O Brasil atravessa um momento decisivo na agenda digital. A União Europeia apresentou a versão preliminar da decisão de adequação que reconhece a LGPD como compatível com a GDPR. Trata-se do processo mais abrangente já realizado pela Comissão Europeia, que projeta o país como referência internacional em privacidade e proteção de dados. Esse reconhecimento cria um ambiente de maior segurança jurídica para o fluxo transfronteiriço de informações, amplia a confiança mútua entre jurisdições e posiciona o Brasil de forma mais competitiva no cenário global.

Esse avanço, entretanto, convive com eventos preocupantes. Os recentes ataques cibernéticos envolvendo intermediários do PIX, no âmbito de Open Finance – como os casos da Sinqia e da C&M Software – revelaram falhas graves de governança e gestão de credenciais, resultando em perdas bilionárias. Ainda que parte dos recursos tenha sido bloqueada rapidamente, a dimensão dos incidentes evidencia como cadeias de fornecedores críticos podem se tornar pontos vulneráveis, capazes de comprometer a resiliência do sistema.

Do ponto de vista da LGPD, esses incidentes não se limitam a perdas financeiras, mas configuram potenciais violações de segurança da informação que geram obrigações legais específicas. É necessário que as instituições, em cenários de ataques cibernéticos, possuam planos de resposta a incidentes de segurança de dados robustos. Estes planos devem contemplar, de acordo com o Art. 48 da LGPD, a **comunicação obrigatória à Autoridade Nacional de Proteção de Dados (ANPD)** e aos **titulares de dados afetados** sobre o incidente, detalhando a natureza dos dados comprometidos, as medidas de segurança utilizadas, os riscos e as providências tomadas para mitigar os danos.

Além disso, a relevância da gestão de fornecedores exige a necessidade de cláusulas contratuais rigorosas com todos os fornecedores críticos e intermediários, especialmente no Open Finance e Open Insurance. Esses contratos, fundamentados nos Arts. 39, 42 e 43 da LGPD, devem definir claramente as responsabilidades de cada agente (controlador e operador). A due diligence jurídica sobre esses terceiros deve ser contínua e aprofundada, para além da simples auditoria técnica.

No setor de seguros, um evento de natureza semelhante poderia ocorrer, com a diferença de que, em vez de movimentações financeiras imediatas, o risco maior estaria no uso indevido ou vazamento de dados pessoais. No ambiente securitário os impactos de um vazamento podem ser silenciosos, acumulativos e de difícil mensuração a curto prazo. Muitas vezes, as consequências de um ataque desse tipo só se manifestam meses ou anos depois, de forma difusa e com efeitos duradouros. Surge, então, o protagonismo dos **Relatórios de Impacto à Proteção de Dados Pessoais (RIPD/DPIA)**, conforme o Art. 38 da LGPD, além de normas e orientações da ANPD. Esses relatórios são ferramentas essenciais para identificar e mitigar proativamente os riscos associados ao tratamento de dados pessoais em sistemas complexos como o Open Insurance – e outros sistemas “Open” – modelando cenários de vazamento e uso indevido de dados para avaliar os impactos de longo prazo e propor medidas preventivas.

Naquele cenário, em harmonia com o RIPD/DPIA, ganha ainda mais relevância a proteção das credenciais dos clientes. Tanto a gestão das credenciais quanto sistemas de autenticação frágeis ou pouco sofisticados ampliam a superfície de ataque e aumentam a exposição a riscos. Por isso, é essencial investir em mecanismos modernos e robustos de verificação de identidade, capazes não apenas de evitar acessos indevidos, mas também de empoderar o cliente, garantindo a ele maior controle e transparência sobre quando, como e por quem seus dados estão sendo acessados.

É por isso que, no contexto do Open Insurance, o cumprimento rigoroso da LGPD assume papel central. Mais do que atender a uma obrigação legal, trata-se de um requisito essencial para garantir a confiança dos consumidores em um modelo que se baseia justamente no compartilhamento de dados pessoais. A aderência à LGPD oferece não apenas segurança jurídica, mas também diferenciação competitiva para as instituições que demonstrarem compromisso

efetivo com a privacidade e a proteção dos dados. Em um ambiente aberto e integrado, a conformidade legal deve caminhar lado a lado com controles tecnológicos e boas práticas de governança, assegurando que a inovação avance sem comprometer direitos fundamentais dos clientes.

É fundamental, portanto, que as instituições abordem os desafios práticos da **gestão do consentimento em um ambiente de múltiplos participantes**, garantindo que ele seja livre, informado e inequívoco, e que possa ser revogado a qualquer tempo (Art. 8º da LGPD). Isso exige um mapeamento jurídico detalhado dos fluxos de dados, uma **arquitetura de consentimento granular** que distinga os propósitos de tratamento e a implementação de mecanismos para auditoria e demonstração da base legal para cada operação de tratamento de dados. A atuação de um **Encarregado de Dados (DPO)** com autonomia e conhecimento jurídico é fundamental neste contexto.

Esse conjunto de fatores reforça a necessidade de estratégias contínuas de monitoramento, inteligência aplicada à detecção de anomalias e auditoria rigorosa sobre terceiros. Modelos abertos e integrados, como o Open Insurance e o Open Finance, exigem não apenas conformidade legal e regulatória, mas também solidez operacional e maturidade em cibersegurança. A confiança dos consumidores, afinal, é um ativo intangível que precisa ser protegido com rigor.

O reconhecimento europeu é um passo histórico e deve ser celebrado. Mas, para que ele se converta em vantagem real, o país precisará transformar o avanço normativo em práticas consistentes de segurança e governança. O futuro do Open Insurance – e da economia digital brasileira – dependerá de como conseguiremos equilibrar inovação, regulação e resiliência, garantindo que os marcos conquistados hoje se traduzam em proteção efetiva e em um mercado mais sólido amanhã.

*__Alfredo Viana__, Superintendente Jurídico da Confederação Nacional das Seguradoras, e __Karini Madeira__, Superintendente de Acompanhamento Técnico da Confederação Nacional das Seguradoras

(21.10.2025)