pode ter base legal de interesse legítimo da empresa, mas será que é proporcional? Não haveria maneira menos intrusiva de aferir engajamento? O princípio da minimização e o respeito à autonomia individual devem guiar as decisões. Uma boa prática surgindo é realizar Relatórios de Impacto de Proteção de Dados

(DPIA) específicos para sistemas de IA, avaliando riscos à privacidade e formas de mitigá-los antes da implementação.

A Motorola Solutions sabe que lida com dados sensíveis de segurança pública e declara aderência a padrões rígidos de proteção (criptografia, controles de acesso) e conformidade com normas como CJIS (nos EUA) para uso de dados de justiça, por exemplo (Motorola Solutions, 2025b). Internamente, toda e qualquer iniciativa de IA possivelmente passa por aval jurídico e de segurança para garantir conformidade. Isso é parte da governança: envolver as áreas de compliance, jurídica e segurança da informação no ciclo de vida dos projetos de IA. Como resultado, a empresa pode assegurar aos clientes que suas tecnologias seguem "privacy by design" e "security by design", o que é tanto um imperativo ético quanto um diferencial competitivo num mercado cada vez mais preocupado com privacidade. A responsabilização (accountability) e a manutenção do controle humano surgem como outro desafio-chave. Sistemas de IA podem tomar decisões em milissegundos que afetam pessoas – quem é responsável se uma decisão automatizada causar um dano? As organizações devem delinear claramente quando o humano deve intervir ou validar. Uma prática recomendada é a do *Human-in-the-loop*, já citada, especialmente para decisões de alto impacto (Motorola Solutions, 2023). Isso preserva uma camada de julgamento humano e facilita atribuição de responsabilidade. Por exemplo, se um algoritmo recomendar a demissão de um empregado por suposta baixa produtividade (com base em métricas monitoradas), a decisão final deve ser de um gestor humano que avalie o contexto; assim, a responsabilidade permanece com o gestor e não se delega cegamente à máquina. Em vigilância, se a IA alerta "pessoa suspeita", um operador humano deve confirmar antes de uma abordagem policial ser deflagrada. Ao mesmo tempo, deve-se treinar os humanos para não se tornarem complacentes confiando demais na IA (risco do fenômeno de "automation bias"). Governança implica criar procedimentos onde os usuários de IA são instruídos a sempre conferir informações críticas e ter ceticismo saudável. A cultura corporativa deve ser moldada para ver a IA como assistente, não árbitro supremo (Motorola Solutions, 2023). Por exemplo, no uso do Assist Chat, a Motorola enfatiza que ele traz dados e sugestões mas cabe aos profissionais decidir ações (Motorola Solutions, 2025b). Essa mentalidade precisa permear todas as aplicações.

Um último desafio é social e comunicacional: conquistar e manter a confiança dos diversos stakeholders (funcionários, clientes, público, reguladores) no uso da IA. Isso se atinge atendendo aos pontos anteriores (transparência, equidade, privacidade etc.), mas também com diálogo e educação. As organizações devem estar abertas a ouvir preocupações – por exemplo, se funcionários temem que o chatbot interno esteja "espionando" conversas, a empresa deve abordar isso diretamente, explicando limites e objetivos, e acolhendo sugestões ou queixas (Screencorp, 2024). Com a sociedade, é importante participar de debates públicos, colaborar em formulação de boas práticas e se antecipar a escândalos. Porque um erro ético na adoção de IA pode virar crise de imagem rapidamente (Gonçalves, 2024). A Volkswagen, no caso do comercial com IA da Elis Regina, enfrentou forte reação contrária e desgaste reputacional (BBC News Brasil, 2023). Isso mostra que inovar com IA na comunicação requer sensibilidade ética e respeito à memória/identidade – não se pode, por exemplo, simplesmente "ressuscitar" alguém via IA para fins mercadológicos sem prever reações emocionais e dilemas de consentimento póstumo (Arbix, 2023 apud BBC News). Assim, incluir perspectivas éticas e até filosóficas no processo decisório de campanhas e projetos é fundamental.

