Opinião: Os desafios das empresas com as regras KYC

Em um mundo cada vez mais conectado, o avanço tecnológico desempenha um papel fundamental, proporcionando recursos e oportunidades inéditas. No entanto, esse cenário traz consigo desafios significativos. Sempre há quem utilize as tecnologias para fins ilícitos. Nessa toada, nos deparamos com notícias de incidentes de segurança que expõem dados pessoais e causam prejuízos significativos a titulares e organizações públicas e privadas.

A disponibilização indevida de CPF, por exemplo, permite uma série de fraudes, tais como obtenção de crédito, contratação de serviços e aquisição de produtos. Tais incidentes ainda podem incluir destruição ou uso indevido de dados, interrupção do serviço ofertado durante e após o ataque, além da perda de produtividade. Somados a esses prejuízos, ainda devem ser consideradas as despesas associadas à restauração dos dados e sistemas, à investigação da causa e das falhas de mecanismos e, sobretudo, aos danos reputacionais.

Para evitar e combater esses danos, visando proteger a si mesmas e seus clientes, muitas empresas utilizam mecanismos conhecidos como *Know Your Customer*. O *KYC* — ou, em tradução, "Conheça Seu Cliente" —, é um processo fundamental para verificar e autenticar a identidade de clientes em potencial antes do início da relação comercial.

Ao coletar informações e documentos que verifiquem a identidade do cliente, as empresas buscam garantir que estão lidando com pessoas reais e confirmar que são quem dizem ser. Os principais objetivos do *KYC* podem ser resumidos em prevenção de atividades fraudulentas ou suspeitas e possibilidade de que as empresas conheçam seus clientes e identifiquem possíveis riscos e comportamentos suspeitos.

Sobre os incidentes de segurança, o setor financeiro é particularmente afetado, uma vez que lida com um volume substancial de transações e informações confidenciais dos clientes, que podem vir a ser utilizadas de forma indevida caso caiam nas mãos erradas.

É preciso analisar a interseção entre três elementos essenciais para a segurança das empresas: *Know Your Customer* (*KYC*), a Lei Geral de Proteção de Dados (LGPD) e as normas publicadas pelo Banco Central do Brasil (BCB). Ainda que esses três pontos sejam fundamentais para garantir a conformidade normativa, compatibilizá-los pode ser um verdadeiro desafio para as empresas no cenário atual.

A LGPD, lei que entrou em vigor em 2020 no Brasil, estabelece princípios e regras para o tratamento de dados pessoais e tem como objetivo proteger a privacidade e a segurança das informações dos indivíduos. Um dos princípios-chave previstos pela lei e que devem guiar o tratamento dos dados pessoais é o princípio da necessidade, que limita o tratamento de dados ao mínimo necessário para a realização das finalidades específicas, assegurando que apenas dados pertinentes e não excessivos sejam coletados e utilizados, evitando seu uso indiscriminado.

Por outro lado, as empresas que compõem o grupo de instituições supervisionadas pelo Banco Central (BC) devem cumprir um extenso conjunto normativo, visando garantir a higidez do Sistema Financeiro Nacional, prevenindo, por exemplo, a realização de atividades ilícitas, como lavagem de dinheiro, financiamento ao terrorismo e proliferação das armas de destruição em massa (PLD/FT). Nesse sentido, as instituições financeiras devem cumprir obrigações legais e regulatórias, incluindo requisitos de *KYC*, que envolvem a verificação da identidade dos clientes e a análise de seus perfis e transações.

Em meio a essa complexidade regulatória, as empresas têm dificuldades para conciliar as exigências da LGPD com o regramento estabelecido pelo BC. O desafio reside em encontrar um equilíbrio entre a obrigação de proteger a privacidade e a segurança dos dados pessoais estabelecida pela LGPD e a necessidade de coletar informações para fins de *KYC*, cumprindo deveres legais e regulatórios.

