RECURSO ESPECIAL Nº 2250674 - MG(2025/0493227-8)

RELATOR	**:**	**MINISTRO RICARDO VILLAS BÔAS CUEVA**
RECORRENTE	:	EMÍLIO ANTÔNIO QUEIRÓZ MURTA
ADVOGADO	:	EMÍLIO ANTÔNIO QUEIRÓZ MURTA (EM CAUSA PRÓPRIA) - RJ115207
RECORRIDO	:	NVIO BRASIL BITSO INSTITUICAO DE PAGAMENTO LTDA
ADVOGADOS	:	FRANCISCO KASCHNY BASTIAN - SP306020 GUILHERME KASCHNY BASTIAN - SP266795

EMENTA

RECURSO ESPECIAL. PROCESSUAL CIVIL. DIREITO DO CONSUMIDOR. AÇÃO INDENIZATÓRIA. NEGATIVA DE PRESTAÇÃO JURISDICIONAL. NÃO OCORRÊNCIA. SOCIEDADES PRESTADORAS DE SERVIÇOS DE ATIVOS VIRTUAIS (SPSAVs). CÓDIGO DE DEFESA DO CONSUMIDOR. APLICABILIDADE. FRAUDE EM TRANSAÇÕES COM CRIPTOATIVOS. RESPONSABILIDADE OBJETIVA. PRESTAÇÃO DE SERVIÇO. DEFEITO. NÃO COMPROVAÇÃO.

1. A controvérsia dos autos resume-se a saber: a) se houve negativa de prestação jurisdicional; b) se incide o Código de Defesa do Consumidor nas transações realizadas por sociedades prestadoras de serviços de ativos virtuais e c) se a sociedade demandada responde por prejuízos decorrentes de golpe praticado por terceiros em operações envolvendo criptoativos.

2. Não há falar em negativa de prestação jurisdicional se o Tribunal de origem motiva adequadamente sua decisão, ainda que de forma sucinta, solucionando a controvérsia com a aplicação do direito que entende cabível à hipótese, apenas não no sentido pretendido pela parte.

3. As sociedades prestadoras de serviços de ativos virtuais (SPSVAs), autorizadas a funcionar pelo Banco Central do Brasil, estão submetidas às normas do Código de Defesa do Consumidor, por expressa dicção do art. 13 da Lei nº 14.478/2022.

4. Toda a compreensão que esta Corte Superior já firmou no tocante às obrigações impostas às instituições bancárias e às instituições de pagamento, inclusive no que se refere à incidência do Código de Defesa do Consumidor (Súmula nº 297/STJ), é inteiramente aplicável às sociedades prestadoras de serviços de ativos virtuais, às quais também é atribuído o dever de proteção e transparência nas relações com os clientes.

5. A responsabilidade das sociedades prestadoras de serviços de ativos virtuais somente poderá ser afastada se comprovada a inexistência de defeito na prestação do serviço ou a culpa exclusiva do consumidor ou de terceiro, a teor do disposto no § 3º do art. 14 do Código de Defesa do Consumidor.

6. As operações relacionadas com a compra, venda, troca e custódia de criptoativos podem envolver uma só prestadora (*exchange*) ou várias plataformas distintas, cada qual atraindo, nessa segunda hipótese, a responsabilidade por vícios porventura existentes nos serviços que cada uma prestou, a ser aferida a partir das incumbências legalmente atribuídas a cada uma delas.

7. Para fins de responsabilização das SPSAVs por eventuais falhas na prestação de serviço é preciso inicialmente delimitar qual o tipo de serviço por ela prestado para, em seguida, verificar se foram observadas as normas regulamentares a elas aplicáveis.

8. As incumbências legais das sociedades prestadoras de serviços de ativos virtuais, popularmente conhecidas como *exchanges*, estão previstas na

Resolução BCB nº 520/2025, também podendo ser levadas em consideração, para fins de responsabilização dessas empresas, as medidas de autorregulação por elas voluntariamente adotadas – devida diligência ao cliente (*know your client*), identificação das transações (*know your transaction*) e comunicação das operações suspeitas às autoridades competentes.
9. Hipótese em a fraude ocorreu no momento em que o autor transferiu os valores, por ele previamente depositados e convertidos para criptoativos dentro da plataforma ré, para uma carteira digital (*wallet*) vinculada a uma outra plataforma, responsável pela custódia desses ativos, a evidenciar que o serviço de custódia de ativos virtuais, no qual se verificou a suposta fraude, não foi prestado pela ré, não podendo ela ser responsabilizada pela reparação do prejuízo sofrido.
10. Recurso especial não provido.

