Ofício nº 01/2022

São Paulo, 02 de março de 2022.

A Suas Senhorias

Senhor **Roberto Campos Neto**
DD. Presidente do Banco Central do Brasil

Senhor **Paulo Souza**
DD. Diretor de Fiscalização

Senhor **Otavio Ribeiro Damaso**
DD. Diretor de Organização do Sistema Financeiro e Resolução

Senhor **Otavio Ribeiro Damaso**
DD. Diretor de Regulação

Banco Central do Brasil – BCB
Setor Bancário Sul (SBS), Quadra 3, Bloco B, Edifício Sede
Brasília – DF – 70074-900

C/c a Sua Senhoria
Senhor **Waldemar Gonçalves Ortunho Júnior**
DD. Diretor-Presidente da Autoridade Nacional de Proteção de Dados – ANPD
Esplanada dos Ministérios, Bloco C, 2º andar
Brasília – DF – 70046-900

Assunto: **Arranjo PIX. Dados Pessoais. Riscos Legais. Exposição.**

Senhores Presidente, Diretores e Diretor-Geral

Cumprimentando V. Sas., e baseada no **direito constitucional de petição** (CF, art. 5º, inc. XXXIV, al. *a*), nossa entidade, na condição de representante dos interesses nacionais e de muitos, cidadãos e organizações, que se servem de arranjos de pagamento instituídos pelo Banco Central do Brasil – como o Pix –, expõe, haja vista os muitos incidentes de segurança envolvendo ***chaves Pix*** e ***dados pessoais***, preocupações relacionadas com esse arranjo, que na verdade pode até mesmo ser considerado um verdadeiro ecossistema de pagamentos.

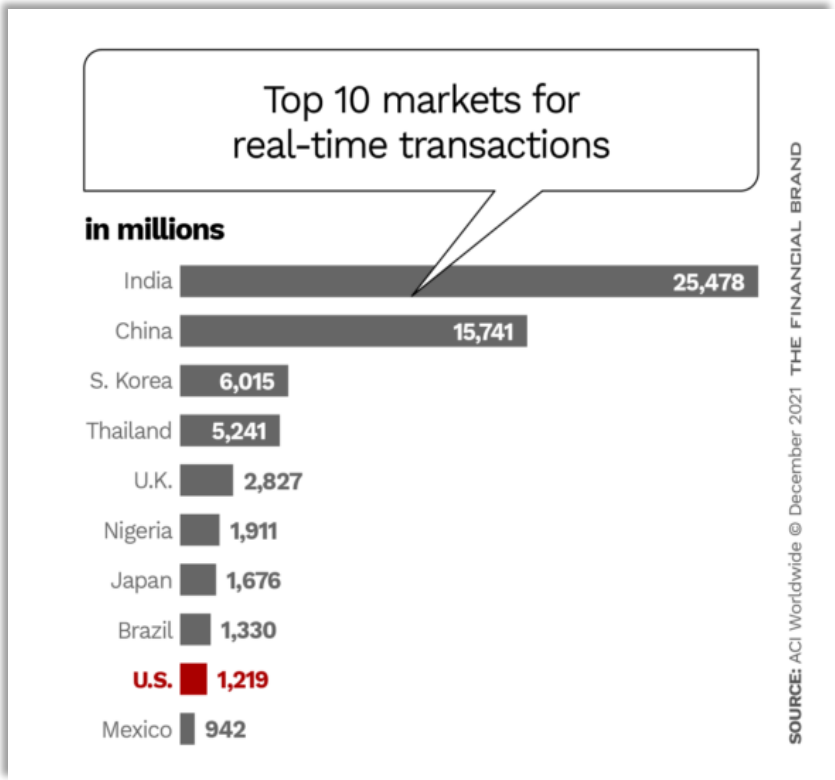
Para tanto, trazemos fatos e elementos para iniciar uma interlocução embasada em dados e informada com vossas senhorias, com o objetivo de sugerir aprimoramentos no cenário atual.

1. Parte A: Quadro Atual

Números de 2021, do Relatório ACI Worldwide e GlobalData, demonstram que quase 71 bilhões de transações de pagamento em tempo real foram globalmente processadas em 2020, indicando crescimento de mais de 41%, se considerado o ano de 2019. Pagamentos digitais passaram a ocupar o lugar do dinheiro e do cheque, principalmente com o avanço da pandemia provocada pelo coronavírus[1].

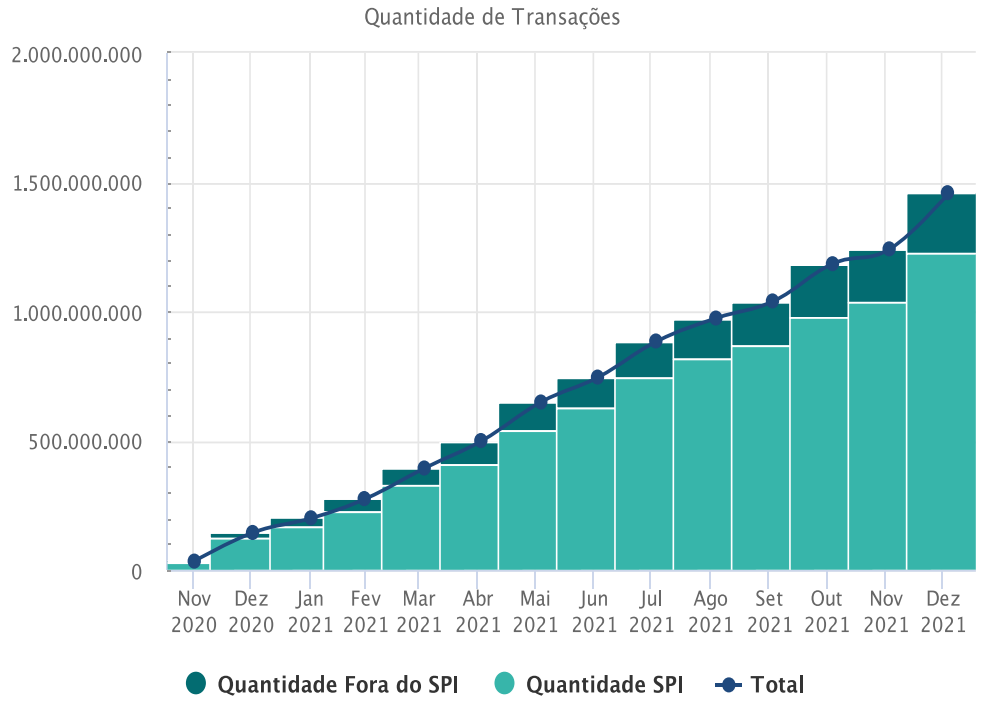
O mesmo relatório aponta uma projeção de taxas de crescimento superiores a 23% até 2025 para o mercado mundial de pagamentos instantâneos, alcançando países economicamente diversos como Brasil, México e Malásia.