Ainda que as obrigações legais e regulatórias a serem cumpridas pelas instituições financeiras no que diz respeito aos procedimentos de *KYC* sejam um fato consumado, há quem critique e busque obstaculizar tais mecanismos de proteção, utilizando-se do argumento de que tais procedimentos representariam uma violação à privacidade. Trata-se de posicionamento equivocado, pois não só há como coexistirem em harmonia, como constituem um subsistema normativo regulatório que deve ser aplicado e interpretado de forma sistemática.

No que diz respeito à LGPD, há bases legais aptas a justificar o tratamento dos dados pessoais necessários à autenticação, sendo fundamental que as empresas encaixem a operação em alguma das previstas na lei. Destacamos as principais: (a) execução de procedimentos preliminares relacionados ao contrato (artigo 7º, inciso V), já que para autorizar o compartilhamento dos dados e, consequentemente, realizar a contratação da empresa prestadora de serviços, é necessário verificar a autenticidade do cadastro do solicitante; (b) prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos (artigo 11, II, g), quando são tratados dados pessoais sensíveis nos processos de autenticação, como, por exemplo, dados biométricos das digitais e reconhecimento facial; ou (c) cumprimento de obrigação legal ou regulatória (artigo 7º, II ou artigo 11, II, a, LGPD), a depender das regulações do setor.

Somado à justificativa legal, basta que a empresa siga as diretrizes e princípios previstos na LGPD, com destaque para o princípio da finalidade, necessidade e transparência. Quanto ao da finalidade, o objetivo do tratamento é o de alcançar um resultado único, específico e legítimo, que é o de fornecer o serviço selecionado pelo consumidor de modo seguro. Os dados coletados para a finalidade de autenticação não devem ser, portanto, utilizados para outros objetivos senão os informados inicialmente.

Quanto ao segundo, a avaliação da necessidade de mecanismos de autenticação deve analisar o risco da operação, aferindo o grau de sensibilidade dos dados e do cometimento de ilícitos. Nessa linha, o *Good Practice Guide* (*GPG* 45) [1] publicado pelo *Government Digital Services* (*GDS*) do Reino Unido para auxiliar organizações públicas e privadas nos mecanismos de verificação de identidade de usuários traz um processo de verificação de identidade composto por cinco partes.

Segundo o *GPD* 45, não é necessário passar por todas as etapas do processo em um primeiro momento. É possível realizá-las de forma gradual, conferindo um nível de confiabilidade para cada etapa. Após a avaliação dos riscos dos serviços, a organização poderá decidir qual nível de confiabilidade atender (baixo, médio, alto, muito alto), sendo, por exemplo, recomendável adotar um nível de confiabilidade mais alto, se o serviço oferecido apresentar alto risco de crimes relacionados à identidade. Essa lógica pode ser aplicada para todos os setores, regulados ou não no Brasil.

Recomenda-se, ainda, que as informações a respeito do tratamento de dados pessoais estejam dispostas de forma transparente, clara, precisa e acessível aos titulares na Política de Privacidade e nos Termos e Condições de Uso, com canais de comunicação para esclarecimento de eventuais dúvidas.

Em relação às normas do BC, para que as instituições possam alcançar a conformidade regulatória, é necessário obter um rol mínimo de dados e informações de seus clientes, de modo a permitir o início de uma relação comercial. Além de cumprir as obrigações específicas de *KYC*, as quais são diretamente ligadas à prevenção à lavagem de dinheiro, financiamento ao terrorismo e proliferação de armas de destruição em massa (PLD/FT), previstos na Circular BCB nº 3.978/2020 [2], instituições financeiras e não financeiras precisam preencher os requisitos do Cadastro de Clientes do Sistema Financeiro Nacional (CCS), consolidado pela Resolução BCB nº 179/2022 [3].

