A NOVA ERA DIGITAL E OS GOLPES DIGITAIS
THE NEW DIGITAL ERA AND DIGITAL SCAMS

ATALA CORREIA[1]
DOUGLAS CAMARINHA GONZALES[2]
FABRICIO MURARO[3]

Resumo

O artigo tem como objetivo explicitar os principais casos de fraudes ocorridas por meio de aplicativos digitais e de pagamento. Busca-se compreender a lógica dos deveres contratuais entre as partes envolvidas, bem como a noção de *compliance* dos aplicativos financeiros diante das obrigações previstas na legislação consumerista, bancária e de proteção de dados. A partir da análise dos principais casos, conclui-se que a aferição da responsabilidade está diretamente relacionada à conduta do correntista e ao grau de sofisticação do golpe, que se vale da tecnologia digital. Essa análise é essencial para verificar se o atual estado da técnica está em conformidade com o entendimento consolidado no Tema 331 da TNU.

Abstract

This article aims to outline the main cases of fraud committed through digital and payment applications. It seeks to understand the logic behind the contractual duties between the involved parties, as well as the concept of compliance within financial applications considering consumer, banking, and data protection legislation. Based on the analysis of key cases, it is concluded that the assessment of liability is directly related to the account holder's conduct and the level of sophistication of the scam, which leverages digital technology. This analysis is essential to determine whether the current state of the art aligns with the understanding established in Theme 331 of the TNU (National Uniformization Panel of Federal Special Courts).

1 Juiz de Direito do Tribunal de Justiça do Distrito Federal. Doutor em Direito Civil pela USP. Professor de Direito Civil pelo IDP – Brasília.

2 Juiz Federal do Tribunal Regional Federal da 3ª Região (SP e MS). Doutor em Direito Econômico e Mestre em Direito do Estado pela Faculdade de Direito da USP. Professor Adjunto da FAAP.

3 Doutor em Direito Econômico pela USP. Professor de Direito Constitucional em Três Lagoas.

Palavras-chave: Responsabilidade aplicativos digitais; fraudes digitais; plataformas digitais golpes.

Keywords: Liability in digital applications; digital fraud; scams on digital platforms.

1_ INTRODUÇÃO

A debutagem do sec. XXI inicia-se repleto de transformações, cujo marco comum é a difusão da tecnologia digital sobre as diferentes interações humanas de produção, expressão social, relacionamento, divisão de trabalho, de controle político e por consequência, de regramento jurídico-social.

As forças das plataformas digitais repercutem, pois, muito além da seara técnica da informática, mas para toda a sociedade, até como forma de moldar a opinião pública e, ainda, comportamentos sociais. Dentre as preocupações atuais, a mais eloquente é a segurança das transações bancárias – mediante tecnologia que confira proteção e segurança ao patrimônio e aos dados dos usuários.

Malgrado os bons avanços de comunicação social e a difusão pluralista de vozes nas redes sociais, o lado B dessas mudanças veio acompanhado de crimes digitais de toda ordem, quer no Brasil, quer no estrangeiro – um reflexo do atual estágio de civilização que ainda carece de predicados éticos fundamentais.

As experiências recentes nos assustam com *e-mails,* ligações, mensagens, *spams* e até um esquema orquestrado de quadrilhas digitais especializadas em golpes e estelionatos nos aplicativos bancários, ao colocar o cidadão comum, em especial os vulneráveis na mira dos golpistas. Recebemos todas as semanas um *fishing* (mensagem suspeita) como armadilha ao correntista ou ao próprio contribuinte para pagar uma conta inexistente ou fraudada, bem como diversas ligações telefônicas de quadrilhas especializadas, muitas das vezes com o número explicitado do próprio banco do correntista em seu celular.

Nesse contexto, esse artigo busca algumas reflexões jurídicas a respeito do alcance desses golpes aos correntistas e a responsabilidade desse e das instituições, como o próprio Caixa 24 horas (ao não impedir a proteção de dados) ou até as empresas de pagamento ou telefonia que conferem um tratamento tecnológico factível ao engodo, ao não impedir o uso dos números de telefonia dos bancos por parte dos estelionatários.

Dona Maria recebe um telefonema, cujo identificador de chamada aponta (fraudulentamente) ser da gerência do seu banco, oportunidade em que é alertada

sobre uma suspeita de golpe em seu cartão de crédito – a compra de uma geladeira. Sob violenta emoção, segue à risca todas as instruções do locutor que pede a ela para confirmar ou não a compra - ao contestar a compra, uma máquina de voz se apresenta para solicitar sua senha: ingenuamente a protagonista digita ao telefone sua senha bancária, cujos dados são angariados por um maquinário eletrônico, vulgo "chupa-cabra".