Muito embora o Brasil ainda seja relativamente novo nesse mercado, é fato que transações via pagamentos instantâneos no arranjo Pix têm aprovação de 85% dos cidadãos brasileiros, representam 7 em cada 10 operações dos *bancarizados* e contam com cerca de 360 milhões de chaves cadastradas no arranjo, segundo estudo da Febraban[2]. Mas esses elementos ainda não competem com outros países em que os pagamentos instantâneos, ou *instant payments* também encontraram terreno fértil, como mostra o levantamento adiante, referido em *The Financial Brand*[3]:



[1] Cf. Relatório ACI Worldwide e GlobalData, disponível em https://investor.aciworldwide.com/news-releases/news-release-details/global-real-time-payments-transactions-surge-41-percent-2020#:~:text=Top%2010%20countries%20globally%20by,th%20place%20with%202.8bn. Acesso: 20.02.2022.
[2] Disponível em https://noomis.febraban.org.br/temas/meios-de-pagamento/pix-e-aprovado-por-85-dos-brasileiros-diz-estudo-da-febraban. Acesso: 20.02.2022.
[3] Disponível em https://thefinancialbrand.com/126573/7-major-payment-trends-that-will-shake-up-banking-in-2022/. Acesso: 20.02.2022.

Em simetria, o Banco Central do Brasil (BCB), nas estatísticas relacionadas ao Sistema de Pagamentos Instantâneos (SPI)[4], demonstra o significativo – e consistente – avanço do uso do Pix como instrumento de transações financeiras em tempo real, como se vê no gráfico abaixo[5]:



No curso dessa tendência, muitos e graves desafios surgem. Nesse sentido, usuários, governo, instituições financeiras e outros tantos agentes precisam, antes de mais nada, identificá-los e estabelecer com celeridade e visão estratégica os rumos a serem tomados. Num mundo em que as transações financeiras derivam para o que vem sendo chamado *hyperfast payment* (HFP) – sistemática e modelagem P2P –, operadores devem ter em mente que o arranjo de pagamento instantâneo não é um fim em si mesmo.

Dentre esses desafios, um grupo que pode ser destacado e é considerado 7T (ou *seven trends*), consiste em pelo menos sete argumentos: **i**) *bancarização* e *desbancarização*; **ii**) substituição do dinheiro em espécie; **iii**) digitalização massiva; **iv**) maior e melhor uso de criptomoedas; **v**) virtualização de transações; **vi**) rastreabilidade; e **vii**) utilização crescente de dados pessoais.

Como conceito, os FPSs (*Fast Payment Sistems*) embutem muitas vantagens, e podem se inserir no macroconceito de "benefício social por inclusividade". Mas o problema é que sistemas com perfil 7/24/365 (*full-on*) precisam vencer obstáculos não necessariamente inerentes e que nem sempre têm a ver com velocidade (3,4 bilhões de transações, em média[6], segundo o Banco Central Europeu) ou imediata disponibilidade de fundos. Não raro, esses obstáculos estão mais na linha da **segurança**, **privacidade** e **rigor regulatório**, ainda que o discurso de acessibilidade, ampla cidadania financeira e disponibilidade imediata de recursos, embora louvável, possa ser questionado. Entretanto, os bons índices não são suficientes para que esses obstáculos sejam ignorados.

[4] Disponível em https://www.bcb.gov.br/estabilidadefinanceira/estatisticas_spi. Acesso: 20.02.2022.
[5] Disponível em https://www.bcb.gov.br/estabilidadefinanceira/estatisticaspix. Acesso: 20.02.2022.
[6] Cf. https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op229~4c5ec8f02a.en.pdf. Acesso: 20.02.2022.

Bons arranjos de pagamento colhem sucesso justamente porque consideram todos os "efeitos colaterais" e "riscos próprios e impróprios", independentemente de sua origem – seja ela legal, logística, regulatória ou tecnológica. Justamente por isso, em 2020, em sua reunião ordinária, os representantes de governos e de bancos centrais do G20 endossaram um relatório[7] que, conquanto mais direcionado a práticas anticorrupção e antilavagem de recursos, já advertia para a necessidade de que instituições e governo adotassem medidas para garantir transparência, governança, responsabilidade, regularidade e conformidade legal às transações de tráfego imediato. Mais ainda: esse relatório (dado a público em 2021) *reforçou a recomendação de abordagem dos riscos associados a arranjos de pagamento, com ênfase para os de natureza imediata, notadamente à medida que o volume de transações aumenta em escala mundial*.

Isso significa que, quando se trata de arranjos de *pagamento instantâneo* – expressão definida nas diretrizes do BIS (*Bank for International Settlements* ou Banco de Compensações Internacionais)[8] –, "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, quase sempre justificada pela premência concorrencial com outros atores, cuja vivência internacional é avassaladoramente mais madura, conduziu à adoção de padrões operacionais não suficientemente - ou só minimamente - seguros.

Esse posicionamento traduziu-se no que é conhecido por *acceptable side cost*, conceito também chamado *acceptable risks*, que consiste na "**estratégia consciente de reconhecer a possibilidade de riscos pequenos ou infrequentes sem tomar medidas para proteger, segurar ou evitar esses riscos**"[9]. Isso implica que os custos necessários para essas medidas seriam demasiadamente altos para se justificar, considerada a baixa probabilidade de uma ocorrência negativa ou seu pequeno impacto.

Porém, essa lógica não funciona adequadamente quando se trata de arranjos de pagamento, cujas vulnerabilidades devem ser avaliadas em seus impactos sociais, por instituidores, fiscalizadores e reguladores. Isso se explica porque arranjos de pagamento dependem, intrinsecamente, da inter-relação de muitos fatores e elementos, ***entre os quais os dados que usuários devem tornar disponíveis para que tenham acesso às funcionalidades da ferramenta***. Nesse caso, os riscos não se demonstram aceitáveis, pois a probabilidade de ocorrências negativas e seus impactos está longe de ser baixa. Ademais, os riscos do arranjo crescem exponencialmente, considerando a exposição do usuário a fraquezas que lhe são impostas pela usabilidade do arranjo[10].

Nesse sentido, tem-se altos riscos à privacidade do usuário, o que é somando à falta de transparência e de informações suficientes e adequadas sobre a utilização do arranjo e suas consequências. Tampouco fica evidente ao usuário e titular de dados pessoais como ocorre o seu tratamento, quem são os agentes envolvidos nas operações, e em decorrência disso, quais agentes podem ser acionados dentro da cadeia de proteção de dados pessoais. Esse tipo de tratamento envolve dados que podem ser considerados de natureza sensível. A sua exposição ou risco de exposição têm

[7] Disponível em https://www.fatf-gafi.org/media/fatf/documents/reports/Opportunities-Challenges-of-New-Technologies-for-AML-CFT.pdf. Acesso: 20.02.2022.
[8] Disponível em https://www.bis.org/cpmi/publ/d154.pdf. Acesso: 20.02.2022.
[9] MILES, Roger. *Conduct Risk Management*. [s. ed.], Londres: Kogan Page Ltd, 2017, pp. 108 e ss.
[10] Cf. https://www.finextra.com/blogposting/11339/instant-payments-a-critical-assessment. Acesso: 20.02.2022.

o viés de colocar o titular em situação discriminatória e degradante. Esses dados devem, portanto, ser tratados conforme a sua natureza: dados sensíveis, cuja operação é de alto risco, devendo ser realizado Relatório de Impacto à proteção de dados pessoais, com a adoção de medidas de mitigação de riscos e de segurança apropriadas.

De igual modo, riscos à segurança também devem ser mitigados, até porque um arranjo de pagamentos, como qualquer outro instrumental que exponha o usuário em alguma medida, precisa assegurar que as transações não apenas ocorram dentro de ambiente tecnologicamente protegido, mas que também sejam **confiáveis**. E, nesse contexto, a **confiabilidade** não é apenas **do** sistema, mas **no** sistema. O recente (íssimo) arranjo instituído pelo Banco Central – o **Pix** – carece da implementação de medidas de segurança suficientes para proteção do usuário e minimização dos riscos envolvidos na operação.

