Expansão dessas tecnologias em bancos, seguradoras e plataformas digitais reforça discussões sobre LGPD, segurança da informação e responsabilidade corporativa

Por Izabela Rücker Curi, advogada e sócia do escritório
Rücker Curi Advocacia e Consultoria Jurídica

O uso de biometria e reconhecimento facial vem se tornando uma das principais ferramentas de autenticação e segurança no ambiente corporativo brasileiro. Bancos, seguradoras, plataformas digitais e empresas de diferentes segmentos têm ampliado a adoção dessas tecnologias em processos de validação de identidade, prevenção a fraudes e controle de acesso.

O avanço da biometria acompanha a forte digitalização das relações financeiras e empresariais no país. Dados da Federação Brasileira de Bancos (Febraban) apontam que mais de 80% das transações bancárias no Brasil já são realizadas por canais digitais. Já o Instituto Brasileiro de Geografia e Estatística (IBGE) indica que 89,1% da população brasileira com 10 anos ou mais utiliza internet, reforçando a expansão das interações digitais e o aumento da demanda por mecanismos mais robustos de autenticação e segurança.

Ao mesmo tempo, o tema passou a ocupar espaço crescente nas discussões jurídicas relacionadas à proteção de dados pessoais e governança corporativa. Pela legislação brasileira, dados biométricos são classificados como dados pessoais sensíveis pela Lei Geral de Proteção de Dados Pessoais (LGPD), o que exige um nível mais elevado de proteção e cautela no tratamento dessas informações.

A expansão dessas tecnologias também tem atraído maior atenção regulatória. A Autoridade Nacional de Proteção de Dados (ANPD) vem ampliando debates sobre o uso de reconhecimento facial e dados biométricos, especialmente em situações que envolvem monitoramento, autenticação e identificação automatizada.

O tema ganhou ainda mais destaque diante do crescimento das fraudes digitais no país. Levantamentos da Serasa Experian apontam que o Brasil registrou no ano passado mais de 6,9 milhões de tentativas de fraude em um único semestre, com uma ocorrência a cada 2,3 segundos. O setor bancário aparece entre os principais alvos dos criminosos digitais, em um ambiente marcado pelo crescimento de golpes envolvendo cartões, transações via Pix e roubo de dados pessoais.

Esse avanço das fraudes reforça a busca das empresas por mecanismos mais eficientes de autenticação e prevenção de riscos, ampliando o uso de biometria e reconhecimento facial em operações financeiras e processos de validação de identidade. A utilização dessas tecnologias busca reduzir vulnerabilidades operacionais e fortalecer processos de identificação em operações cada vez mais digitais.

Ao mesmo tempo, a adoção desses sistemas exige estruturas sólidas de governança. A coleta e o armazenamento de dados biométricos demandam políticas claras de proteção da informação, definição adequada de acessos e monitoramento constante das práticas de segurança adotadas pelas empresas e seus fornecedores.

A utilização inadequada desses dados pode gerar impactos relevantes, tanto sob o ponto de vista regulatório quanto reputacional. Vazamentos, compartilhamentos indevidos ou tratamentos incompatíveis com a finalidade informada ampliam a exposição jurídica das organizações e reforçam a necessidade de controles preventivos.

Outro aspecto importante envolve a transparência. O uso de mecanismos automatizados de identificação exige que titulares tenham acesso adequado às informações relacionadas ao tratamento de seus dados, especialmente quando essas ferramentas influenciam processos de autenticação e validação.

A integração entre áreas jurídicas, compliance, tecnologia e segurança da informação passa a ser cada vez mais necessária nesse ambiente. A análise preventiva dos fluxos de tratamento de dados biométricos contribui para reduzir vulnerabilidades e fortalecer a conformidade regulatória.

O avanço da biometria e do reconhecimento facial demonstra como inovação e proteção de dados passaram a caminhar de forma inseparável no ambiente corporativo. Mais do que incorporar novas tecnologias, o desafio das empresas está em estruturar mecanismos capazes de garantir segurança jurídica, proteção da informação e confiança nas relações digitais.

(22.05.2026)