

FOTOS: ISTOCK



IA NAS CONCESSIONÁRIAS: SEGURANÇA EM PRIMEIRO LUGAR

Por: **WILSON LAURIA**

A Inteligência Artificial (IA) está transformando rapidamente o ambiente corporativo. No varejo automotivo, as concessionárias já utilizam ferramentas de IA para atendimento ao cliente, marketing, análise de dados, produtividade administrativa e automação de processos. Entretanto, a adoção acelerada dessas tecnologias também amplia riscos relevantes de segurança cibernética, privacidade e proteção de dados.

O principal problema é que a velocidade de adoção da IA tem superado a implementação de controles de segurança e mecanismos de governança. Segundo o relatório Cost of a Data Breach Report 2025, da IBM, 63% das organizações ainda não possuem políticas formais de governança para IA, enquanto o uso não autorizado de ferramentas de inteligência artificial — conhecido como Shadow AI — cresce rapidamente.

Ao mesmo tempo, o Verizon Data Breach Investigations Report 2026 (DBIR) mostra que criminosos cibernéticos já utilizam IA para potencializar ataques de phishing, engenharia social e para desenvolvimento de malware.

Esse cenário exige atenção especial das concessionárias, que operam ambientes altamente conectados e com um número exponencial de partes relacionadas.

O NOVO CENÁRIO DE RISCO

O DBIR 2026 aponta que a exploração de vulnerabilidades se tornou o principal vetor de acesso inicial em incidentes cibernéticos, representando 31% dos casos analisados. Além disso, o Ransomware continua crescendo e já responde por 48% dos vazamentos investigados.

Outro dado relevante é o aumento de 60% nos incidentes relacionados a terceiros. Isso é particularmente importante para o setor automotivo, cuja operação depende fortemente de fornecedores digitais e plataformas externas.

- O relatório da IBM também revela que:
- 20% das organizações sofreram incidentes relacionados ao uso de Shadow AI; e
 - 97% dos incidentes envolvendo IA ocorreram em ambientes sem controles adequados de acesso.
 - Na prática, isso significa que muitas empresas estão adotando IA sem supervisão adequada, ampliando a superfície de ataque e aumentando o risco de vazamento de dados, fraudes e interrupções operacionais.

GOVERNANÇA, GESTÃO DE RISCOS E COMPLIANCE

Sob a ótica da Governança, a Inteligência Artificial deve ser tratada como um tema estratégico e não apenas tecnológico. A liderança precisa compreender que o uso inadequado dessas ferramentas pode gerar:

- exposição de dados de clientes e parceiros;
 - impactos reputacionais;
 - prejuízos financeiros; e
 - comprometimento produção.
- A Gestão de Riscos deve incorporar a IA aos processos corporativos de segurança cibernética. Antes da adoção de qualquer ferramenta, algumas perguntas são fundamentais:
- Os dados enviados são armazenados?
 - Existe compartilhamento com terceiros?
 - O fornecedor possui controles adequados?
 - Há risco de exposição de informações estratégicas?
- Segundo a IBM, incidentes relacionados ao Shadow AI adicionaram, em média, USD 670 mil ao custo de um vazamento de dados.
- Na dimensão de Compliance, o uso inadequado de IA

pode violar políticas internas, contratos de confidencialidade e requisitos regulatórios. Um simples comando inserido por um colaborador em uma plataforma pública pode expor dados pessoais, contratos ou informações estratégicas da concessionária.

CONCLUSÃO

A Inteligência Artificial possui enorme potencial para aumentar eficiência e competitividade das concessionárias. Contudo, sua utilização sem governança, supervisão e controles de segurança pode ampliar significativamente os riscos cibernéticos da organização.

O desafio não é impedir o uso da IA, mas garantir que ela seja utilizada de forma segura, responsável e alinhada às práticas de Governança, Gestão de Riscos e Compliance. ■

Wilson Lauria é CEO da GRCIBER Soluções. Especialista em Cyber Security and Executive Strategy pela Stanford University (EUA). Professor Convidado na Escola Superior de Defesa e na Fundação Getúlio Vargas. Membro da Comissão de Gestão de Riscos Corporativos do IBGC.

As colunas mantidas pela ABRADIT NEWS têm por objetivo trazer diferentes pontos de vista e informações aos executivos da Rede. As opiniões são de responsabilidade dos articulistas, não refletindo necessariamente o posicionamento da Associação ou da Rede Toyota do Brasil.