Dos golpes mais triviais e ingênuos, é o conhecido "Golpe do Motoboy", onde a mesma história se repete, mas o correntista deve escrever uma carta ao Banco com sua senha e entregá-la juntamente com o cartão bancário cortado ao meio a um entregador, "o motoboy" que efetivamente busca o "brinde" na casa do correntista.

Outro exemplo mais eloquente é o envio de uma conta de um colégio ou uma prestadora de serviços, oportunidade em que o interessado paga a fraudulenta conta, ao passo que o beneficiário é outro, um laranja do fraudador.

Tais engrenagens criminosas desafiam os gestores de bancos e as autoridades protetoras dos consumidores, cujas ferramentas jurídicas devem perpassar por crivos tecnológicos apurados para afastar as fraudes – mediante o uso de diversas técnicas como a dupla chave eletrônica; o *token* de identificação; o envio de código ao celular ou *email* do correntista; ou até mesmo, a necessidade de comparecimento pessoal do correntista ao próprio banco ou ao INSS.

O cerco aos fraudadores chega às raias das plataformas digitais que intermedeiam situações eloquentes de fraudes, já que a *compliance* dessas deve fazer um mínimo escrutínio a respeito da identidade, *ranking* de segurança ou dados bancários, como uma mínima prestação de contas – de sorte que a jurisprudência atual é um ensaio de experiência para aferir as responsabilidades dos intermediários que fraquejam com a segurança de suas publicidades e aplicativos – comportamento muitas vezes tido como abusivos, situação que engendra corresponsabilidade desses intermediários (até plataformas de pagamento).

Como é sabido, a mentalidade criativa da criminalidade é surpreendente e os golpes são praticados muitas vezes sob o manto da ingenuidade colaborativa dos correntistas, como nos dois exemplos acima, *modus operandi* particularmente sensível aos idosos e vulneráveis, assim qualificados juridicamente.

Justamente nessa tênue linha da colaboração ingênua dos correntistas e da tecnologia defasada ou inapropriada aplicativos (APPs) digitais bancários divisa-se refinada reflexão sobre a responsabilidade civil das instituições bancárias ou a culpa exclusiva do terceiro golpista; ou até mesmo, a culpa concorrente de ambos.

Em juízo delibativo, aplica-se a máxima popular: "nem tanto à terra, nem tanto ao mar"; isso é, tanto o correntista como as instituições financeiras têm deveres e

responsabilidade direto e colaterais para evitar as fraudes e golpes digitais: o primeiro assume obrigação contratual de não entregar o seu cartão e senha a terceiros; ao passo que as instituições devem zelar pela segurança eletrônica de seus aplicativos e respectivos dados bancários de seus correntistas; além de manter hígido e seguro o aplicativo digital para não permitir a quebra de seu círculo de segurança ou funcionalidade.

Como é sabido, tanto o correntista como as instituições financeiras têm deveres contratuais e, por consequência, responsabilidades diretas de seu agir para prevenir fraudes e golpes digitais: o primeiro detém dever de sigilo sob sua senha e utilização personalíssima de seu cartão – obrigação de não fornecê-los a terceiros; ao passo que as instituições devem zelar efetivamente pelo sigilo dos dados bancários de seus correntistas e sobretudo de manter um aplicativo digital eficiente e blindado à intervenção de *hackeamento,* justamente para impedir fraudes de todo gênero.

Assim, em casos correlatos de demandas indenizatórias advindas de fraudes bancárias, o juiz da causa afere o teor do engodo promovido por terceiros que maliciosamente ludibriam o correntista, bem como em que medida a tecnologia facilitou o estelionato, ou até deixara de impedir seu rastreio ou de outro modo não se utilizara de medidas tecnológicas de segurança viáveis atualmente.

Nesse passo, deve-se logo perquirir se o correntista agiu deliberadamente contra seu compromisso contratual de sigilo de senha e uso privativo do cartão ou não; se houve falibilidade de segurança no aplicativo eletrônico da instituição financeira ao não engendrar fases apropriadas de segurança e checagem de credenciamento de novos dispositivos, entre outras gestões de combate à fraude e ao estelionato.

