

SISTEMA FINANCEIRO

Até o momento, em 2024, foram registrados 13 casos de exposição de dados sensíveis relacionados ao meio de pagamento instantâneo, ante apenas um no ano passado

Aumenta vazamento de dados e de chaves Pix

» FERNANDA STRICKLAND

A segurança no sistema Pix é fundamental para garantir a confiança dos usuários e preservar a integridade das transações financeiras em tempo real. Somente em 2024, foram registrados 13 casos de exposição de dados sensíveis relacionados ao meio de pagamento instantâneo — um crescimento significativo em comparação a 2023, em que foi constatado apenas uma ocorrência.

Eleito o meio de pagamento preferido dos brasileiros, vem ganhando novos recursos — entre eles, o pagamento agendado e, posteriormente, pagamento por aproximação. Diante de seu uso abrangente, a proteção contra fraudes e ataques cibernéticos é essencial para evitar prejuízos tanto para usuários quanto para empresas.

De acordo com Alexander Coelho, sócio do Godke Advogados e especialista em Direito Digital e Proteção de Dados, ao introduzir novas funcionalidades, como o agendamento de pagamentos e a opção por aproximação, o Pix amplia sua conveniência, mas também precisa redobrar os cuidados com segurança e proteção de dados.

“O agendamento de pagamentos, por exemplo, requer que informações do usuário fiquem armazenadas por mais tempo, o que exige um fortalecimento das medidas de segurança para evitar acesso indevido. Se não houver proteção adequada, o armazenamento prolongado desses dados aumenta o risco de que informações sejam capturadas em vazamentos ou acessadas por terceiros mal-intencionados”, explica.

No caso do pagamento por aproximação, a segurança depende de uma implementação cuidadosa do sistema de autenticação, especialmente por meio de dispositivos móveis. “A autenticação em dois fatores e a utilização de chaves dinâmicas e criptografia robusta são essenciais para proteger o usuário em transações que possam ser realizadas inadvertidamente ou em proximidade com outros dispositivos”, acrescenta Coelho.

Ele ressalta que o pagamento por aproximação exige que o usuário esteja atento a notificações e bloqueios automáticos em caso de movimentações suspeitas, uma vez que o uso físico pode aumentar o risco de transações fraudulentas em áreas de grande circulação.

Essas inovações, ainda que tragam praticidade, também ressaltam a importância de práticas de segurança robustas e da educação dos usuários sobre medidas de proteção. “Novos recursos também representam novas superfícies de ataque para fraudadores, e é crucial que tanto os provedores quanto os usuários estejam vigilantes e preparados para proteger esses dados”, defende o especialista.

Para Rafael Federici, sócio do CNF Advogados e especialista em Direito Digital e Proteção de Dados, o Pix tem uma estrutura central gerenciada pelo Banco Central do Brasil e é considerado um sistema altamente seguro, especialmente porque as informações das transações trafegam de forma criptografada na Rede do Sistema Financeiro Nacional, que é uma rede totalmente apartada da internet.

No entanto, o advogado explica que qualquer transação via Pix começa na autenticação dos usuários, que é feita por bancos, instituições de pagamento e fintechs. Para que isto ocorra, estes participantes necessitam guardar as chaves PIX dos usuários e os dados cadastrais básicos a elas associados.

“Normalmente, os vazamentos de dados não ocorrem por

Proteção

Para evitar vazamentos e proteger suas informações pessoais e empresariais, siga estas práticas recomendadas por especialistas



1. Crie senhas fortes e únicas:

Utilize senhas complexas e diferentes para cada conta. Evite usar informações pessoais como datas de nascimento ou nomes de familiares. O ideal é combinar letras maiúsculas e minúsculas, números e caracteres especiais.

2. Ative autenticação em duas etapas (2FA):

Sempre que possível, ative a autenticação em duas etapas. Ela adiciona uma camada extra de segurança, exigindo um segundo fator de verificação além da senha, como um código enviado para seu celular.

3. Cuidado com e-mails e links suspeitos:

Evite clicar em links ou abrir anexos de e-mails de remetentes desconhecidos. Golpes de phishing são comuns e tentam roubar suas informações pessoais ou financeiras. Sempre verifique a origem dos e-mails antes de interagir.