RELATÓRIO

Trata-se de recurso especial interposto por EMILIO ANTONIO QUEIROZ MURTA, com fundamento no art. 105, III, "a" e "c", da Constituição Federal, contra acórdão do Tribunal de Justiça do Estado de Minas Gerais assim ementado:

> *"EMENTA: DIREITO CIVIL E DO CONSUMIDOR. APELAÇÃO CÍVEL. PLATAFORMA DE INTERMEDIAÇÃO DE CRIPTOMOEDAS. FRAUDE PRATICADA POR TERCEIRO. RESPONSABILIDADE CIVIL DA EXCHANGE. INEXISTÊNCIA. RELAÇÃO DE CONSUMO NÃO CARACTERIZADA. FORTUITO EXTERNO. AUSÊNCIA DE FALHA NA PRESTAÇÃO DO SERVIÇO. RECURSO DESPROVIDO.*
> *I. CASO EM EXAME*
> *1. Recurso de apelação interposto por Emílio Antônio Queiroz Murta contra sentença que julgou improcedentes os pedidos formulados em ação declaratória de obrigação de fazer, cumulada com indenização por danos materiais e morais, ajuizada em face de NVIO Brasil Instituição de Pagamento Ltda. ('Bitso Brasil').*
> *2. O autor alegou que transferiu 11.749,15 USDT (Tether) para uma carteira digital fraudulenta por meio da plataforma da requerida, pleiteando a responsabilização da exchange pelos prejuízos sofridos.*
> *3. A sentença recorrida concluiu pela inexistência de falha na prestação do serviço da requerida, afastando a responsabilidade civil e julgando improcedentes os pedidos do autor.*
> *II. QUESTÃO EM DISCUSSÃO*
> *4. Há duas questões em discussão: (i) definir se há relação de consumo entre as partes, com a consequente aplicação do Código de Defesa do Consumidor; e (ii) estabelecer se a plataforma de intermediação de criptomoedas pode ser responsabilizada pelos danos sofridos pelo autor em razão da fraude praticada por terceiro.*
> *III. RAZÕES DE DECIDIR*
> *5. A relação entre as partes não se enquadra como relação de consumo, pois o autor atuou como investidor de criptoativos, assumindo os riscos inerentes às operações, não se verificando a vulnerabilidade necessária para aplicação do Código de Defesa do Consumidor.*
> *6. Exchanges de criptomoedas não se equiparam a instituições financeiras reguladas, sendo inaplicável a jurisprudência que reconhece a responsabilidade objetiva de bancos por fraudes em operações bancárias.*
> *7. A transferência dos ativos digitais foi realizada pelo próprio autor, mediante suas credenciais e senha pessoal, inexistindo qualquer indício de comprometimento da segurança da plataforma da requerida.*
> *8. A jurisprudência consolidada afasta a responsabilidade das plataformas de criptomoedas quando não há falha sistêmica ou defeito na prestação do serviço, configurando-se, na hipótese, fortuito externo que rompe o nexo causal.*
> *9. O dano moral não se caracteriza pela simples frustração financeira decorrente de golpe aplicado por terceiro, sendo necessária demonstração de ofensa à dignidade ou constrangimento excepcional, o que não ocorreu no caso concreto.*
> *IV. DISPOSITIVO E TESE*