Caso categórico a falha contratual do correntista, ao fornecer seu cartão e senha a terceiro, reconhece-se sua exclusiva culpa, consoante julgado repetitivo do STJ, o RESp n. 1.633.785/SP, da Terceira Turma do Superior Tribunal de Justiça. Já se a fraude fora consumada, em face de falha tecnológica do aplicativo que facilmente habilitou outro dispositivo, até por meio de telefonema de terceiro, resta factível o reconhecimento de *compliance* não seguida pela instituição financeira, quer nas transações comuns, quer por meio do PIX, sobretudo mediante o uso de novo aparelho não habilitado anteriormente no sistema.

A aplicação do direito segundo a premissa do cuidado e da gestão do risco pelas partes é um mecanismo jurídico proporcional às expectativas das partes e da legislação, seguindo pelo posicionamento reiterado de julgados na Justiça Federal, firmados em sede de recurso representativo de controvérsia, através do Tema n. 331 da TNU – Turma Nacional de Uniformização dos Juizados Especiais Federais, cuja semântica do enunciado retrata essa correlação de responsabilidades dos envolvidos:

> 1. O uso indevido de cartão de débito ou crédito por terceiro, mediante fraude, constitui, em regra, fortuito interno para os fins da Súmula 479/STJ, salvo se comprovada culpa exclusiva do consumidor ou de terceiro (art. 14, § 3º, inciso II, do Código de Defesa do Consumidor). 2. Em princípio, a realização de operação com o uso de cartão e senha descaracteriza a responsabilidade do banco por configurar quebra do dever contratual de cuidado do cliente. 3. Todavia, não se configura a excludente de responsabilidade se, independentemente de prévia comunicação da ocorrência pelo titular do cartão, (i) as circunstâncias em que as operações foram realizadas e o perfil do consumidor revelarem fortes indícios de fraude detectáveis pelo banco; ou (ii) não restar claramente demonstrado o descumprimento consciente, pelo consumidor, do dever contratual de cuidado no uso do cartão, seja em razão do grau de sofisticação dos meios de engenharia social empregados pelos fraudadores, seja pela condição de hipervulnerabilidade da vítima.

Geralmente, a corresponsabilidade da instituição financeira advém da má gestão tecnológica ao não gerir ou prevenir a fraude; ou ainda ao impedir o estorno bancário, quando munida de documentação apropriada, oportunidade em que deixara de agir de modo regulamentar, a teor da RESOLUÇÃO N. 147/2021 do BACEN:

> "Art. 32. V - **responsabilizar-se por fraudes no âmbito do Pix decorrentes de falhas nos seus mecanismos de gerenciamento de riscos**, compreendendo a inobservância de medidas de gestão de risco definidas neste Regulamento e em dispositivos normativos complementares;

A *vexata quaestio* dos casos buscam, pois, aferir se o sistema de *compliance* das instituições financeiras poderiam impedir a ocorrência do evento, ao conferir tratamento de falta de segurança na prevenção e combate às fraudes. Nessa vertente, surgem duas questões para fazer frente às disposições legais referentes à responsabilidade e contenção de risco: i) houve por parte da instituição financeira desrespeito às disposições de segurança de dados pela Lei Geral de Proteção de Dados; ii) o cometimento de fraudes realizado pelos criminosos, poderia ser evitado ou até sido limitado, a teor da legislação e tecnologia atual por parte das instituições financeiras.

As respostas dessas indagações aferirão a responsabilidade conjunta ou não das partes, frente à análise do risco para facilitação ou não da fraude em apreço, fiel às disposições legais e o atual estado da técnica da tecnologia antifraudes.

Caso as respostas sejam positivas, em geral há corresponsabilidade da instituição financeira, quer do ponto de vista da legislação do consumidor, quer do ponto de vista da Lei Geral de Proteção de Dados – LGPD, as quais obrigam expressamente os fornecedores de um lado, bem como o controlador e o fornecedor pela segurança e higidez de seus serviços e operações. Vale, pois, explicitar a legislação citada com seus contornos e peculiaridades próprios ao caso de fraudes.

Quanto à legislação consumerista, a Lei 8.078/90 já há muito disciplina a situação de solidariedade entre aqueles que prestam o serviço, através de terceiros, vinculando esse último, quando comercializa o serviço em sua plataforma. Vejam as disposições legais:

> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
>
> § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
>
> § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.
>
> *(...)*
>
> *Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.*
>
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
>
> I - *o modo de seu fornecimento;*
>
> ***II - o resultado e os riscos que razoavelmente dele se esperam;***
>
> *(...)*
>
> *Art. 25. É vedada a estipulação contratual de cláusula que impossibilite, exonere ou atenue a obrigação de indenizar prevista nesta e nas seções anteriores.*
>
> § 1° Havendo mais de um responsável pela causação do dano,

todos responderão solidariamente pela reparação prevista nesta e nas seções anteriores.