4. Mantenha seus dispositivos atualizados:

Instale as atualizações de segurança e patches fornecidos pelos fabricantes de software e dispositivos. Essas atualizações corrigem vulnerabilidades conhecidas que podem ser exploradas por hackers.

5. Prefira serviços com criptografia:

Escolha plataformas que oferecem criptografia de ponta a ponta para proteger suas comunicações e dados armazenados. Isso assegura que apenas você e as partes autorizadas possam acessar suas informações.

6. Monitore suas contas regularmente:

Verifique com frequência suas contas bancárias, de crédito e outras plataformas para identificar qualquer atividade suspeita. Considere utilizar serviços de monitoramento de crédito para detectar fraudes rapidamente.

7. Implemente políticas de segurança de dados:

Se você gerencia uma empresa, desenvolva políticas claras sobre como os dados confidenciais devem ser protegidos, armazenados e compartilhados. Eduque seus funcionários sobre essas políticas e a importância de segui-las.

8. Limite o acesso a dados sensíveis:

Apenas pessoas autorizadas devem ter acesso a dados confidenciais. Revise regularmente as permissões de

acesso e faça ajustes quando necessário para evitar exposição desnecessária de informações.

9. Utilize criptografia de dados:

Implemente criptografia tanto para dados armazenados quanto para dados em trânsito. Mesmo que alguém consiga interceptar as informações, elas estarão protegidas e inacessíveis sem a chave de criptografia.

10. Realize treinamentos de conscientização em segurança:

Forneça treinamento contínuo aos seus funcionários sobre práticas de segurança cibernética, incluindo como identificar tentativas de phishing e como proteger informações sensíveis. Isso ajuda a criar uma cultura de segurança dentro da empresa.

11. Controle de redes Wi-Fi:

Evite usar redes Wi-Fi públicas ou não seguras para acessar informações sensíveis ou realizar transações financeiras. Quando necessário, utilize uma Rede Privada Virtual (VPN) para garantir que sua conexão esteja protegida.

12. Revise configurações de privacidade:

Verifique regularmente as configurações de privacidade das suas contas de mídia social e outras plataformas digitais. Limite o acesso às suas informações pessoais para proteger sua privacidade.

13. Desconfie de ofertas excessivamente boas:

Golpes de phishing muitas vezes se disfarçam de promoções ou ofertas muito vantajosas. Se algo parecer bom demais para ser verdade, desconfie, pois pode ser uma tentativa de roubo de dados.

14. Faça backup regular de dados:

Realize backups frequentes das suas informações importantes, seja em serviços de armazenamento na nuvem ou em dispositivos físicos, como discos rígidos externos. Isso garante que, em caso de ataque ou falha, seus dados estarão protegidos.

15. Use antivírus e firewalls:

Mantenha programas antivírus e firewalls atualizados para proteger seus dispositivos contra malware e outras ameaças cibernéticas. Esses sistemas ajudam a detectar e bloquear tentativas de acesso não autorizadas.

Fonte: Membro da Comissão Especial de Privacidade e Proteção de Dados da OAB/SP, Antonielle Freitas



Isso evidencia uma necessidade urgente de revisão e fortalecimento das medidas de segurança adotadas pelas instituições financeiras e de pagamento”

Antonielle Freitas, membro da Comissão Especial de Privacidade e Proteção de Dados da OAB/SP

falhas no sistema central de transações gerenciado pelo Banco Central, mas sim nas pontas da operação, ou seja, nas instituições que realizam a autenticação de usuários. Os vazamentos ocorrem invariavelmente por falhas de segurança da informação nas instituições participantes, ou seja, vulnerabilidades provocadas por configurações inadequadas, softwares desatualizados, erro humano ou ataques cibernéticos”, afirma.

Problema alarmante

Os recorrentes vazamentos de

dados envolvendo o sistema Pix têm gerado crescente preocupação entre especialistas, usuários e autoridades. Antonielle Freitas, membro da Comissão Especial de Privacidade e Proteção de Dados da OAB/SP, alerta sobre a gravidade da situação. “É alarmante que este seja o 13º vazamento de dados pessoais vinculados ao Pix apenas neste ano. Isso evidencia uma necessidade urgente de revisão e fortalecimento das medidas de segurança adotadas pelas instituições financeiras e de pagamento”, afirma Freitas.

