Chaimovich e Zappelini: Megavazamentos de chaves Pix

25/03/2022

O Instituto de Estudos Estratégicos de Tecnologia e Ciclo de Numerário (ITCN) vem atuando na proteção e na defesa de usuários finais dos mais diversos meios de pagamento, consumidores e cidadãos. Preocupado com o fato de o Banco Central (Bacen) ser, ao mesmo, o implementador, fiscalizador e regulador do Pix e, ainda, com os frequentes vazamentos de chaves Pix, bem como de dados sensíveis de milhares de clientes de instituições financeiras, o ITCN subscreveu, neste mês de março, ofícios ao Bacen e à ANPD (Autoridade Nacional de Proteção de Dados). Neles, solicitou a instauração de processo administrativo para apurar não só as circunstâncias dos incidentes que ocorreram, mas também para que o Bacen avalie a sua responsabilidade, no âmbito das atividades que exerce no cerne do arranjo, perante a Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente quanto ao controle e à gestão do tratamento de dados relacionados a este ecossistema de pagamentos instantâneos.

No documento entregue à ANPD, o Instituto requer a instauração de processo administrativo sancionador cobrindo particularmente os recentes incidentes de vazamento de dados relacionados ao Banese e à Aceso, alcançando o Banco Central. Nesse sentido, o Bacen precisa implementar mecanismos de controle isentos e independentes, dotados de governança ativa e de resultados, em relação às operações de tratamento de dados pessoais realizadas no arranjo do Pix.

É importante ressaltar que tanto o Instituto quanto seus associados têm plena consciência de que transações via pagamentos instantâneos no arranjo Pix possuem aprovação da ampla maioria da sociedade brasileira, e não se pretende limitar as alternativas de pagamentos dos cidadãos, apenas somar àquelas já existentes, desde que com todos os devidos cuidados em relação à *segurança* e à *privacidade* de seus usuários, bem como atentando a aspectos de *regulação* desses serviços. Existem diversos desafios nesse contexto, e vamos destacar aqui tão somente aqueles ligados à segurança, física e de dados, dos usuários; incluindo fatores que influenciam diretamente na sua privacidade. Como desdobramentos fundamentais desses desafios, vale destacar a questão da desbancarização da população; da suposta substituição do

dinheiro em espécie por meios exclusivamente eletrônicos e da utilização crescente de dados pessoais.

Arranjos de pagamento obtém sucesso quando são consideradas todas as frentes de potenciais efeitos colaterais e riscos advindos de sua utilização, sejam eles de ordem legal/regulatória, logística ou tecnológica. Isso significa que, quando se trata de arranjos de pagamento instantâneo — expressão definida nas diretrizes do BIS (Banco de Compensações Internacionais) —, "efeitos" e "riscos" devem ser parte de qualquer análise prévia de viabilidade segura. O problema é que, em certos países, a pressa em estruturar tais arranjos pode conduzir à adoção de padrões operacionais não suficientemente — ou apenas minimamente — seguros.

Pensando nos arranjos de pagamento, as vulnerabilidades dos usuários devem ser avaliadas em seus impactos sociais, tanto por instituidores como por fiscalizadores e reguladores desses verdadeiros ecossistemas. Isso porque arranjos de pagamento dependem da relação de muitos fatores, entre os quais os dados que usuários devem tornar disponíveis para que tenham acesso às funcionalidades da ferramenta. A probabilidade de ocorrências negativas e seus impactos não é baixa e os mecanismos atualmente utilizados demonstram-se inadequados e insuficientes, o que não é aceitável. Esses dados devem, portanto, ser tratados conforme a sua natureza, ou seja, como dados sensíveis, que estão inseridos em variadas operações de alto risco, devendo ser realizado Relatório de Impacto à Proteção de Dados Pessoais, e adotadas medidas apropriadas de mitigação de riscos e de segurança. Afinal, eles têm o viés de causar danos e culminar na exposição e discriminação dos usuários, assim como aconteceu nos vazamentos mencionados.