Há anos, especialmente com a publicação do *Relatório de Vigilância do Sistema de Pagamentos Brasileiro* de 2013[11], o arranjo começou a ser gestado na criação do grupo de trabalho *GT Pagamentos Instantâneos*, integrado pelo BCB e agentes do mercado, cujos trabalhos se encerraram em 2018, do que resultou a publicação dos Comunicados nº 32.927/18[12] e nº 34.085/19[13], detalhando os requisitos-base do ecossistema de pagamentos instantâneos.

Um propósito do Banco Central com essas medidas, origem do arranjo de pagamentos instantâneos conhecido por Pix, foi incrementar a eficiência e a segurança daquele ecossistema, assim como induzir competitividade, abrangência e inclusão financeira, segundo explicava a Carta Circular nº 4.006/20[14]. Em sequência, foi editada a Resolução nº 1/20, que instituiu formalmente o Pix, como previra o Bacen[15].

Contudo, mesmo secundado por outras normas e medidas, parte expressiva voltada à operacionalidade do arranjo, não foi suficiente – ou eficaz o bastante – para que o Pix se mostrasse hígido, seguro e confiável, considerando as tecnologias disponíveis e razoáveis para tanto.

Sob o prisma estatístico, o Pix parece ter encontrado aderência na rotina dos brasileiros[16]. No entanto, não é amplamente divulgado o número de eventos negativos envolvendo o Pix, o que também assolou os cidadãos e as empresas. A quantidade (e intensidade) de "golpes" aumentou, dos mais simples aos sofisticados, e, como indica a Febraban, alguns – como o falso representante de instituição financeira ou de falsa central de atendimento – cresceram 340% no curso da pandemia[17].

Evidentemente, o fenômeno social "golpes" não é recente, ou mesmo exclusivo de ambientes digitais. Contudo, com a *Internet* e a popularidade dos meios eletrônicos de negócio, somados à velocidade de transmissão de dados, práticas criminosas cresceram em progressão

---

[11] Disponível em https://www.bcb.gov.br/content/estabilidadefinanceira/spb_docs/RELATORIO_DE_VIGILANCIA_SPB2013.pdf. Acesso: 20.02.2022.
[12] Disponível em https://www.bcb.gov.br/content/estabilidadefinanceira/especialnor/Comunicado32927.pdf. Acesso: 20.02.2022.
[13] Disponível em https://www.bcb.gov.br/content/estabilidadefinanceira/especialnor/Comunicado32927.pdf. Acesso: 20.02.2022.
[14] Disponível em https://www.bcb.gov.br/pre/normativos/busca/downloadNormativo.asp?arquivo=/Lists/Normativos/Attachments/50926/C_Circ_4006_v1_O.pdf. Acesso: 20.02.2022.
[15] Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-bcb-n-1-de-12-de-agosto-de-2020-271965371. Acesso: 20.02.2022.
[16] Disponível em https://dados.gov.br/dataset/estatisticas-do-spi-sistema-de-pagamentos-instantaneos. Acesso: 20.02.2022.
[17] Disponível em https://febraban.org.br/noticia/3638/pt-br/. Acesso: 24.02.2022.

geométrica[18]. Registros de 2021[19] indicam que, somados, os canais digitais concentram ao redor de 70% de todas as transações realizadas, respondem por 80% dos pagamentos de contas e são instrumento para 90% de todo o volume de crédito contratado no Brasil. Nos EUA, fraudes e crimes vinculados a transações financeiras digitais apontam para aumento de 47% (2020)[20]; e na Europa o relatório *Financial Fraud in Digital Space*, elaborado pela Agência de Cibersegurança da União Europeia (2018)[21], indica um cenário de forte alta dos riscos e vulnerabilidades das transações eletrônicas.

Trecho do *white paper* preparado pelo ex-encarregado da Comissão de Segurança da União Europeia, publicado no *Global Engage*, comenta[22]:

> "A Era Digital chegou com um ritmo que poucos previam, ***trazendo novas ameaças e deixando muitos para trás em termos de conscientização e comportamento de segurança digital***. ***A segurança digital não pode ser obtida apenas por meio de legislação, mas requer envolvimento intenso e contínuo de toda a cadeia de valor digital, desde cidadãos e fornecedores digitais até corporações, agências de aplicação da lei e governos.*** Infelizmente ainda estamos atrasados.
>
> "Ainda estamos muito dispersos e descoordenados enquanto construímos muitos silos e implementamos muitos sabores locais diferentes. ***E por todas essas razões, os criminosos cibernéticos estão prosperando.***" (tradução livre) (destaques)[23].

Ainda que medidas de proteção e salvaguarda hajam sido postas em prática pelo Banco Central, exige-se maiores investimentos estratégicos com relação a "golpes" relacionados ao arranjo. Veículos de imprensa e publicações especializadas recentes trazem uma série de notícias sobre "fraudes" e outros crimes vinculados ao Pix, em regra atingindo pessoas físicas. "Cinco mil golpes digitais em um mês", diz uma das reportagens[24]; outra informa que "Pix é a preferência e golpes disparam"[25]; e uma terceira faz alusão ao número de "sequestros-relâmpago" ocorridos, visando a obter transferências via Pix por violência ou grave ameaça[26].

Por óbvio, atos criminosos não desqualificam uma boa iniciativa, e tampouco podem ser sempre explicados 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 *full fail safe* ainda não sejam possíveis, mas deve ser considerada a gravidade do quadro, com a adoção de medidas adicionais. É importante falar também, considerando esse cenário, em **educação digital**: de que maneira capacitar a população para lidar com os golpes de maneira mais

---

[18] Cf. SMITH, Russell. *Crime in the Digital Age*. [s. ed.], Londres: Taylor & Francis Ltd, [s. d.], pp. 54/55

[19] Cf. https://portal.febraban.org.br/noticia/3648/pt-br/. Acesso: 24.02.2022.

[20] Disponível em https://www.iii.org/fact-statistic/facts-statistics-identity-theft-and-cybercrime. Acesso: 24.02.2022.

[21] Disponível em https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/financial-fraud-in-the-digital-space. Acesso: 24.02.2022.

[22] Disponível em http://www.global-engage.com/life-science/cyber-crime-in-the-digital-age/. Acesso: 24.02.2022.

[23] Texto original: "The Digital Age has arrived with a tempo few had predicted, bringing new threats and leaving many behind in terms of digital security awareness and behavior. Digital security cannot be obtained through legislation alone but requires intense and continuous involvement by the entire digital value chain from citizens and digital suppliers to corporations, law enforcement agencies and governments. We are unfortunately still lagging behind. We are still too scattered and too uncoordinated while building too many silos and implementing too many different local flavors. And for all those reasons, cyber criminals are prospering."

[24] Disponível em https://exame.com/tecnologia/pix-vira-isca-e-criminosos-criam-mais-de-5-mil-golpes-digitais-em-um-mes/. Acesso: 24.02.2022.

[25] Disponível em https://www.istoedinheiro.com.br/pix-cresce-entre-transferencias-e-golpes-dsiparam-veja-6-dicas-para-nao-cair-em-nenhum-deles/. Acesso: 24.02.2022.