10. Recurso desprovido.
Tese de julgamento:
1. A relação jurídica entre plataformas de intermediação de criptomoedas e seus usuários não configura, por si só, relação de consumo, salvo demonstração de vulnerabilidade específica do investidor.
2. A responsabilidade das exchanges de criptomoedas por prejuízos decorrentes de fraudes praticadas por terceiros somente se configura quando há falha na prestação do serviço ou violação de deveres de segurança, o que não ocorreu no caso concreto.
3. O fortuito externo rompe o nexo causal e afasta a responsabilidade da plataforma quando as operações questionadas foram realizadas pelo próprio usuário, sem comprovação de defeito no sistema da exchange.
4. O dano moral não se configura unicamente pela perda financeira resultante de fraude, sendo necessária a comprovação de violação à dignidade ou sofrimento psicológico excepcional.
Dispositivos relevantes citados: Código de Defesa do Consumidor, art. 14, § 3º, II; Código de Processo Civil, art. 373, I.
Jurisprudência relevante citada: STJ, REsp nº 1.599.511/MG, Rel. Min. Paulo de Tarso Sanseverino, j. 21.02.2017; STJ, AgInt no REsp nº 1.899.126/SP, Rel. Min. Moura Ribeiro, j. 09.03.2021" (e-STJ fls. 297-298).

Os embargos de declaração opostos na origem foram rejeitados.

Em suas razões recursais (e-STJ fls. 337-361), o recorrente aponta, além de divergência jurisprudencial, violação dos seguintes dispositivos legais, com as respectivas teses:

a) art. 1.022, II, parágrafo único, II, do Código de Processo Civil - o órgão julgador incorreu em negativa de prestação jurisdicional ao deixar de enfrentar os questionamentos formulados nos embargos de declaração, relativamente à aplicação do CDC, à inversão do ônus da prova e à falha de segurança na intermediação de criptoativos;

b) art. 14 do Código de Defesa do Consumidor - o acórdão recorrido deixou de reconhecer a responsabilidade objetiva do fornecedor de serviços (*exchange* de criptomoedas) por falha na prestação, consistente na ausência de mecanismos de segurança capazes de impedir a transferência dos criptoativos para a "wallet" fraudulenta;

c) art. 6º, VIII, Código de Defesa do Consumidor e art. 373, § 1º, do Código de Processo Civil - impõe-se, na espécie, a inversão do ônus da prova, não se podendo exigir do consumidor a produção de prova impossível, podendo ainda ser aplicada a distribuição dinâmica do ônus da prova, por possuir a *exchange* maior facilidade técnica e informacional para comprovar a ausência de falha de segurança nas operações eletrônicas;

d) art. 186 e 927 do Código Civil - a *exchange* tem o dever de indenizar os prejuízos suportados pelo consumidor em razão de fraude eletrônica ocorrida na plataforma.

Apresentadas as contrarrazões (e-STJ fls. 366-387), e admitido o recurso na origem, subiram os autos a esta Corte Superior.

É o relatório.

VOTO

A irresignação não merece prosperar.

Na origem, EMILIO ANTONIO QUEIROZ MURTA ajuizou a presente demanda contra NVIO BRASIL INSTITUIÇÃO DE PAGAMENTO LTDA. ("BITSO BRASIL"), alegando, em síntese, ter sido vítima de golpe ao adquirir criptoativos e transferi-los para uma carteira digital (*wallet*) por meio da plataforma ré, que promove a intermediação desse tipo de negócio na internet.

Afirma o autor que, após transferir seus investimentos em criptoativos para a sua carteira digital, veio a descobrir posteriormente que se tratava de uma carteira falsa, sendo da plataforma ré, segundo seu entendimento, a responsabilidade pelo ressarcimento dos prejuízos sofridos, seja por não ter garantido meios de segurança capazes de identificar que a chave de transferência fornecida na forma de endereço eletrônico partia de uma carteira digital falsa, a revelar a existência de defeito na prestação do serviço, seja em virtude dos riscos inerentes ao negócio por ela explorado.

Ao final, o autor requer seja a ré condenada a: a) prestar todas as informações capazes de identificar os titulares dos endereços eletrônicos (chaves de acesso) utilizados para as transferências de USDT, de sua plataforma digital para a carteira digital falsa, e a qual corretora pertencem os referidos endereços; b) ressarcir o autor no valor de R$ 59.685,68 (cinquenta e nove mil seiscentos e oitenta e cinco reais e sessenta e oito centavos), acrescidos de juros e correção desde o desembolso, e c) pagar danos morais, no valor de R$ 20.000,00 (vinte mil reais).