Embora o Banco Central tenha destacado que os dados expostos sejam de natureza cadastral — como nome, CPF, instituição de relacionamento, agência e número da conta — e não incluam informações sensíveis, como senhas ou saldos financeiros, os riscos ainda são significativos. Dados cadastrais podem ser usados em golpes de engenharia social, como tentativas de fraudes financeiras e roubo de identidade.

A Lei Geral de Proteção de Dados (LGPD) estabelece que as instituições financeiras têm o dever de adotar medidas técnicas e administrativas robustas para proteger informações pessoais contra acessos não autorizados e outros tipos de incidentes. No entanto, casos como esses demonstram que as falhas

nos sistemas ainda são recorrentes, comprometendo a segurança dos usuários.

“Esses dados podem ser utilizados em tentativas de fraude ou para fins de engenharia social”, alerta Freitas. Ela enfatiza que, além da identificação das falhas, é imprescindível que as instituições implementem medidas corretivas e adotem uma postura transparente com os titulares dos dados. “A transparência na comunicação com os titulares dos dados é fundamental. O Banco Central e as instituições envolvidas devem garantir que as notificações sejam claras e forneçam orientações sobre como os titulares podem se proteger contra possíveis fraudes.”

Para mitigar os riscos, o Banco Central orientou que os usuários sejam informados sobre os incidentes exclusivamente por canais oficiais, como aplicativos ou internet banking. Segundo Freitas, essa medida reduz a possibilidade de golpes adicionais, mas deve ser acompanhada de uma política mais ampla de proteção.

“Por fim, é importante que as medidas sancionadoras previstas na regulação vigente sejam aplicadas de forma rigorosa para que sirvam de exemplo e incentivo para que todas as instituições reforcem suas práticas de segurança e conformidade com a LGPD”, pontua a especialista.

Brasil S/A

por Antonio Machado



machado@cidadebiz.com.br

Nem vem que não tem

Três cenários se avistam depois da forte pancada, exagerada até, do Banco Central, ao elevar de 11,25% ao ano para 12,25% a taxa de juro básica, a Selic, mostrando-se o “adulto na sala” em meio à algazarra tanto do governo, encantado com o crescimento movido a gasto público, quanto do mercado financeiro, ensandecido com os riscos potenciais de descontrole das contas nacionais.

Sem mudanças capazes de repor a trajetória da inflação a meta de 3% ao ano, hoje dilatada pela máxidevalorização do real frente ao dólar e pelo universo de mais de 100 milhões de pessoas recebendo algum tipo de renda mensal paga com dinheiro público, o BC indicou mais duas altas equivalentes da Selic, elevando-a a 14,25% até a reunião do Copom de março. Ou mais: o Itaú, por exemplo, prevê que a taxa do overnight chegará a 15% e ficará assim o ano inteiro.

Juro alto é o caroiço de abacate entalado na garganta da economia.

“A magnitude total do ciclo de aperto monetário será ditada pelo firme compromisso de convergência da inflação à meta e dependerá da evolução da dinâmica da inflação”, alertou o BC. Alertou quem?

Os que supõem que a nova diretoria, liderada pelo atual diretor de Política Monetária, Gabriel Galípolo, será leniente com sua missão, dada pelo mandato de autonomia operacional e baseada no que lhe impõe como diretor do Conselho Monetário Nacional, subordinado ao presidente Lula.

Não se espere acanhamento se o PT tentar intimidar o BC, como fez com o presidente de saída, Roberto Campos Netto. Ou seja: com Galípolo e os novos diretores, o BC assumiu o assento do motorista.

Tem também um alerta aos traders de títulos da dívida do Tesouro Nacional, os tais fariálimers, acostumados a especular com o caos. Gestores de fundos, não os bancos, formam os preços de mercado dos juros e do câmbio, cabendo à CVM (Comissão de Valores Mobiliários) fiscalizá-los e regulá-los. Se houver leniência nessa função, algo será feito. A ortodoxia não é por convicção, é por necessidade.

Esta é a realidade daqui para frente, lembrando que, ao contrário das cadeiras ministeriais, as do BC têm mandato e missões legais.