[26] Disponível em https://www.bbc.com/portuguese/brasil-58286706. Acesso: 24.02.2022.

informada? Como munir o cidadão de dados sobre o fato de que seus dados podem ser utilizados para fins escusos, e precisam ser protegidos pelas instituições que prestam serviços para eles?

Ademais, sugestões a serem consideradas incluem a reflexão sobre as fraudes *man in the middle*, que, embora mais sofisticadas, podem ser prevenidas por iniciativas de **instituidores** e **operadores** – o uso de protocolos de comunicação de alta segurança, o emprego de revisores de página de acesso e a aplicação de *mixer* de chaves pessoais[27] – e por cuidados básicos pelos **usuários**.[28]

No mais, de volta à questão sobre ***incidentes de segurança envolvendo dados pessoais*** de usuários do Pix, algumas preocupações adicionais merecem ser avaliadas.

Nesse espectro, o quadro pode ser ilustrado por meio de **dois grandes incidentes** que foram comunicados e noticiados:[29]

- O primeiro (**setembro, 2021**) levou ao "vazamento" de 414.526 chaves Pix que o Banco do Estado de Sergipe S. A. (Banese) guardava e armazenava[30]; e

- O segundo (**dezembro, 2021**) provocou o "vazamento" de 160.147 chaves Pix acauteladas na Acesso Soluções de Pagamento S.A.

O Banco Central, como lhe cabia, emitiu comunicações 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".

Vale sublinhar **três pontos de atenção**:

i) Pela natureza dos comunicados, o Banco Central não considerou que chaves Pix – foco do vazamento – ***são dados pessoais de primeiro grau***;

ii) O vazamento das chaves Pix ***também abriu portas para o vazamento de dados pessoais típicos***, como aqueles que compõem o cadastro dos usuários do arranjo; e

iii) O texto dos comunicados deixa entrever que o BC centrou sua preocupação, essencialmente, em "dados financeiros", inclusive os protegidos pelas normas de sigilo bancário, ***porém além deles, há dados pessoais típicos, que a legislação de proteção à privacidade e dados pessoais abrange e igualmente protege***.

---

[27] Cf. https://opensource.com/article/20/4/mitm-attacks. Acesso: 24.02.2022.

[28] Cf. https://www.itgovernance.eu/blog/en/how-to-defend-against-man-in-the-middle-attacks. Acesso: 24.02.2022.

[29] Foram noticiados outros vazamentos menores, como o vazamento recente de mais de 2.000 chaves de clientes da Logbank Soluções. No entanto, em virtude da quantidade de informações vazadas, focamos nos dois eventos maiores. Outras informações sobre o caso podem ser obtidas em: Pagamentoshttps://agenciabrasil.ebc.com.br/economia/noticia/2022-02/bc-comunica-vazamento-de-dados-de-21-mil-chaves-pix.

[30] A primeira comunicação feita pela instituição financeira dava conta de que o vazamento atingira 395.009 chaves Pix.

Foi, inclusive, instaurada investigação pela Secretaria Nacional do Consumidor (Senacon), que, entre outros elementos, requereu ao Banese[31]:

- As **ações adotadas para eliminar falhas na prestação do serviço**, com vistas à melhoria da segurança da privacidade dos dados.
- As categorias de **dados que teriam sido acessados**;
- As **medidas tomadas** para mitigar os efeitos do vazamento;
- Indicação de **quanto tempo** os dados ficaram expostos; e
- Reconhecimento de que os dados **vazaram de suas bases ou de base mantida por operadores que tratam dados mediante sua solicitação**.

Esse tipo de incidente de segurança preocupa operadores dos arranjos de pagamento mundo afora, pois envolve não somente **dados financeiros** dos usuários – os titulares – como também outros **dados pessoais** seus. Um vazamento de dados financeiros é um evento grave, com proporções desconhecidas e imensuráveis, já que expõe o indivíduo a riscos de toda ordem, sobre si e sobre seus recursos e patrimônio; para a instituição financeira, atrai descrédito e afeta a credibilidade; e para o instituidor do arranjo quase sempre significa colocar em xeque seus controles, processos e protocolos, com riscos sistêmicos de efeitos imponderáveis.

Mas, quando esse incidente envolve **dados pessoais** do usuário, tudo fica muito mais agravado, considerando que expõe a privacidade e demais direitos e garantias do titular, potencializando e multiplicando os riscos, e o coloca à mercê de um sem-número de fraudes, uso deturpado, chantagens ou, no mínimo, indevida publicidade de parte importante de seu patrimônio imaterial: a **intimidade**.

O vazamento de chaves Pix impacta os dados pessoais de cada um dos titulares atingidos, principalmente quando se sabe o que representa, de fato e na prática, a essência de uma chave Pix: dados pessoais, *coletados* pela instituição que faz a oferta do arranjo, e por ela *compartilhados* com variados agentes, inclusive com o instituidor. Além do mais, uma chave Pix não existe e tampouco subsiste **sem os dados pessoais do usuário que fizeram que seu cadastramento fosse possível**. E essa não é uma premissa funcional ou administrativa, mas meramente operacional, prevista pelo próprio Banco Central, que esclarece que o cadastramento da chave Pix depende da escolha de uma das *tags* possíveis: CPF (ou CNPJ), *e-mail*, número do telefone celular ou combinação aleatória[32].

As três primeiras *tags* são objetivamente **dados pessoais em sua essência**, e mesmo a quarta delas, uma vez gerada pelo usuário, também passa a integrar o rol de seus dados pessoais, tal como acontece com a chave Pix, uma vez definida sua criação. Ou seja: nesse contexto, há pelo menos **cinco dados pessoais** – as quatro *tags* e a chave Pix, que, embora seja, no fundo, uma das *tags*, atinge o *status* de dado pessoal assim que registrada.

---

[31] Cf. https://www.gov.br/mj/pt-br/assuntos/noticias/ministerio-da-justica-e-seguranca-publica-investiga-banco-banese-por-vazamento-de-dados-pessoais-de-consumidores. Acesso: 24.02.2022.

[32] Cf. https://www.bcb.gov.br/estabilidadefinanceira/perguntaserespostaspix#:~:text=O%20Pix%20pode%20ser%20realizado,conta%20para%20receber%20um%20Pix. Acesso: 24.02.2022.

Portanto, o incidente de segurança – por exemplo, um vazamento – que atinja a chave Pix, e mesmo que tão-somente ela, **é um incidente de segurança de dados pessoais**, cabendo assim ser considerado e tratado pelo instituidor do arranjo, por seu participante e pela entidade a quem cabe regular a proteção, segurança e privacidade dos dados pessoais e de seu titular[33].

É exatamente por isso que os riscos relacionados ao Pix e aos recentes vazamentos tanto preocupam, pelos seus perigos reais, latentes e potenciais para a privacidade e o direito à intimidade, tão caros à Constituição Federal.

Nesse sentido, é prudente demonstrar de que maneira tais eventos interagem com a **legislação de proteção aos dados pessoais de pessoas naturais**, e mais especialmente a Lei Geral de Proteção de Dados (LGPD), em vigor desde 2020 e com sanções aplicáveis desde agosto de 2021.

2. Parte B: Pix, Riscos, Vulnerabilidades e Interação com a LGPD

Como qualquer arranjo de pagamentos instantâneos, o Pix não está a salvo de eventos delituosos e atos negligentes[34], e por isso traz **riscos** e **vulnerabilidades inerentes** e **emergentes**.