O magistrado de primeiro grau de jurisdição julgou improcedentes os pedidos formulados na inicial, por entender, essencialmente, que o autor "(...) *foi imprudente em acreditar em terceiro fraudador, que lhe convenceu a transferir recurso da conta digital mantida na plataforma da Bitso, sem os cuidados necessários e recomendáveis a evitar ser vítima de golpe*", e que "(...) *foi o próprio autor quem solicitou a transferência de recursos de sua conta digital e indicou o destinatário, sendo ele, portanto, o responsável pela operação, pois, competia à ré cumprir a ordem do correntista*" (e-STJ fl. 225).

Na sequência, a Décima Quarta Câmara Cível do Tribunal de Justiça de Minas Gerais negou provimento à apelação do autor, mantendo integralmente a sentença, a ensejar a interposição do recurso especial que se passa a examinar.

A controvérsia dos autos resume-se a saber: a) se houve negativa de prestação jurisdicional; b) se incide o Código de Defesa do Consumidor nas transações realizadas por sociedades prestadoras de serviços de ativos virtuais e c) se a sociedade demandada responde por prejuízos decorrentes de golpe praticado por terceiros em operações envolvendo criptoativos.

Inicialmente, não há falar em negativa de prestação jurisdicional nos declaratórios, a qual somente se configura quando, na apreciação do recurso, o Tribunal de origem insiste em omitir pronunciamento acerca de questão que deveria ser decidida, e não foi.

Concretamente, verifica-se que o órgão julgador enfrentou todas as questões suscitadas pelas partes recorrentes, concluindo, no entanto, mediante decisão fundamentada, que: a) "(...) *não há qualquer prova de que a plataforma Bitso tenha sido alvo de invasão, fraude interna ou qualquer comprometimento de segurança* "; b) "(...) *as exchanges de criptoativos não podem ser responsabilizadas por fraudes externas, praticadas por terceiros, quando não há indícios de falha na segurança da*

plataforma ou violação de normas de proteção ao consumidor"; c) "(...) *a própria vítima, por erro ou imprudência, indicou os endereços para os quais os valores deveriam ser transferidos, autorizando as transações*"; d) "(...) *ao se cadastrar na plataforma da recorrida e realizar transações em criptoativos, não se colocou na posição de consumidor vulnerável, mas sim de investidor, assumindo os riscos inerentes às operações com ativos digitais*" e e) "(...) *a apelada não pode ser responsabilizada pelos prejuízos financeiros suportados pelo apelante, por não estar configurada qualquer falha na prestação dos serviços, mas a ação do autor que procedeu à transferência dos seus ativos sem se assegurar do destino que lhes era dado*" (e-STJ fls. 304-306).

Frisa-se que, mesmo à luz do art. 489 do Código de Processo Civil, o órgão julgador não está obrigado a se pronunciar acerca de todo e qualquer ponto suscitado pelas partes, mas apenas a respeito daqueles capazes de, em tese, de algum modo, infirmar a conclusão adotada pelo órgão julgador (inciso IV), não se podendo confundir, portanto, negativa de prestação jurisdicional ou ausência de fundamentação com decisão contrária aos interesses da parte.

A propósito:

> *"AGRAVO INTERNO NOS EMBARGOS DE DECLARAÇÃO NO AGRAVO EM RECURSO ESPECIAL. EMBARGOS À EXECUÇÃO. CONTRATO DE PRESTAÇÃO DE SERVIÇOS ADVOCATÍCIOS. VIOLAÇÃO AOS ARTS. 489, § 1º, IV, E 1.022, II, DO CPC/2015. INEXISTÊNCIA. DISSÍDIO JURISPRUDENCIAL. NÃO DEMONSTRADO. OMISSÃO. PECULIARIDADES DE CADA CASO. INVIABILIDADE. AGRAVO NÃO PROVIDO.*
> *1. Não há falar em violação dos arts. 489 e 1.022 do CPC/2015, pois o Tribunal de origem dirimiu as questões pertinentes ao litígio, apresentando todos os fundamentos jurídicos pertinentes à formação do juízo cognitivo proferido na espécie, apenas não foi ao encontro da pretensão da parte agravante.*
> *(...)*
> *4. Agravo interno a que se nega provimento"* (AgInt no AREsp 1.518.865/DF, relator Ministro LUIS FELIPE SALOMÃO, QUARTA TURMA, julgado em 10/12/2020, DJe de 1º/2/2021).