De aplicação conjunta com a mencionada norma de PLD/FT e com outras tais como as que dispõem sobre regras para abertura de contas de depósito [4] e de pagamentos [5], as instituições devem adotar procedimentos e controles que permitam verificar e validar a identidade e a qualificação dos titulares da conta e, quando for o caso, de seus representantes, bem como a autenticidade das informações fornecidas pelo cliente, inclusive mediante confrontação dessas informações com as disponíveis em bancos de dados de caráter público ou privado.

Ilustrando essa situação, as instituições devem reunir as seguintes informações para validar a identidade e qualificação de titulares pessoas físicas: (1) nome completo, (2) nome completo da mãe, (3) data de nascimento, (4) número de inscrição no CPF, (5) endereço residencial, (6) número de telefone + DDD, (7) comprovante de renda, (8) avaliação se é Pessoa

Exposta Politicamente, (9) data de início e, se for o caso, término do relacionamento com a instituição, (10) dados bancários, dentre eles conta, agência, banco e CPF responsável.

É claro que também devem observar requisitos de segurança da informação, de modo a mitigar riscos de eventual vazamento desses dados, inclusive devendo manter tais dados armazenados e à disposição do Bacen por até dez anos, com eventuais falhas ou inobservâncias dessas obrigações podendo gerar consequências graves à instituição e até mesmo a seus administradores, visto que a atividade de supervisão do regulador pode ser atraída em eventual processo administrativo sancionador [6] que ocasione penalidades a estes atores.

É importante pontuar que a questão pode transcender o âmbito administrativo e resultar em condenações em instâncias judiciais. Seguindo o entendimento da Súmula 479 do STJ [7], caso as instituições financeiras não assegurem o acesso seguro aos seus serviços, o consumidor poderá vir a ser ressarcido em danos materiais e até mesmo morais, em virtude de eventual fraude ocasionada pela falta de mecanismos de segurança do banco, tal como julgado recentemente pela 21ª Câmara de Direito Privado do Tribunal de Justiça de São Paulo [8].

Assim, ao compartilhar alguns dados pessoais para fins de autenticação, o titular acaba renunciando à parcela de sua privacidade, tendo, em contrapartida, ganhos relevantes com a mitigação de riscos e prejuízos futuros por uso indevido de seus dados pessoais.

Nesse contexto, conclui-se que, a LGPD e as normas publicadas pelo BC desempenham papéis essenciais no contexto regulatório brasileiro. É fundamental que caminhem lado a lado para garantir a proteção dos dados pessoais e a segurança financeira. Caso os mecanismos de autenticação sejam implementados seguindo uma lógica de proporcionalidade/necessidade e respeitando as diretrizes da legislação de privacidade, só há um único resultado possível: maior segurança para as empresas e, sobretudo, para os titulares de dados pessoais envolvidos nas operações.

[1] ICO. Digital Identity Position Paper. Disponível em: https://ico.org.uk/media/about-the-ico/documents/2619686/ico-digital-identity-position-paper-20210422.pdf. Acesso em: 25.06.2023.

[2] Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2023/10/Circ_3978_v4_L.pdf

[3] Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=179

[4] Resolução CMN nº 4.753/2019. Disponível em: https://cdn-conjur.s3.amazonaws.com/uploads/2023/07/Res_4753_v3_L.pdf

[5] Resolução BCB nº 96/2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=96

[6] Resolução BCB nº 131/2021. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=131

[7] Súmula 479, Superior Tribunal de Justiça. "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito das operações bancárias".

[8] Processo: 1002473-40.2022.8.26.0011. Link: https://esaj.tjsp.jus.br/cposg/search.do?conversationId=&paginaConsulta=0&cbPesquisa=NUMPROC&numeroDigitoAnoUnific
40.2022&foroNumeroUnificado=0011&dePesquisaNuUnificado=1002473-

40.2022.8.26.0011&dePesquisaNuUnificado=UNIFICADO&dePesquisa=&tipoNuProcesso=UNIFICADO#?cdDocumento=11. Acesso em: 22.06.2023.

Fonte: https://conjur.jumps.com.br/2023-out-28/opiniao-desafios-empresas-regras-kyc/