Há dois focos de atenção nesse momento:

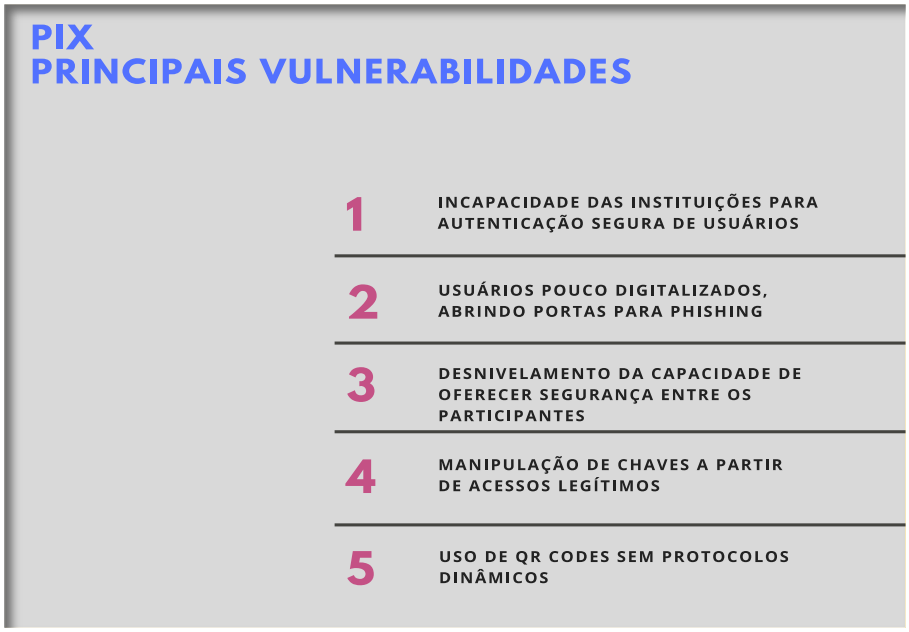
- **Riscos** do Pix:
  - Operacionais ("golpes" e outras ações ilegais); e
  - Incidentes de segurança envolvendo dados pessoais de usuários titulares.
- **Vulnerabilidades** do arranjo.

O problema fica ainda mais sério quando esses dois elementos interagem, produzindo um cenário de fragilidade do arranjo e potencial de exposição do usuário. Embora algumas *back doors*, brechas que permitem contornar a segurança de determinado sistema, do Pix sequer sejam conhecidas[35], outras, no entanto, já têm destaque, e a tecnologia produziu resposta para elas. Mas, se algumas dessas fragilidades simplesmente existem, isso já é motivo suficiente para que medidas sejam adotadas, ainda que em caráter preditivo, para proteger o usuário e o sistema. Mesmo se essas medidas mostrarem eficácia mitigada, só o fato de terem sido aplicadas demonstra o interesse dos agentes em aprimorar a segurança e a credibilidade das transações.

---

[33] Cf. https://www.cl.cam.ac.uk/~rja14/Papers/anderson-frb-kansas-mar27.pdf. Acesso: 24.02.2022.
[34] Cf. https://www.lexisnexis.com/risk/intl/pt/resources/whitepaper/Understanding-The-New-Payment-Methods-CSMB.pdf. Acesso: 24.02.2022.
[35] Cf. https://www.securityreport.com.br/destaques/alerta-de-fraude-febraban-destaca-principais-golpes-usando-o-pix/#.YfGFHfXMK3I. Acesso: 24.02.2022.

Entre essas fragilidades se destacam as seguintes:



Porém, há *outras vulnerabilidades*, consideradas nível "zero-zero", que delineiam cenário ainda mais complexo. Para isso, apresentamos o quadro abaixo:

É intuitivo afirmar que o arranjo Pix possui atrativos, como os já conhecidos velocidade de transferência, disponibilidade e preço (custo) por transação, notadamente quando comparado com as tarifas de TED e DOC. As instituições financeiras que aderem ao arranjo manuseiam técnicas de prevenção de fraudes, cujo principal – e mais complexo – desafio talvez seja descobrir não quando "golpes" vão acontecer, ou onde, mas ***como***. Mas, além disso, algumas técnicas, como as preditivas e de *over table*[36], são desafiadas a reduzir os "falsos positivos", aquelas transações não problemáticas bloqueadas pelo algoritmo por suspeita de fraude. Outro ponto é que o Pix foi

[36] Expressão, emprestada do mundo dos jogos, que significa a tentativa de descobrir, analisando as cartas abertas na mesa e aquelas que estão "acima da mesa" (não conhecidas), quais cartas, probabilisticamente, têm mais chances de chegar primeiro ao jogo.

pensado para possibilitar a entrada de número incerto (mas expressivo) de "provedores de serviço", quer para iniciar uma transação, quer para fornecer acesso à infraestrutura unificada do BCB, de forma que a liquidação LBTR[37] ocorra no SPI.

Observa-se que essas etapas e agentes apresentam tendência a vulnerar o processo em si e o sistema, afetando sua segurança e, em consequência, a privacidade de usuários. A falha em uma dessas etapas não atinge somente o processo de autenticação da transação, feita pelo Banco Central, mas toda a cadeia, acarretando instabilidade[38].

Outro ponto de vulnerabilidade no sistema encontra-se n***a plataforma única do BC***. Não se trata de discutir apenas a adoção de "base única", mas do fato de que eventual indisponibilidade do Pix – como ocorre em um evento de DDoS[39] –, em vez de prejudicar apenas usuários determinada instituição, afeta o serviço como um todo. Assim, um ataque de DDoS, por exemplo, pode permitir, via contaminação cruzada, a exposição da base de dados pessoais criada pelas instituições envolvidas, públicas e privadas, abrindo espaço para que *hackers* e *crackers* aproveitem a oportunidade para capturar ou sequestrar tais dados ou atingi-los de maneira que se tornem inservíveis.

Outro elemento consiste na questão de que o Banco Central é o **instituidor** do Pix (Resolução nº 1/20, arts. 1º, 90, §2º, inc. I, e 92, inc. IX) e tem também papel ***regulador*** *e* ***fiscalizador***, pois tem competência para disciplinar as **atividades econômicas**, em simetria com o Conselho Monetário Nacional (CF, arts. 173 e 174, e Lei nº 4.595/64, art. 9º). Isso implica que o BCB é, simultaneamente, *instituidor*, *regulador*, *normatizador* e *fiscalizador* do arranjo[40].

Esse "poder ramificado" (ou "desdobrado"), fruto da centralização adotada pela Constituição e "concentrado" na autarquia federal, traz dificuldades, e grande parte delas impacta não apenas no espaço do próprio BC, mas na confiabilidade do Pix e de todo o Sistema de Pagamentos Brasileiro (SPB) (Lei nº 12.865/13, art. 6º)[41], além de lançar sombras sobre a "higidez de princípios e propósitos" do Sistema Financeiro Nacional.

Em cenário diverso, o contento brasileiro traz exercício do poder ramificado-concentrado sobre o Pix, no qual as ações de controle cabem ao BCB, o que acaba desencadeando as dificuldades e problemas acima descritos, gerando a necessidade de correção de eventuais distorções nesse sentido.