Ora, como já esclarecido pela moderna legislação do consumidor, o reconhecimento de fornecedor engloba o prestador de serviço intermediário, quer ele represente ou não os serviços originários, já que a fraude geralmente é consumada pela desídia no congelamento dos valores angariados pelo esquema criminoso, quando essas são devidamente instadas com documentos críveis para tanto.

Por sua vez, a própria Resolução 147 do BACEN vincula a empresa que operacionaliza os valores do PIX de gerir mecanismos de devolução em caso de fraude, a teor dos artigos seguintes:

"Art. 39-B. **Os recursos oriundos de uma transação no âmbito do Pix deverão ser bloqueados cautelarmente pelo participante prestador de serviço de pagamento do usuário recebedor quando houver suspeita de fraude**.

§ 1º A avaliação de suspeita de fraude deve incluir:

I - a quantidade de notificações de infração vinculadas ao usuário recebedor, à sua chave Pix e ao número da sua conta transacional;

II - o tempo decorrido desde a abertura da conta transacional pelo usuário recebedor;

III - o horário e o dia da realização da transação;

IV - o perfil do usuário pagador, inclusive em relação à recorrência de transações entre os usuários; e

V - outros fatores, a critério de cada participante.

§ 2º O bloqueio cautelar deve ser efetivado simultaneamente ao crédito na conta transacional do usuário recebedor.

§ 3º O participante prestador de serviço de pagamento deverá comunicar imediatamente ao usuário recebedor a efetivação do bloqueio cautelar.

§ 4º O bloqueio cautelar durará no máximo 72 horas.

§ 5º Durante **o período em que os recursos estiverem bloqueados cautelarmente, o participante prestador de serviço de pagamento do usuário recebedor deve avaliar se existem indícios que confiram embasamento à suspeita de fraude.**

§ 6º Concluída a avaliação de que trata o § 5º:

> **I - os recursos serão devolvidos ao usuário pagador, nos termos do Mecanismo Especial de Devolução, de que trata a Seção II do Capítulo XI, caso se identifique fundada suspeita de fraude na transação; ou**
>
> II - cessará imediatamente o bloqueio cautelar dos recursos, comunicando-se prontamente o usuário recebedor, nas hipóteses em que não forem identificados indícios de fraude na transação.

Categórico, pois, o dever de cuidado e gestão das instituições financeiras, bem como as empresas correlatas - como o Caixa 24 horas ou até empresas intermediárias de pagamento[4] – os quais devem também prevenir fraudes, bem como instituir mecanismos operacionais e tecnológicos que impeçam a consumação desses delitos – ou até a restituição monetária de valores injustamente surrupiados dos correntistas.

> Ademais, a própria LGPD reitera essas ordens de dever de cuidado:
>
> *Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.*
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.
>
> *Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.*

4 Vide Autos n. **0012320-25.2021.4.03.6306, Acórdão proferido aos 15.08.2023, pela 7ª TR dos JEF de SP, publicado no DJe 25.08.2023.**

Deveras, somente mediante a análise do caso concreto e o comportamento displicente do correntista, em cotejo com a tecnologia de segurança dos aplicativos, ter-se-á condições para aferir as circunstâncias e as providências que as partes tomaram tecnológica e operacionalmente, se em compasso às premissas de boa governança em segurança financeira, *compliance*, deveres antifraude da instituição financeira[5] – como as devidas comunicações de duas fases e os alertas de operação necessários à segurança dos consumidores.

Ademais, como é sabido, o juiz deve interpretar o Direito à luz dos fins sociais e das exigência do bem comum (art. 4º LINDB), pois diversas transações bancárias exigem ativação ou limite diário, bem como avisos circunstanciais, em face das diversas fraudes que assolam a população brasileira, de sorte que a instituição financeira e os demais operadores bancários (intermediadora de pagamentos), pois têm o dever de zelo e cuidado para impedir e afastar a fraude, sobretudo impedindo sua ocorrência e efeitos continuado.

Somente através desses critérios técnicos e operacionais, o juiz da causa terá panorama processual para aferir a gestão de risco das partes, para melhor aferir a corresponsabilidade das partes e a própria relação de causalidade de toda cadeia de eventos - em face da corresponsabilidade da instituição financeira para operacionalizar sistemas antifraude, com cautelas e alertas de operações ostensivamente atípicas e em série.

A síntese conclusiva é que a aferição da culpa das partes passará necessariamente por um crivo fático e valorativo, à luz das circunstâncias operacionais do aplicativo digital do bancário em xeque com sua operabilidade de segurança, além das provas de vazamento bancário para estabelecer a responsabilidade civil das partes.