Resumindo, os desafios éticos e de governança são transversais e determinantes para que os impactos positivos da IA superem os negativos. Governar o uso da IA significa criar políticas, comitês e processos que assegurem conformidade legal e aderência a princípios morais, e também cultivar uma cultura onde a IA seja utilizada de forma responsável, transparente e centrada no ser humano. Empresas como a Motorola Solutions que investem em iniciativas de transparência (rótulos de IA) e articulam publicamente um compromisso com "IA responsável" se colocam na frente para enfrentar esses desafios. Em contraste, organizações que negligenciarem essas

questões arriscam-se a consequências sérias: desde ações judiciais, sanções (vide LGPD prevendo multas) até perda de confiança e danos irreparáveis à reputação (Gonçalves, 2024). No cenário atual – em que o público e as autoridades estão cada vez mais atentos ao uso da IA – a ética aplicada não é opcional, mas sim condição para a sustentabilidade da inovação tecnológica dentro das organizações.

Falar de inteligência artificial (IA) na Motorola não é apenas discutir desempenho. É decidir que tipo de tecnologia a empresa deseja colocar no mundo. Um caminho viável é instituir programas permanentes de ética digital aplicados à IA. Na prática, isso significa ter um calendário regular de oficinas e microtreinamentos, além de canais de escuta ativa que realmente funcionem — uma caixa de entrada supervisionada, reuniões abertas trimestrais e um painel de acompanhamento dos temas levantados por colaboradores, clientes e organizações da sociedade civil. Com isso, inovação deixa de ser sinônimo de "fazer mais rápido" e passa a ser "fazer certo e com propósito".

A participação das partes interessadas precisa ir além do convite formal. Um desenho possível é criar um comitê misto (engenharia, jurídico, RH, atendimento, marketing e representantes externos) para co-construir diretrizes éticas. Quando quem desenvolve, quem usa e quem fiscaliza sentam à mesma mesa, a empresa reduz resistências, antecipa riscos e fortalece legitimidade. Em outras palavras: governança de IA não vira um checklist regulatório, mas um compromisso estratégico e público com responsabilidade.

Esse compromisso ganha corpo com códigos internos específicos para IA. Em vez de textos genéricos, o ideal é um documento curto, claro e acionável, que traga: (i) princípios de transparência e explicabilidade compatíveis com o produto; (ii) salvaguardas de privacidade desde a coleta até o descarte de dados; (iii) responsabilidades explícitas por decisões automatizadas; e (iv) procedimentos para revisão quando houver impacto significativo sobre pessoas. O código, acompanhado de exemplos reais e casos-limite, orienta do protótipo ao pós-lançamento e dá previsibilidade jurídica e reputacional.

Para além do "autocontrole", auditorias independentes e periódicas ajudam a separar intenção de prática. Especialistas externos podem testar modelos para vieses, avaliar processos de dados e conferir a execução das salvaguardas. Relatórios com sumários públicos — preservados os segredos industriais — aumentam a confiança de clientes, investidores e reguladores e, de quebra, geram vantagem competitiva: quem demonstra maturidade ética costuma acelerar aprovações e reduzir retrabalho.

Nada disso se sustenta se a ética ficar confinada a um comitê. O tema precisa entrar nos rituais da cultura: integração de novos colaboradores, trilhas de liderança, planos de carreira e avaliação de desempenho. Metas simples ajudam a tirar o assunto do abstrato, como tempo de resposta a preocupações éticas, número de ajustes realizados em modelos após feedback e índice de satisfação de usuários afetados. Quando os times percebem que "fazer o certo" é reconhecido e medido, a responsabilidade deixa de ser obrigação externa e passa a fazer parte da identidade da organização — o que aumenta a resiliência diante de crises ou dilemas tecnológicos.

Em síntese, combinar escuta ativa, código prático, auditoria externa e incorporação cultural desloca a conversa da eficiência a qualquer custo para a inovação responsável. É um movimento incremental, mas decisivo: protege pessoas, reduz riscos e alinha tecnologia aos valores que a própria Motorola afirma defender.

5 CONCLUSÕES E CONTRIBUIÇÃO TECNOLÓGICA/SOCIAL

Neste estudo sobre os impactos da Inteligência Artificial na comunicação organizacional, tendo a Motorola Solutions como fio condutor, foi visto que tecnologia e humanidade podem, sim, caminhar juntas. A IA acelera fluxos, qualifica decisões e libera tempo para o que é mais humano: escuta, criatividade, mediação. Mas foi possível entender também que eficiência sem

propósito não basta. O que sustenta a transformação é a forma como as organizações a governam — com clareza de responsabilidades, critérios de uso e prestação de contas.