O BCB assume, atualmente, "**três linhas de defesa**"[42] que as boas práticas recomendam para a gestão de riscos:

a) Primeira linha: pessoas que **gerenciam** e têm **propriedade** de riscos;

---

[37] Sigla para Liquidação pelo Valor Bruto em Tempo Real.
[38] Cf. https://efagundes.com/blog/potenciais-vulnerabilidades-ciberneticas-do-pix/. Acesso: 24.02.2022.
[39] Sigla para *Distributed Denial of Service*.
[40] V. Lei nº 12.865/13, Resolução CMN nº 4.282/13 e Resolução BCB n° 150/21.
[41] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12865.htm. Acesso: 24.02.2022.
[42] Sobre o modelo das "três linhas": https://na.theiia.org/translations/PublicDocuments/Three-Lines-Model-Updated-Portuguese.pdf. Acesso: 24.02.2022.

b) Segunda linha: pessoas que **supervisionam** riscos; e

c) Terceira linha: pessoas que **fornecem avaliações independentes**.

No caso do Banco Central, nele estão centralizadas esas três linhas de defesa, de maneira que, quanto ao Pix, ele é simultaneamente gerenciador, proprietário, supervisor e emissor de avaliação sobre seu comportamento e decisões. Essas três linhas atuam coordenadamente, e cada qual tem um papel definido: execução, supervisão e avaliação, que encontra obstáculos quando se concentram em um só agente.

Nota-se que, conforme o Decreto da Governança[43] – que se aplica às autarquias, como o BCB – (vide arts. 2º, inc. IV, 5º, inc. III, e 17) a implementação de uma governança de resultados, inclusive em sede de riscos e vulnerabilidades, é uma determinação legal, que também está na legislação que disciplina o Governo Digital[44].

Por esse motivo o TCU, no seu Referencial Básico de Governança, registra:

> "***A alta administração e as instâncias de governança têm a responsabilidade de prestar contas sobre o estabelecimento dos objetivos, a definição de estratégias para alcançar esses objetivos e o estabelecimento de estruturas de governança.*** *A instância máxima de governança e a alta administração têm a responsabilidade de, em conjunto, assegurar a existência, o monitoramento e a avaliação de um sistema efetivo de gestão de riscos e controle interno, bem como de utilizar as informações resultantes desse sistema para apoiar seus processos decisórios e gerenciar riscos estratégicos*." (destaques)[45].

Isso se relaciona com a implementação de mecanismos de ***governança responsável***, cuja missão é permitir que as três linhas de defesa sejam não apenas postas em prática, mas que, atuando em harmonia, não se sobrepujem entre si ou funcionem isoladamente.

Na governança responsável, a organização precisa avaliar suas dificuldades e limitações. E isso não significa declinar de competências. Ademais, *a avaliação externa apenas robustece as ações tomadas, assegura sua conformidade legal e ética, atrai confiabilidade para as instâncias decisórias e dá solidez isencional a suas orientações*.

Nesse rumo, toda "**boa governança pública alia o desempenho e a conformidade ao tomar e implementar decisões sustentáveis – estratégica, ética e legalmente adequadas**" (destaques)[46], o que importa dizer que a decisão sobre a governança no setor público (e no privado) deve ser pautada por seus efeitos no interesse público.

---

[43] Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2017/Decreto/D9203.htm. Acesso: 24.02.2022.
[44] Disponível em https://www.in.gov.br/en/web/dou/-/lei-n-14.129-de-29-de-marco-de-2021-311282132. Acesso: 24.02.2022.
[45] Disponível em https://portal.tcu.gov.br/data/files/FA/B6/EA/85/1CD4671023455957E18818A8/Referencial_basico_governanca_2_edicao.PDF. Acesso: 24.02.2022.
[46] Cf. https://repositorio.enap.gov.br/bitstream/1/4281/1/5_Livro_Governan%C3%A7a%20Gest%C3%A3o%20de%20Riscos%20e%20Integridade.pdf.

Com a **Lei Geral de Proteção de Dados**[47], segurança e privacidade ganharam outro viés, e muito mais relevância. A evolução legislativa e regulatória da proteção de dados pessoais no Brasil intensificou-se na primeira década do século e o país busca seguir as transformações jurídicas ocorridas em países como Estados Unidos e, principalmente, o compasso do contexto da União Europeia, mediante o advento do Regulamento Geral de Proteção de Dados Pessoais 2016/679 ("GDPR", *General Data Protection Regulation*).

Dentre as consequências impostas por esse cenário, vemos que o Brasil, além de se mostrar apto a garantir nível mínimo de conformidade com os padrões internacionalmente estabelecidos, pretende conquistar novos espaços de diálogo, como é o caso da participação do país na Organização para a Cooperação e Desenvolvimento Econômico (OCDE), que voltou a ser discutida em 2022. Um dos requisitos para a participação é, exatamente, o comprometimento com uma cultura de proteção de dados pessoais. Isso começa com a Administração Pública, como primeiro passo desse processo.

De volta ao vazamento de **chaves Pix**, é visível e latente que uma chave é um "apelido" que diz da existência da conta na base de contas de uma instituição financeira[48]. É por ela que o DCIT[49], local de armazenamento de informações e contas dos usuários, consegue saber quem transfere quantias e a quem as transfere. Fazendo referência à nossa atual legislação, qualquer informação "relacionada a pessoa natural identificada ou identificável" (art. 5º, I, da LGPD) é considerada dado pessoal.

A LGPD determina, em seu artigo 5º, II, que dado pessoal sensível é o "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural". Em sentido análogo e comparativo, a GDPR prevê, em seu artigo 1º, que o diploma trata da proteção de dados pessoais das pessoas singulares e que são dados pessoais as informações relativas a uma pessoa singular identificada ou identificável (artigo 4º).

Apesar de a lei ser omissa sobre a classificação de "dados financeiros de pessoas físicas" enquanto dados sensíveis, é claro o parágrafo 1º do artigo 11º (que cuida do tratamento de dados pessoais sensíveis) da LGPD quando dispõe que "§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais que revele dados pessoais sensíveis e que possa causar dano ao titular, ressalvado o disposto em legislação específica."

Em adição, o artigo 5º da Constituição Federal, em seu inciso X, estabelece que a intimidade e a vida privada são direitos invioláveis. Assim, o tratamento de dados financeiros de um indivíduo, quando feito de modo equivocado, pode ferir justamente esse direito fundamental. Toda movimentação financeira está vinculada a uma pessoa física, configurando dado pessoal. Esses dados ligam-se a um CPF, outro elemento identificador.

---

[47] Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso: 24.02.2022.
[48] Cf. https://www.bcb.gov.br/acessoinformacao/perguntasfrequentes-respostas/faq_pixpagtoinstantaneo. Acesso: 24.02.2022.
[49] Sigla para Diretório de Identificadores de Contas Transacionais.

Em suma, dados financeiros não apenas têm o viés de possibilitar a perfilização do titular de dados, mas o expõem, identificando-o como pessoa confiável ou não no setor financeiro. A mesma lógica é aplicável a dados financeiros revelados.

Relacionado a esse arcabouço, relevante mencionar dois motivos técnicos que esclarecem objetivamente o que há por trás de uma chave Pix (dados pessoais): essa chave é *representada* por um de quatro dados pessoais – três **típicos** (CPF, *e-mail* ou número do telefone celular) e um **atípico** (combinação alfanumérica aleatória); e, já que essa chave, uma vez criada e registrada, passa a se referir a uma pessoa natural, e somente a ela, assume o *status* de dado pessoal.

De conseguinte, *se há vazamento de chave Pix, há vazamento de dado pessoal*; trata-se de *incidente de segurança*.