> *"PROCESSUAL CIVIL. AGRAVO INTERNO NO RECURSO ESPECIAL. APRECIAÇÃO DE TODAS AS QUESTÕES RELEVANTES DA LIDE PELO TRIBUNAL DE ORIGEM. AUSÊNCIA DE AFRONTA AO ART. 489 e 1.022 DO CPC/2015. REEXAME DO CONTRATO E DO CONJUNTO FÁTICO-PROBATÓRIO DOS AUTOS. INADMISSIBILIDADE. INCIDÊNCIA DAS SÚMULAS N. 5 E 7 DO STJ. DECISÃO MANTIDA.*
> *1. Inexiste afronta aos arts. 489 e 1.022 do CPC/2015 quando o acórdão recorrido pronuncia-se, de forma clara e suficiente, acerca das questões suscitadas nos autos, manifestando-se sobre todos os argumentos que, em tese, poderiam infirmar a conclusão adotada pelo Juízo.*
> *(...)*
> *4. Agravo interno a que se nega provimento"* (AgInt no REsp 1.659.130/RS, relator Ministro ANTONIO CARLOS FERREIRA, QUARTA TURMA, julgado em 30/11/2020, DJe de 9/12/2020).

Assiste razão ao recorrente quanto à incidência das normas de proteção ao direito do consumidor nas transações realizadas pelas sociedades prestadoras de serviços de ativos virtuais, por expressa dicção do **art. 13 da Lei nº 14.478/2022** ("Marco Legal dos Criptoativos"):

> *"Art. 13. Aplicam-se às operações conduzidas no mercado de ativos virtuais, no que couber, as disposições da Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor)."*

Além disso, toda a compreensão que já se firmou no tocante às obrigações impostas às instituições bancárias, **inclusive em relação à incidência do Código de Defesa do Consumidor (Súmula nº 297/STJ)**, é inteiramente aplicável às **instituições de pagamento**, a exemplo da ora recorrida, às quais também é atribuído o dever de processar com segurança as transações dos usuários finais, por expressa disposição do art. 7º da Lei nº 12.865/2013:

> *"Art. 7º Os arranjos de pagamento e* ***as instituições de pagamento observarão os seguintes princípios****, conforme parâmetros a serem estabelecidos pelo Banco Central do Brasil, observadas as diretrizes do Conselho Monetário Nacional:*
>
> *I - interoperabilidade ao arranjo de pagamento e entre arranjos de pagamento distintos;*
>
> *II -* ***solidez e eficiência dos arranjos de pagamento e das instituições de pagamento****, promoção da competição e previsão de transferência de saldos em moeda eletrônica, quando couber, para outros arranjos ou instituições de pagamento;*
>
> *III - acesso não discriminatório aos serviços e às infraestruturas necessários ao funcionamento dos arranjos de pagamento;*
>
> *IV -* ***atendimento às necessidades dos usuários finais, em especial liberdade de escolha, segurança, proteção de seus interesses econômicos****, tratamento não discriminatório, privacidade e* ***proteção de dados pessoais****, transparência e acesso a informações claras e completas sobre as condições de prestação de serviços;*
>
> *V -* ***confiabilidade, qualidade e segurança dos serviços de pagamento****; e*
>
> *VI - inclusão financeira, observados os* ***padrões de qualidade, segurança*** *e transparência equivalentes em todos os arranjos de pagamento.*
>
> *Parágrafo único. A regulamentação deste artigo assegurará a capacidade de inovação e a diversidade dos modelos de negócios das instituições de pagamento e dos arranjos de pagamento."* (grifou-se)

A propósito:

> *"RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. DISPOSITIVOS CONSTITUCIONAIS. VIOLAÇÃO. ANÁLISE. IMPOSSIBILIDADE. INSTITUIÇÃO DE PAGAMENTOS. GOLPE DE ENGENHARIA SOCIAL. FALSA CENTRAL DE ATENDIMENTO. OPERAÇÕES REALIZADAS. CIRCUNSTÂNCIAS. ANÁLISE. NECESSIDADE. PRESTAÇÃO DE SERVIÇO. DEFEITO CONFIGURADO.*
> *1. A controvérsia dos autos resume-se a saber se as instituições de pagamento, à semelhança das instituições bancárias, estão obrigadas a desenvolver mecanismos inteligentes de prevenção e bloqueio de fraudes, capazes de identificar comportamentos atípicos e agir rapidamente para evitar prejuízos.*
> *2. Nos termos do art. 105, III, da Constituição Federal, não compete a esta Corte o exame de suposta violação de dispositivos constitucionais, ainda que para fins de prequestionamento, sob pena de invasão da competência atribuída ao Supremo Tribunal Federal.*
> *3. De acordo com a orientação emanada da Súmula nº 479/STJ, as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.*
> *4.* ***Toda a compreensão que esta Corte Superior já firmou no tocante às obrigações impostas às instituições bancárias, inclusive no que se refere à incidência do Código de Defesa do Consumidor (Súmula nº 297/STJ), é inteiramente aplicável às instituições de pagamento, às quais também é atribuído o dever de processar com segurança as transações dos usuários finais, por expressa disposição do art. 7º da Lei nº 12.865/2013****.*
> *5. A responsabilidade das instituições de pagamento, e de todos aqueles que integram os denominados arranjos de pagamento, somente poderá ser*

afastada se comprovada a inexistência de defeito na prestação do serviço ou a culpa exclusiva do consumidor ou de terceiro, a teor do disposto no § 3º do art. 14 do Código de Defesa do Consumidor.
6. Constitui atribuição das instituições financeiras, e de todas aquelas que participam dos denominados arranjos de pagamento, criar mecanismos capazes de identificar e coibir a prática de fraudes e de mantê-los em constante aprimoramento, em virtude do dever de gerir com segurança as movimentações de dinheiro dos seus clientes e do elevado grau de risco da atividade por elas desempenhada.
7. Se o serviço não fornece a segurança que dele se pode esperar, levando em consideração o modo do seu fornecimento e o resultado e os riscos que razoavelmente dele se esperam, é ele defeituoso, nos termos do § 1º do art. 14 do Código de Defesa do Consumidor.
8. Uma vez comprovada a hipótese de vazamento de dados por culpa da instituição financeira ou instituição de pagamento, será dela, em regra, a responsabilidade pela reparação integral de eventuais danos. Hipótese descartada no caso concretamente examinado.
9. Para a identificação de possíveis fraudes, os sistemas de proteção contra fraudes desenvolvidos pelas instituições bancárias/de pagamento devem considerar i) as transações que fogem ao perfil do cliente ou ao seu padrão de consumo; ii) o horário e o local em que as operações foram realizadas; iii) o intervalo de tempo entre uma e outra transação; iv) a sequência das operações realizadas; v) o meio utilizado para a sua realização; vi) a contratação de empréstimos atípicos em momento anterior à realização de pagamentos suspeitos; enfim, diversas circunstâncias que, conjugadas, tornam possível ao fornecedor do serviço identificar se determinada transação deve ou não ser validada.
10. A validação de operações suspeitas, atípicas e alheias ao perfil de consumo do correntista deixa à mostra a existência de defeito na prestação do serviço, a ensejar a responsabilização das instituições financeiras e das instituições de pagamento.
11. Hipótese em que a) todas as operações bancárias, em um total de 14 (quatorze), foram realizadas no mesmo dia; b) a conta era utilizada como uma espécie de poupança, com pouquíssimas movimentações, e c) as transações realizadas fogem do perfil de consumo do correntista.
12. Recurso especial provido" (REsp 2.222.059/SP, Rel. Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 7/10/2025, DJEN de 13/10/2025 - grifou-se).

Na hipótese, a própria recorrida admite estar autorizada pelo Banco Central do Brasil "(...) *a funcionar como* ***instituição de pagamento regulada****, nas modalidades de emissor de moeda eletrônica e emissor de instrumento de pagamento pós-pago*" (e-STJ fl. 95 - grifou-se), não havendo dúvida, portanto, por qualquer ângulo que se examine, quanto à aplicabilidade do Código de Defesa do Consumidor.