Na prática, isso significa tratar a IA como parte de um sistema sociotécnico. Pessoas continuam no centro: a máquina sugere, o humano decide. Para isso funcionar, é preciso um trilho de governança que una política, processo e cultura. Foram relatados princípios claros (uso responsável, privacidade por padrão, mínimo de dados necessário), de comitês multidisciplinares que avaliam riscos antes do lançamento de funcionalidades, de procedimentos operacionais padrão que deixam explícito quando e como a IA pode apoiar (e quando não pode), e de rotinas de auditoria que verificam desempenho, vieses e segurança de ponta a ponta.

Governança também é transparência. Usuários e públicos devem saber quando há IA "por trás do balcão", que dados são processados e qual é o papel do humano na decisão final. Etiquetas de IA, manuais de uso em linguagem acessível e canais para contestação e correção de erros aproximam a tecnologia das pessoas e constroem confiança. Do lado interno, métricas de qualidade (acurácia, falso positivo/negativo), de equidade (desempenho por grupos), e de experiência (tempo de resposta, utilidade percebida) alimentam ciclos de melhoria contínua. Nada disso se sustenta sem segurança e compliance. A cadeia de dados precisa ser protegida do dispositivo à nuvem; contratos com fornecedores devem refletir padrões técnicos e éticos; e equipes precisam de treinamento recorrente — não só "qual botão apertar", mas como interpretar saídas, identificar limites e reportar problemas. Em paralelo, a liderança dá o tom: incentiva o uso responsável, recompensa prudência, e deixa claro que resultados não valem qualquer custo. É assim que a inovação deixa de ser um salto no escuro para virar um caminho trilhado com luz.

A experiência analisada mostra que, quando a IA é implantada com governança forte e foco no humano, os ganhos aparecem onde mais importam: mensagens mais claras, decisões mais ágeis, respostas mais coordenadas em momentos críticos. E surgem outros dividendos, menos mensuráveis, porém decisivos: confiança entre áreas, orgulho de pertencimento, reputação junto à sociedade. É esse o convite desta conclusão: que cada organização trate a IA não como um fim em si, mas como uma parceira. Com ética como norte, processos como caminhos e pessoas no comando, a comunicação organizacional pode ser mais eficiente sem perder seu propósito — e a tecnologia, finalmente, fazer o que prometeu: ampliar o melhor do que já existe.

REFERÊNCIAS BIBLIOGRÁFICAS

.

ABERJE – Associação Brasileira de Comunicação Empresarial. Tendências da Comunicação Organizacional – 5ª edição (2024). **Revista Lide**, 25 set. 2024. Disponível em: https://www.revistalide.com.br/noticias/tecnologia-inovacao/pesquisa-aponta-que-54-das-empresas-devem-utilizar-inteligencia-artificial-na-comunicacao-este-ano. Acesso em: 28 jul. 2025.

BARBOSA, Lucia Martins; PORTES, Luiza Alves Ferreira. A Inteligência Artificial**. Revista Tecnologia Educacional**, Rio de Janeiro, n. 236, p. 16–27, 2023. Disponível em: http://abt-br.org.br/wp-content/uploads/2023/03/RTE_236.pdf. Acesso em: 19 mar. 2024.

BBC News Brasil (2023) – BRAUN, Julia. Os dilemas de usar inteligência artificial para trazer pessoas mortas de volta à vida**. BBC News Brasil**, 05 jul. 2023. Disponível em:https://www.bbc.com/portuguese/articles/cx9p9x01y84o . Acesso em: 06 jul. 2023.

BORGONOVO, Elton. Como a IA transforma a segurança preditiva na América Latina. **TI Inside,** 9 out. 2024. Disponível em: https://tiinside.com.br/09/10/2024/como-a-ia-transforma-a-seguranca-preditiva-na-america-latina/. Acesso em: 28 jul. 2025.

BOURNE, Clea. AI cheerleaders: public relations, neoliberalism, and artificial intelligence. **Public Relations Inquiry,** v. 8, n. 2, p. 109–125, 2019. DOI: 10.1177/2046147X19835250.

BUOLAMWINI, Joy; GEBRU, Timnit. Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification. In: Proceedings of Machine Learning Research, v. 81, p. 1–15, 2018. Disponível em: http://proceedings.mlr.press/v81/buolamwini18a.html. Acesso em: 28 jul. 2025.