O ponto, agora, está em saber **onde** esse incidente ocorre. Nos casos conhecidos, tanto o do Banese quanto o da Acesso, o Banco Central comunicou que a ocorrência de "falhas pontuais" nos controles internos das instituições financeiras teria sido a causa, e isso levaria a inferir que os incidentes – na percepção veiculada pelo BC – ocorreram **nas** instituições financeiras. Em razão disso, a **responsabilidade** pelos incidentes e medidas legais e administrativas necessárias caberia apenas às instituições. De outro modo: ao BC não caberia, quanto à proteção de dados pessoais, qualquer ação sobre os incidentes. Porém, isso implica compreender o papel do BC na cadeira de proteção de dados pessoais, por meio da qual o grau de responsabilidade varia de acordo com o poder de gestão, ou melhor, de decisão sobre o tratamento, afinal "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo" (art. 42).

Sob esse viés, cabe considerar que:

1. O Banco Central é o *instituidor*, *normatizador*, *fiscalizador* e *regulador* do arranjo Pix (Resolução nº 1/20, arts. 1º, 90, §2º, inc. I, e 92, inc. IX), atuando como figura central do SPB (Lei nº 12.865/13, art. 6º) e tem competência legal para *disciplinar* as práticas do Pix, exercendo *gestão* sobre as plataformas operacionais (infraestrutura)[50]. Só isso já demonstra que, entre o BC e os participantes do arranjo, há um estreito vínculo. Mais ainda: o Pix é um **sistema**, com **bases compartilhadas entre os agentes**, inclusive de dados pessoais, até porque, sem isso, não seria possível ao BC validar transações e operações dentro do arranjo. Isto é, o BC tem poder decisório quanto ao tratamento de dados pessoais no âmbito do arranjo. E aquele a quem competem as decisões referentes ao tratamento de dados pessoais é o agente controlador;

2. Com isso, Bacen e instituições financeiras são, ***controladoras*** de dados pessoais (LGPD, art. 5º, incs. VI e IX) nas atividades que realizam no âmbito do Pix e na medida que realizam escolhas sobre como e por quem o tratamento será realizado. E é assim porque lhes competem "**as decisões referentes ao tratamento de dados**

[50] Cf. https://www.bcb.gov.br/estabilidadefinanceira/papeldobcpix. Acesso: 24.02.2022.

pessoais" (destaques). Mas, já que estabelecem, entre si, no sistema Pix, os meios e as finalidades para tratamento de dados pessoais necessários ao arranjo. Em decorrência disso, se há incidente de segurança envolvendo os dados pessoais vinculados ou relacionados ao Pix, ambas as partes têm responsabilidade sobre o evento. Tanto que a LGPD prevê que o controlador (qualquer um, mesmo conjunto) precisa "*comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares*" (destaques) (art. 48);

3. Outro ponto a considerar é que, no âmbito do sistema Pix, o tratamento de dados pessoais tem uma mesma finalidade-base, quer para o BC, quer para as instituições que participam do arranjo (ainda que haja finalidades específicas para cada parte). Tanto que a ANPD, em documento publicado em 2021[51], diz exatamente isso;

4. O tratamento de dados pessoais no âmbito do Pix não é uma necessidade exclusiva das instituições participantes. Elas e o Banco Central, em alguma medida, têm que tratar esses dados para operacionalizar o arranjo, dar segurança às transações e ter meios de identificar possíveis fraudes ("golpes"). De alguma maneira, ambos tratam dados pessoais. Assim, ambos devem tomar as ações de segurança requeridas pela LGPD (art. 46, *caput*), sob pena de responsabilização (art. 44, par. ún.). Logo, se o BC é instituidor, normatizador, fiscalizador e regulador do arranjo, e se tem gestão sobre a infraestrutura operacional a ele necessária, ou não exigiu das instituições participantes aquelas ações, ou as exigiu, mas não fiscalizou suas implementação e eficácia, cabível sua responsabilização, na medida de seu papel para as consequências dos vazamentos;

5. Controladores, **em qualquer posição**, têm responsabilidade pelos riscos ou danos relevantes causados aos titulares (LGPD, art. 5º, inc. V). É o que estipula a LGPD (art. 42, *caput* e inc. II), estabelecendo, nessa hipótese, o conceito de "controlador diretamente envolvido no tratamento":

> "**O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.**
>
> "II – ***os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados*** **respondem solidariamente**, (...)." (destaques).

[51] Disponível em https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf.

6. A posição adotada pelo GDPR[52] é também essa. Seu Considerando 75 diz que pode o risco ou dano aos titulares de dados pessoais:

> "(...) *resultar de operações de tratamento de dados pessoais suscetíveis de causar danos físicos, materiais ou imateriais, em especial quando o tratamento possa dar origem à discriminação, à usurpação ou roubo da identidade, a perdas financeiras, prejuízos para a reputação, perdas de confidencialidade de dados pessoais protegidos por sigilo profissional,* (...), *ou a quaisquer outros prejuízos importantes* (...);" (destaques)[53];

7. No tratamento de dados pessoais do arranjo Pix – no que se refere à instituição normatização e fiscalização -, o Banco Central é nitidamente um "**controlador dominante**"[54], eis que lhe cabe papel destacado advindo de sua condição de instituidor. Nesse caso, sua responsabilidade sobre o tratamento dos dados, dentro de sua estrutura ou no âmbito das instituições participantes, é sempre proeminente. Por isso, tem ele o poder-dever de comunicar um vazamento ao órgão regulador de dados (ANPD). E não apenas por motivo de "transparência", como afirmado em notas públicas, **mas por obrigação legal** (LGPD, art. 48, *caput*). As notas não suprem a comunicação exigida pela LGPD, que, endereçada à autoridade de dados, deve conter os elementos nela previstos (art. 48, §1º);

8. Outro aspecto a ressaltar é que a ANPD, embora por meios informais, tomou conhecimento a respeito do incidente envolvendo a Acesso e ***ainda não instaurou o processo administrativo sancionador*** referido na Resolução nº 1/21[55], conquanto o tenha feito no caso do Banese[56]; e

9. O arranjo Pix em termos de garantias fundamentais, segurança, proteção à privacidade e operação assegurada, ainda precisa de adaptações. O Pix é um serviço (uma facilidade financeira) sob a tutela do Banco Central. Como serviço, formulado à base da Lei nº 10.214/03[57], esse arranjo e seus operadores (BCB e instituições financeiras) estão, nos casos de falha do serviço, sob o Código de Defesa do Consumidor (CDC)[58] (art. 14) (texto repetido pela LGPD – arts. 42, *caput*, e 43). Assim, também sob a ótica do usuário-consumidor do Pix, há clara responsabilidade do BC e das participantes[59].

---

[52] Sigla para General Data Protection Regulation, aprovado pela Regulação europeia nº 2016/679, disponível em https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[53] Texto original: "The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to physical, material or non-material damage, in particular: where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage; where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;".

[54] A expressão se refere ao controlador que, mesmo numa relação conjunta com outro controlador, tem, seja pela natureza da finalidade do tratamento, seja pela especificidade do ambiente em que o tratamento ocorre, seja por uma posição decisória superior, exerce papel preponderante nas ações e decisões relacionadas ao tratamento dos dados pessoais.

[55] Disponível em https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-1-de-28-de-outubro-de-2021-355817513. Acesso: 20.02.2022.