No entanto, a despeito da incidência das normas consumeristas na espécie, razão não assiste ao autor quanto à pretendida responsabilização da parte ré pela reparação dos prejuízos que alega ter sofrido.

Para melhor compreensão da controvérsia, faz-se necessário apresentar algumas peculiaridades atinentes às operações envolvendo criptoativos, tarefa que ficou bem menos sofrida para o operador do Direito a partir da edição da Lei nº 14.478/2022 e seus respectivos regulamentos.

Com o avanço do uso da tecnologia digital nas mais diversas áreas de conhecimento, surgiram as denominadas "*criptomoedas*", idealizadas a partir de 2008 para servir como meio de pagamento descentralizado, ou seja, sem a intervenção de uma autoridade central, valendo ressaltar que essa nova modalidade de representação digital de valores destoa, em inúmeros aspectos, dos métodos até então utilizados globalmente.

De início, impõe-se registrar a atecnia do uso da expressão "*criptomoedas*", tendo em vista que tais ativos não possuem todas as características de uma moeda – entendida como o ativo financeiro emitido por uma instituição financeira oficial, de aceitação geral e curso forçado garantido por lei, utilizado na troca de bens e serviços, com poder liberatório (capacidade de pagamento) instantâneo – e tampouco se confundem com a definição de moeda eletrônica de que trata a Lei nº 12.865/2013, sendo mais adequado, portanto, o uso da expressão "*criptoativos*".

Em seu endereço eletrônico, o Banco Central do Brasil reforça a compreensão de que os ativos virtuais "*não têm as características de uma moeda, ou seja, de meio de troca, de reserva de valor e de unidade de conta, mas, sim, as características de ativo*", decorrendo o seu valor *"exclusivamente da confiança entre quem adquire e quem emite*" (https://www.bcb.gov.br/meubc/faqs/p/moedas-virtuais-criptomoedas-ou-criptograficas - acessado em 21/1/2025).

Anota-se, a propósito, que a Terceira Seção desta Corte Superior já teve a oportunidade de decidir que

> *"(...) a operação envolvendo compra ou venda de criptomoedas não encontra regulação no ordenamento jurídico pátrio, pois* ***as moedas virtuais não são tidas pelo Banco Central do Brasil (BCB) como moeda, nem são consideradas como valor mobiliário pela Comissão de Valores Mobiliários (CVM)****, não caracterizando sua negociação, por si só, os crimes tipificados nos arts. 7º, II, e 11, ambos da Lei n. 7.492/1986, nem mesmo o delito previsto no art. 27-E da Lei nº 6.385/1976"* (CC 161.123/SP, Rel. Ministro Sebastião Reis Júnior, Terceira Seção, julgado em 28/11/2018, DJe de 5/12/2018 - grifou-se).

Em linguagem simples, criptoativos são ativos digitais de emissão não governamental, protegidos por criptografia e transacionados eletronicamente, podendo ser utilizados como investimento, meio de pagamento ou transferência de valores.

Uma boa definição conceitual de criptoativo é aquela trazida na Instrução Normativa RFB nº 1.888, de 3 de maio de 2019, que, a par de instituir a obrigatoriedade imposta ao contribuinte de prestar de informações relativas às operações realizadas com criptoativos à Receita Federal, estabeleceu que

> *"(...)*
> ***I - criptoativo:*** [é] *a* ***representação digital de valor*** *denominada em sua própria unidade de conta, cujo preço pode ser expresso em moeda soberana local ou estrangeira, transacionado eletronicamente com a utilização de criptografia e de tecnologias de registros distribuídos, que pode ser utilizado como forma de investimento, instrumento de transferência de valores ou acesso a serviços, e que não constitui moeda de curso legal; e*
> ***II - exchange de criptoativo:*** [é] *a pessoa jurídica, ainda que não financeira, que oferece serviços referentes a operações realizadas com criptoativos, inclusive* ***intermediação***, ***negociação*** *ou* ***custódia****, e que pode aceitar quaisquer meios de pagamento, inclusive outros criptoativos"* (grifou-se).