Três cenários disponíveis

Um BC reconhecido como técnico e profissional, além de conhecedor das mumunhas do tal “mercado” disfarçadas de rigor acadêmico, com a ajuda de comentaristas de olhar compungido, fará bem à economia e ao governo, ao menos enquanto carecer de formuladores no ministério.

Como o presidente se espreme entre um Congresso de larga maioria conservadora, incompreensão sobre a insatisfação popular depois de mais de 20 anos de políticas de transferência de renda sem grande impacto na transformação social, e empresariado boca de siri, com temor de ser ativo no debate político, restam-lhe poucas opções.

No primeiro cenário, o governo Lula emula a transição da gestão de Dilma Rousseff. Ela escancarou o Tesouro Nacional na campanha pela reeleição, assumiu o segundo mandato tentando frear o que já estava empenhado na gestão pública, e fracassou. Dado o que veio em seguida para ela, dificilmente o presidente fará o mesmo.

No segundo cenário, haveria uma ligeira mudança no jogo ensaiado entre ele e o ministro Fernando Haddad, de modo a que o pacotinho de contenção de despesas obrigatórias, que crescem há anos acima do ritmo do PIB, fique um pouco mais salgado. Essa via se inviabilizou com as idas e vindas da dupla, dando tempo a que o Congresso se articulasse para não aparecer como algoz de políticas sociais meritórias, porém, sem aderência com a realidade fiscal.

No terceiro, mais provável, o governo estica até onde o Congresso permitir, e sua permissão tem correlação com os fundos das emendas com os quais os parlamentares irrigam suas bases eleitorais e as mesas da Câmara e do Senado pilotam as votações de projetos de lei e emendas constitucionais. É o conhecido arroz com feijão.

As verdades incômodas

Algumas verdades incômodas precisam ser ditas. A primeira é que o crescimento tem sido puxado há anos mais por estímulos fiscais ao consumo, não por ações diretas para empinar a oferta, conforme os modelos bem-sucedidos na Ásia e, logo no pós-Guerra, nos EUA e na Europa (e aqui também dos anos 1950 a 1970).

Outra verdade é que governos endividados e bancados por dívidas de curto prazo e juros altos enriquecem quem tem renda e caixa livres para aplicar em papéis. Não há como diminuir esse desequilíbrio só com transferências e isenções tributárias, a proposta do governo para tentar atrair a classe média, na qual tem menos apelo eleitoral.

Uma terceira verdade: dívida contraída para bancar bons projetos de expansão da base produtiva e novas tecnologias não só se paga, como é ela, na modalidade privada, que tem deslançado o programa de concessões e de obras do PAC. Hoje, papéis como debêntures têm maior importância ao investimento que o crédito em banco estatal.

A combinação dessas verdades à visão de que larga parte da população tem renda garantida pelo Estado permitiria implantar um mercado de consumo de massa e, aos poucos, tirar tais estímulos ao longo de, digamos, uma década, com empregos e crédito acessível e barato. Esta é a grande diferença entre países bem-sucedidos no mundo e a América Latina: ênfase mais no crédito que em gasto público, sobretudo direto, além de educação de nível elevado e indução competitiva para exportar. Ou é isso ou é a inação.

Último muro de contenção

Uma mudança para valer não virá de um governante iluminado nem de um plano econômico matador. Virá de construção coletiva.

Da política, que tem que se impor em vez de caçar prebendas do governante de turno, afrontando a vontade de quem o elegeu. Ou seja: o centro não se centrão e a esquerda voltar a suas raízes desenvolvimentistas, abandonando o populismo eleitoral. Virá do empresariado se vendo como parte da solução, que está na tecnologia e não no passado.

E como tem dois anos adiante antes de outra campanha, o presidente precisaria dispor de acesso organizado a ideias e opções tal como teve nos dois primeiros mandatos. Sem isso, terá um Congresso pouco disposto a validar o que o fortaleça para 2026, um mercado financeiro descabelando a racionalidade e o BC como último muro de contenção, entre o caos e o equilíbrio, ao custo de minar a saúde financeira pela falta de ajuste fiscal merecedor de crédito.

Essas são as possibilidades, diminutas para um país promissor.