COULDRY, Nick; YU, Jun. Deconstructing datafication's brave new world. **New Media & Society**, v. 20, n. 12, p. 4473–4491, 2018.

DELOITTE. Vigilância e policiamento preditivo através da IA. **Urban Future with a Purpose – Deloitte Insights**, 2021. Disponível em: https://www.deloitte.com/africa-lusofona/pt/industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html. Acesso em: 28 jul. 2025.

FRANÇA, Glaucia Ellen de Sousa; OLIVEIRA, Maria Lívia Pachêco. O impacto da inteligência artificial na comunicação organizacional. In: 24º Congresso de Ciências da Comunicação na Região Nordeste (Intercom Nordeste), Natal/RN, 08-10 maio 2024. Trabalho de graduação, UFPB. Disponível em: https://sistemas.intercom.org.br/pdf/submissao/regional/12/1587/032820242224406606185 8462b2.pdf. Acesso em: 29 jul. 2025.

GONÇALVES, Marianna Abdo. Inteligência artificial e ameaça reputacional. **Organicom**, São Paulo, v. 21, n. 44, p. 180–185, 2024. DOI: 10.11606/issn.2238-2593.organicom.2024.220397.

GIRARDI, Luana da S.; PASE, André F. Em busca do comando ideal: um duplo olhar sobre a inteligência artificial generativa na comunicação organizacional. **Organicom**, v. 21, n. 44, p. 71–84, 2024. DOI: 10.11606/issn.2238-2593.organicom.2024.220414. Disponível em: https://revistas.usp.br/organicom/article/view/220414. Acesso em: 28 jul. 2025.

IBM. Global AI Adoption Index 2022. Armonk, NY: IBM, 2022. Disponível em: https://newsroom.ibm.com/2022-05-19-Global-Data-from-IBM-Shows-Steady-AI-Adoption-as-Organizations-Look-to-Address-Skills-Shortages,-Automate-Processes-and-Encourage-Sustainable-Operations. Acesso em: 30 jul. 2025.

KARHAWI, Issaaf; GUIMARÃES NETO, Humberto; MARTINS, Lafaiete; OLIVEIRA, Silvio C. de. Discursos circulantes sobre inteligência artificial: articulações discursivas em veículos de comunicação organizacional. **Organicom**, São Paulo, Brasil, v. 21, n. 44, p. 121–132, 2024.

KUNSCH, Margarida M. Krohling de. A comunicação estratégica nas organizações contemporâneas. **Media & Jornalismo**, Lisboa, v. 18, n. 33, p. 13–24, 2018.

LUM, Kristian; ISAAC, William. To predict and serve? **Significance**, v. 13, n. 5, p. 14–19, 2016.

MAGNOLO, Talita Souza; WHITAKER, André Machado Coelho. As relações de poder com a IA: perspectivas corporativistas no campo da Comunicação. **Organicom**, São Paulo, Brasil, v. 21, n. 44, p. 55–70, 2024.

MALWAREBYTES. Malwarebytes ChatGPT Survey Reveals 81% Are Concerned by Generative AI Security Risks. Santa Clara (CA), 27 jul. 2023. Disponível em:https://www.malwarebytes.com/press/2023/06/27/malwarebytes-chatgpt-survey-reveals-81-are-concerned-by-generative-ai-security-risks. Acesso em: 19 mar. 2024.

MARR, Bernard. Starbucks: Using Big Data, Analytics And Artificial Intelligence To Boost Performance. Forbes, 28 mai. 2018. Disponível em: https://www.forbes.com/sites/bernardmarr/2018/05/28/starbucks-using-big-data-analytics-and-artificial-intelligence-to-boost-performance/. Acesso em: 30 jul. 2025.

MEDEIROS, Henrique. Motorola Solutions cria 'rótulos nutricionais' de IA de seus equipamentos. **Mobile Time**, 28 jul. 2025. Disponível em: https://www.mobiletime.com.br/noticias/28/07/2025/motorola-solutions-ia/. Acesso em: 28 jul. 2025.

MOTOROLA SOLUTIONS. Inteligência Artificial aprimora as soluções de ponta a ponta da Motorola Solutions para defesa e segurança pública. Press release, 02 abr. 2019. Disponível em: https://www.motorolasolutions.com/newsroom/press-releases/artificial-intelligence-enhances-motorola-solutions-end-to-end-solutions-fo/inteligncia-artificial-aprimora-as-solues-de-ponta-ponta-da-motorola-soluti.html. Acesso em: 28 jul. 2025.