No caso do Pix, tem-se noticiado diariamente eventos, desde os golpes mais simples aos mais elaborados — como sequestros relâmpagos —, que cresceram de maneira vertiginosa desde a sua implementação. Por óbvio, atos criminosos não desqualificam uma boa iniciativa, e tampouco podem ser explicados exclusivamente por fraquezas de segurança ou de controle. Mas é fato que os mecanismos até agora adotados para proteger os usuários do Pix não se mostraram eficazes e apropriados. Talvez iniciativas isentas de falhas ainda não sejam possíveis, mas deve ser admitida e devidamente considerada a gravidade do quadro, com a adoção de medidas adicionais. É relevante falarmos, também, em educação digital: *de que maneira podemos capacitar a população para lidar com os golpes de maneira mais informada?*

No mais, de volta à questão sobre incidentes de segurança envolvendo dados pessoais de usuários do Pix, outras preocupações merecem ser avaliadas. O quadro pode ser ilustrado por meio de dois grandes incidentes que foram comunicados e noticiados: o primeiro deles levou ao "vazamento" de 414.526 chaves Pix que o Banco do Estado de Sergipe S. A. (Banese) armazenava; e o segundo provocou o "vazamento" de 160.147 chaves Pix da Acesso Soluções de Pagamento S.A. Mencionamos, aqui, apenas os vazamentos de maiores quantidades de dados, mas esses não foram os únicos casos.

O Banco Central emitiu notas públicas sobre os incidentes. Em ambos os casos, a justificativa apresentada pela autarquia foi a presença de "falhas pontuais" no âmbito daquelas instituições. Também assegurou que não teria ocorrido exposição de "*dados sensíveis, como senhas, informações ou saldos financeiros em contas transacionais, ou outras informações sob sigilo*

bancário".

Cabe destacar, aqui, três pontos que merecem nossa atenção: 1) pela natureza dos comunicados, o Banco Central não considerou que chaves Pix — foco do vazamento — são dados pessoais de primeiro grau. Além disso, 2) o vazamento das chaves Pix abriu portas para o vazamento de dados pessoais típicos, como aqueles que integram o cadastro dos usuários do arranjo. Ademais, 3) apesar de o Bacen ter centrado sua preocupação em "dados financeiros", inclusive os protegidos pelas normas de sigilo bancário, é importante ressaltar que, além deles, há dados pessoais típicos, que a legislação de proteção à privacidade e dados pessoais abrange e salvaguarda.

Além disso, vale repisar que o Banco Central é, ao mesmo tempo, instituidor, fiscalizador e regulador do Pix, logo, possuindo competência legal para disciplinar as práticas do Pix, exercendo gestão sobre sua infraestrutura.

Tendo em vista esses fatos e a preocupação com a disseminação de informações perante a sociedade civil, o objetivo do ITCN ao protocolar esses ofícios foi solicitar que, por parte do Banco Central, fosse feita comunicação formal à ANPD sobre os vazamentos de chaves Pix havidos no Banese e na Acesso. Além disso, que houvesse a instauração, pelo BC, de processo administrativo interno para apurar não somente as circunstâncias dos incidentes, mas, também, suas responsabilidades sob a LGPD quanto ao controle e à gestão do tratamento de dados pessoais relacionados ao Pix em ambas as instituições. Finalmente, solicitou-se que o BC adotasse processos e procedimentos para que se evite, quanto possível, a concentração de competências que afete as boas práticas de governança, tendo em vista a atual configuração do sistema Pix. Finalmente, foi solicitada a instauração, pela ANPD, de processo administrativo sancionador, cobrindo os dois incidentes de segurança ocorridos e alcançando o Banco Central e as instituições relacionadas aos vazamentos.

Com isso, pretendemos chamar a atenção para a necessidade de fortalecer os mecanismos de governança e de controle nesta que já é uma forma de pagamento amplamente usada pela população brasileira.

Fonte: https://conjur.jumps.com.br/2022-mar-25/chaimovich-zappelini-megavazamentos-chaves-pix/