SOMOS A ECKOS ESPECIALIZADA EM SOLUÇÕES EMPRESARIAIS

NOSSOS PRINCIPAIS SERVIÇOS:

- GESTÃO PARA LOGÍSTICA REVERSA DE RESÍDUOS
- AUDITORIAS
- DESENVOLVIMENTO DE SISTEMAS
- GESTÃO DE FORNECEDORES
- GESTÃO DE TRATAMENTO DE NÃO CONFORMIDADES
- CONSULTORIA E ASSESSORIA NA IMPLANTAÇÃO E MANUTENÇÃO DAS NORMAS ISO
- REQUISITOS LEGAIS
- TREINAMENTOS
- GESTÃO DE SEGURANÇA DO TRABALHO



FALE COM A GENTE:
(42) 99117-6756
(11) 91837-4179

ECKOSSISTEMAS.COM.BR

FOTOS: ISTOCK



LEGÍTIMO INTERESSE NA LGPD: CONCEITOS, APLICAÇÃO E LIMITES

POR: NATÚRIA PELLIN ARSEGO

No cenário da proteção de dados pessoais, regido pela Lei Geral de Proteção de Dados (LGPD), o consentimento e a execução contratual não são as únicas justificativas para o tratamento de informações. A LGPD prevê diversas bases legais, sendo o legítimo interesse uma das mais estratégicas para o ambiente corporativo.

Considere a situação em que uma concessionária, após uma revisão veicular, contata o cliente para avaliar a experiência, informar a data do próximo retorno e oferecer manutenção preventiva. Essa interação envolve o uso de dados pessoais, mas muitos gestores ainda não sabem justificar em qual base legal essa comunicação se ampara.

Frequentemente, a resposta reside no legítimo interesse, embora sua aplicação exija certa cautela.

Essa base legal é essencial para empresas que gerenciam dados de leads, clientes e parceiros. Atividades de pós-venda, avisos de garantia, recall, prevenção a fraudes e melhoria da experiência do usuário podem ser fundamentadas no legítimo interesse, desde que o contexto esteja adequado.

Contudo, o legítimo interesse não é uma autorização genérica para o tratamento de dados sem consentimento. Flexibilidade não significa liberdade irrestrita.

Antes de invocar o legítimo interesse como ampla justificativa, a empresa deve percorrer um caminho de três etapas conhecido internacionalmente como Legitimate Interest Assessment (LIA):

- 1. Finalidade:** O objetivo deve ser legítimo e razoável. Pesquisas de satisfação são aceitáveis, mas a venda de produtos sem qualquer relação com o serviço prestado e sem aviso prévio pode não ser.
- 2. Necessidade:** O tratamento deve ser indispensável. Se um simples contato com o cliente atinge o objetivo, não há justificativa para o cruzamento excessivo de dados para traçar um perfil comportamental dos clientes.
- 3. Balanceamento:** Deve haver equilíbrio entre o interesse da empresa e os direitos do titular, considerando a expectativa razoável do cliente, o impacto em sua privacidade e a existência de uma relação prévia entre as partes.

No setor automotivo, onde dados de clientes cir-

culam entre contextos de financiamentos, seguros e pós-venda, esse teste é especialmente relevante e a finalidade de cada uso desses dados deve ser avaliada individualmente.

O erro mais grave é usar o legítimo interesse como “carta coringa” para evitar a coleta de consentimento e justificar genericamente qualquer situação de tratamento de dados pessoais. O Art. 10 da LGPD, que disciplina especificamente o legítimo interesse, é expresso ao exigir análise prévia e documentação rigorosa. Nos termos do Art. 10, §3º, a ANPD pode determinar a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para tratamentos fundamentados nessa base legal — instrumento que obriga a empresa a mapear os riscos da atividade e a demonstrar que os

direitos dos titulares foram devidamente ponderados.

A falta de registro dessa análise expõe a empresa a sanções administrativas e à perda de confiança do consumidor ao perceber usos inesperados, e por vezes indevidos, de seus dados.

A conformidade tornou-se um diferencial. Empresas que se preocupam com a proteção dos dados de seus clientes e aplicam o legítimo interesse com transparência e ética transformam obrigações legais em vantagem competitiva e criam uma significativa relação de confiança com seus clientes.

No mercado atual, a confiança é, justamente, o que converte um negócio pontual em um relacionamento duradouro. ■

Natúria Pellin Arsego, Advogada, Graduada pela Faculdade de Desenvolvimento do Rio Grande do Sul (FADERGS). Pós-graduada em Direito Digital e Proteção de Dados através do curso da Escola Brasileira de Direito (EBRADIT) promovido pela FADERGS.

As colunas mantidas pela ABRADIT NEWS têm por objetivo trazer diferentes pontos de vista e informações aos executivos da Rede. As opiniões são de responsabilidade dos articulistas, não refletindo necessariamente o posicionamento da Associação ou da Rede Toyota do Brasil.

EXCELÊNCIA EM GESTÃO PARA CONCESSIONÁRIAS

- Revisão de DEF
- Reforma Tributária
- Planejamento Estratégico
- Budget

11 94146-7558
contato@etopbrasil.com.br