A explicitação do contexto fático é de tamanha relevância que a 3ª Turma do STJ[6] decidiu, por apertada maioria (3X2), ainda em março de 2025 que o banco não é responsável pela fraude caso a correntista instale aplicativo em seu celular que facilite o acesso aos dados bancários e facilita a fraude. Nas palavras do Relator[7]:

5 BRASIL. Justiça Federal. Turmas Recursais dos JEF de SP. Recurso Inominado n. 5000137-03.2023.4.03.6132. Relator: Juiz Federal Douglas Camarinha Gonzales, Julgamento: 28 ago. 2024. Órgão Julgador: Sétima Turma Recursal, v.u.. Publicação: DJe. 06 set 2024.

6 https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202402422302&totalRegistrosPorPagina=40&aplicacao=processos.ea

7 https://www.migalhas.com.br/quentes/426062/stj-banco-nao-responde-por-golpe-do-motoboy-contra-vitima-com-cancer

> *"Certo é que a autora foi ludibriada a fornecer o acesso aos seus dados pessoais e bancários e, por meio da instalação do aplicativo AnyDesk em seu computador, permitiu acesso remoto a ele e possibilitou aos fraudadores a realização de diversas transações bancárias, inclusive em outra instituição".*

Em casos como tais, **não é raro o reconhecimento de culpa recíproca de ambas as partes**: onde de um lado reconhece-se ilícito ao correntista de conferir seus dados bancários sensíveis; de outro, a facilitação de operações por terceiros fraudada em nome de terceiros, que atuam através de empresas de pagamentos, as quais fraquejam a segurança de identidade desses e do próprio manejo de contas correntes, tidas como abusivas ou fantasmas – utilizadas em série pelos fraudadores, em que pese vastas reclamações das respectivas contas.

2_ REFERÊNCIAS BIBLIOGRÁFICAS

BLUM, Rita Peixoto Ferreira. *O direito à privacidade e à proteção de dados do consumidor.* São Paulo: Almedina, 2018.

BRASIL. Justiça Federal. Turmas Recursais dos JEF de SP. *Recurso Inominado n. 5004247-09.2022.403.6317.* Relator: Juiz Federal Douglas Camarinha Gonzales, Julgamento: 26 nov. 2024. Órgão Julgador: Sétima Turma Recursal, v.u.. Publicação: DJe. 04 dez 2024.

BRASIL. Justiça Federal. Turmas Recursais dos JEF de SP. *Recurso Inominado n.* **0012320-25.2021.4.03.6306**. Relator: Juiz Federal Douglas Camarinha Gonzales, Julgamento: 15 ago. 2024. Órgão Julgador: Sétima Turma Recursal, v.u.. Publicação: DJe. 24 ago 2024.

DE LUCCA, Newton. A proteção dos consumidores no âmbito da internet. In: LIMA, Cíntia Rosa Pereira de; NUNES, Lydia Neves Bastos Telles (Coord.). Estudos avançados de direito digital. Rio de Janeiro: Elsevier, 2014.

GONZALES, Douglas Camarinha. Plataformas digitais e discriminação por preços e dados. Tese de Doutorado, Departamento de Direito Econômico da FADUSP, São Paulo, 2024.

GONZALES, Douglas Camarinha; FAIAD, L'Inti Ali Miranda Novas Tecnologias e controle social, ***In*** Direitos fundamentais em processo: estudos em comemoração aos 20 anos da Escola Superior do Ministério Público da União / organizadores: Gonet Branco et al.- Brasília : ESMPU, 2020, p. 117.

GRAU, Eros Roberto. *A Ordem Econômica na Constituição de 1988* (Interpretação e Crítica). 19. ed. São Paulo: Revista dos Tribunais, 2018.

GRAU, Eros Roberto. *Por que tenho medo dos juízes:* a interpretação/aplicação do direito e os princípios. São Paulo: Malheiros, 2013.

TARTUCE, Flávio. A "Lei da Liberdade Econômcia" (Lei n. 13.874/2019) e as principais mudanças no âmbito do Direito Contratual. *Revista Jurídica Luso-Brasileira*, v. 6, n. 1, p. 1005-1020, 2020.

THAMAY, Rennan; GARCIA JUNIOR, Vanderlei; QUEIROZ, Paulo Victor Oliveira; SILVA, Giselly. *A função Social do Contrato* – Atualizado de acordo com a Lei da Liberdade Econômica e o Regime Emergencial. São Paulo: Almedina, 2021