[56] Vj. o comunicado do Banese ao mercado em https://ri.banese.com.br/noticia/banese-comunicado-ao-mercado-15/. Acesso: 20.02.2022.

[57] Disponível em http://www.planalto.gov.br/ccivil_03/leis/leis_2001/l10214.htm. Acesso: 20.02.2022.

[58] Disponível em http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso: 20.02.2022.

[59] STJ, AgInt no AREsp 1173934, disponível em https://scon.stj.jus.br/SCON/jurisprudencia/doc.jsp?livre=%22FALHA+DE+SERVICO%22+BANCO&b=ACOR&p=false&l=10&i=1&operador=e&tipo_visualizacao=RESUMO. Acesso: 20.02.2022.

3. Parte C: Conclusões

Nossa entidade, subscritora deste arrazoado, espera ter demonstrado a V. Sas., sempre com o legítimo interesse dos cidadãos e consumidores à frente, que os dois **incidentes de segurança** até agora noticiados (Banese e Acesso) são fatos de extrema gravidade, comprometem a credibilidade e a confiabilidade do arranjo Pix e colocam em xeque uma posição delicada, segundo a qual vazamentos como tais devem ser tratados no âmbito das instituições financeiras, apenas, sem envolvimento direto do Banco Central.

E assim porque:

a) O Pix, a despeito de sua modernidade conceitual, traz riscos e vulnerabilidades de toda natureza, e o número de "golpes" (ou fraudes) e de eventos delituosos outros que aumentam dia a dia, expondo o usuário a uma enorme variedade de perigos, *sem que, até agora, salvo medidas de ajuste operacional, ações materiais hajam sido postas em prática pelo instituidor*;

b) Esses riscos e vulnerabilidades – inerentes ou emergentes – ***entram em confronto com direitos e garantias individuais e coletivos do cidadão***, como a salvaguarda à intimidade, constitucionalmente assegurada;

c) Como instituidor, normatizador, fiscalizador e regulador do arranjo, é do **interesse** e **responsabilidade** do BC qualquer evento – inclusive e principalmente evento negativo, como um episódio de vazamento de dados – havido no âmbito do sistema Pix;

d) Exercente de posição dominante e impositiva nos arranjos de pagamento, o Bacen concentra em si funções que, conceitualmente, se opõem, o que *diverge das regras e boas práticas de governança no setor público, em contrariedade às normas legais previstas para a administração federal e se opõe aos princípios e diretivas do BIS*;

e) O Banco Central, por ter criado uma estrutura em que nele próprio se acumulam papéis de instituidor, normatizador, fiscalizador e regulador do Pix, na falta de órgão com ***atribuição legal ou atuação operacional que fiscalize suas ações no arranjo, deve regular e fiscalizar suas práticas***;

f) Faz-se imperativa e imediata a necessidade de adoção de sistemáticas de controle e gerenciamento de riscos e vulnerabilidades relacionadas ao Pix;

g) Chaves Pix **são, por definição legal, dados pessoais**, eis que dependem de dados pessoais (CPF, *e-mail*, número de telefone celular) para seu registro, e ainda, mesmo que constituídas por uma combinação aleatória, podem identificar ou fazer identificável o usuário titulares de dados, sendo assim salvaguardadas pela Lei Geral de Proteção de Dados;

h) O Banco Central e as instituições financeiras participantes do Pix são **controladores** de dados pessoais no âmbito das atividades que realizam, sob a LGPD, e por isso têm as obrigações e responsabilidades nela previstas, inclusive no caso de incidente de segurança;

i) No sistema Pix, o tratamento de dados pessoais tem uma mesma finalidade-base, para o BC e para as instituições que dele participam, embora em certos casos possa haver finalidade específica para cada parte;

j) Incidentes de segurança envolvendo dados pessoais, que acarretem riscos ou danos relevantes ao titular, levam os controladores envolvidos a responder por eles em caráter *solidário* (LGPD, art. 42, *caput* e inc. II; Cód. Civil, art. 264[60]);

k) Vazamento de dados pessoais **exige comunicação formal** à ANPD *por ambos os controladores diretamente envolvidos no tratamento*, e por isso BCB e instituições devem dar a conhecer tais eventos àquela Autoridade, visto que nota pública[61] **não** substitui o comunicado exigido pela LGPD, que, além de ser dirigido à ANPD, precisa conter os elementos nela previstos (art. 48, §1º);

l) No tratamento de dados pessoais do arranjo Pix, no caso da instituição, normatização, fiscalização e regulação, o Banco Central é nitidamente um "**controlador dominante**", pois lhe cabe um papel destacado. Nesse caso, sua responsabilidade sobre o tratamento dos dados, dentro de sua estrutura ou no âmbito das instituições participantes, é sempre proeminente. Por isso, tem ele o poder-dever de comunicar qualquer tipo de vazamento ao órgão regulador (não apenas em prol do princípio da "transparência", mas por obrigação legal);

m) Quanto à ANPD – que, embora de modo não formal, tomou bom conhecimento do incidente envolvendo a Acesso –, ***ainda não instaurou processo administrativo sancionador*** (Resolução nº 1/21), conquanto o tenha feito no caso do Banese;

n) Uma vez que o Bacen é "*controlador diretamente envolvido no tratamento*" de que resultou o vazamento, cabe à ANPD oficiar-lhe, solicitando dele as informações, explicações e providências sobre o incidente, dada sua **corresponsabilidade**; e

o) Tanto o BC quanto as instituições financeiras envolvidas nos vazamentos de dados pessoais de usuários respondem, sob o CDC (art. 14), por **falha do serviço**, ou por **falha na prestação do serviço**.

---

[60] Disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso: 24.02.2022.
[61] Cf. https://www.bcb.gov.br/detalhenoticia/17523/nota. Acesso: 24.02.2022.

4. Parte D: Medidas Necessárias

Com o exposto, e acreditando ter demonstrado a gravidade dos incidentes de segurança envolvendo dados pessoais e a incidência da LGPD, sugerimos a seguir medidas a serem adotadas, levando em consideração a proteção dos direitos e garantias fundamentais dos titulares de dados envolvidos, assim como a própria credibilidade dos organismos envolvidos e em respeito aos princípios de prestação de contas, isenção pública, legalidade, publicidade e governança do setor público:

1. **Comunicação formal** do BC à ANPD sobre os vazamentos de chaves Pix havidos no Banese e na Acesso, com os elementos referidos na LGPD (art. 48, §1º);

2. **Instauração**, pelo BCB, de processo administrativo interno para apurar não apenas 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;

3. **Adoção**, pelo BC, de processos e procedimentos para que se evite, quanto possível, a concentração de competências que afete as boas práticas de governança;

4. **Implementação**, por parte do Banco Central, de mais medidas de segurança para usuários do Pix e para o arranjo em si, de forma que riscos sejam prevenidos e seus efeitos, mitigados;

5. **Implementação**, pelo BC, de mecanismos de controle isento e independente, com emprego de governanças ativa e de resultados, em relação ao tratamento de dados pessoais no arranjo do Pix e nas transações relacionadas;

6. **Aplicação**, pelo BCB, de ações e medidas de controle e gestão para tratamento de dados pessoais no sistema do Pix;

7. **Instauração**, pela ANPD, processo administrativo sancionador, cobrindo os dois incidentes de segurança ocorridos e alcançando o Banco Central e as instituições relacionadas aos vazamentos.

_____

Fernando Cardozo Fernandes Rei
Diretor Executivo