MOTOROLA SOLUTIONS. Motorola Solutions Unveils Advanced AI-Powered Safety Ecosystem at LAAD 2025. Press release, 01 abr. 2025a. Disponível em: https://www.motorolasolutions.com/newsroom/press-releases/advanced-ai-powered-safety-ecosystem-unveiled-at-laad-2025.html (versão em português). Acesso em: 28 jul. 2025.

MOTOROLA SOLUTIONS. Motorola Solutions Offers Assist Chat to all U.S. Public Safety Agencies Cost-Free and Expands AI Across Portfolio. Press release, 13 maio 2025b. Disponível em: https://www.motorolasolutions.com/newsroom/press-releases/assist-chat-to-us-public-safety-agencies-cost-free-expands-ai.html. Acesso em: 28 jul. 2025.

MOTOROLA SOLUTIONS. Mission-Critical Artificial Intelligence – Collaborative Intelligence: Humans + AI. Site institucional, 2023. Disponível em: https://www.motorolasolutions.com/en_us/solutions/ai.html. Acesso em: 28 jul. 2025.

OPENAI. March 20 ChatGPT Outage. OpenAI Blog, 24 mar. 2023. Disponível em: https://openai.com/blog/march-20-chatgpt-outage. Acesso em: 21 mar. 2024.

O'NEIL, Cathy. Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy. Nova York: **Crown,** 2016.

PONEMON INSTITUTE. The 2024 Study on the State of AI in Cybersecurity: Ponemon Institute Research Report. Feb. 2024. (Sponsored by MixMode). Disponível em: https://ponemonsullivanreport.com/2024/04/05/the-2024-study-on-the-state-of-ai-in-cybersecurity/. Acesso em: 28 jul. 2025.

RÊGO, Ana Regina. A ética nos usos de "inteligência" artificial: interações, mercado e sociedade. **Organicom,** São Paulo, Brasil, v. 21, n. 44, p. 109–120, 2024.

SATO, Mia; ROTH, Emma. CNET found errors in more than half of its AI-written stories. **The Verge,** 25 jan. 2023. Disponível em: https://www.theverge.com/2023/1/25/23571082/cnet-ai-written-stories-errors-corrections-red-ventures. Acesso em: 28 jul. 2025.

SAAD, Elizabeth Nicolau S. Comunicação organizacional contemporânea: o paradigma da digitalização. **Revista de Comunicação da FAPCOM**, São Paulo, v. 6, n. 12, p. 17–27, 2023.

SCREENCORP. Inteligência Artificial (IA) na Comunicação Interna. **Blog Screencorp**, 20 dez. 2024. Disponível em: https://blog.screencorp.com.br/ia-comunicacao-interna/. Acesso em: 28 jul. 2025.

SEBASTIÃO, Sónia Pedro. Inteligência Artificial em Relações Públicas? Não, obrigado. Percepções dos profissionais de comunicação e RP europeus. Lisboa: **Instituto Superior de Ciências Sociais e Políticas** – U. Lisboa, 2020.

SRIRAM, Akash. Motorola Solutions unveils new features to boost transparency in public safety tech. **Reuters**, 24 jul. 2025. Disponível em: https://www.reuters.com/technology/motorola-solutions-unveils-new-features-boost-transparency-public-safety-tech-2025-07-24/. Acesso em: 28 jul. 2025.

TEDESCO, Raphael. A "Corrida do Ouro" do século XXI – O que dizem as Diretrizes globais para o desenvolvimento da Inteligência Artificial. **Revista Digital Security**, 19 dez. 2023. Disponível em:https://revistadigitalsecurity.com.br/a-corrida-do-ouro-do-seculo-xxi-o-que-dizem-as-diretrizes-globais-para-o-desenvolvimento-da-inteligencia-artificial/. Acesso em: 19 mar. 2024.

ZERFASS, Ansgar; et al. European Communication Monitor 2019: Exploring Trust in the Profession, Transparency, Artificial Intelligence and New Content Strategies. Results of a Survey in 46 Countries. Bruxelas: EACD/EUPRERA, 2019. Disponível em: https://www.communicationmonitor.eu/wp-content/uploads/dlm_uploads/ECM19-European-Communication-Monitor-2019.pdf. Acesso em: 30 jul. 2025.

ZUBOFF, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. Nova York: **PublicAffairs**, 2019.