De forma semelhante, aLei nº 14.478/2022, ao estabelecer as diretrizes a serem observadas na prestação de serviços de criptoativos, dispôs que se considera ativo virtual "(...) *a* ***representação digital de valor*** *que pode ser negociada ou transferida por meios eletrônicos e utilizada para realização de pagamentos ou com propósito de investimento*" (art. 3º, *caput* - grifou-se).

Em comentário ao referido preceito legal, Oscar Valente Cardoso esclarece que o ativo virtual ou criptoativo deve ter três características cumulativamente:

> *"(...)*
> *(a)* ***representação digital de valor****: deve ser uma unidade digital (logo, não física) que possui* ***valor econômico*** *e exerce a primeira função da moeda, ou seja, pode ser utilizada para atribuir um preço a um objeto (como os produtos e serviços);*
> *(b) objeto de negociação ou transferência por meios eletrônicos: deve ser* ***negociável em um ambiente digital****, isto é, o ativo com representação digital de um valor é* ***passível de ser comercializado, trocado ou transferido por meio de tecnologias eletrônicas*** *(como a internet e os sistemas de* blockchain*), sem a necessidade de intervenção física ou presencial. Logo,* ***a negociação ou transferência dos criptoativos pode ocorrer de forma descentralizada, com a dispensa dos intermediários tradicionais, como as instituições financeiras****; e*
> *(c) capacidade de realização de pagamentos ou o propósito de investimento: a capacidade de realização de pagamentos se refere à* ***possibilidade de utilização do criptoativo para efetuar transações comerciais e financeiras****, como se fosse uma moeda convencional. Por sua vez, o propósito de investimento diz respeito à utilização do criptoativo como forma de investimento, com o objetivo de se obter lucro em decorrência de sua valorização no mercado. Na prática, existem criptoativos cuja finalidade principal é a realização de pagamentos, enquanto outros têm maior ênfase no propósito de investimento"* (*Lei das criptomoedas comentada*, São Paulo: Thomson Reuters Revista dos Tribunais, 2023, RL-1.4).

Diferentemente do modelo centralizado atualmente adotado pelas instituições bancárias, as transações envolvendo criptoativos utilizam a tecnologia de registros distribuídos (*Distributed Ledger Technology* – DLT), que funciona sem a presença de uma instituição intermediadora para validá-las, sendo o *blockchain* a mais comum delas.

No *blockchain,* de acordo com o estudo de Carlos Alexandre Rodrigues, "*(...) essa confiança é retirada de uma parte específica e repassada para* ***toda a rede e seus usuários****, os quais passam a ser os responsáveis pela validação e registro histórico das transações*" (*As criptomoedas, o initial coin offering (ICO) e os aspectos regulatórios: em que estágio está o Brasil em relação ao resto do mundo*. Revista dos Tribunais, São Paulo, v. 107, n. 995, set. 2018, pág. 614 - grifou-se).

No exemplo trazido por Daniel de Paiva Gomes e Eduardo de Paiva Gomes, o sistema, baseado na ideia de um grande livro-razão público, descentralizado e distribuído, dentro do qual todos os usuários possuem as mesmas permissões, a fim de permitir que todos verifiquem a cadeia de blocos verdadeira, funciona da seguinte maneira:

> *"(...) imaginemos um exemplo em que 'A' envia 2 bitcoins para 'B'. Os demais nós que compõem o sistema recebem a informação de que tal transação existe e se encontra pendente de validação. Nesse momento, inicia-se uma 'corrida', pois os demais usuários do protocolo Bitcoin utilizam seus computadores para validar a transação da forma mais rápida possível. Aquele que validar a transação recebe bitcoins (aquisição originária e fee* [taxa] *transacional).* ***Após a validação, a transação é inserida em um novo bloco da Blockchain, o qual, posteriormente, é repassado para todos os demais usuários****."* (*Criptoativos, Tokenização, Blockchain e Metaverso* [livro eletrônico]: aspectos filosóficos, tecnológicos, jurídicos e econômicos / Daniel de Paiva Gomes, Eduardo de Paiva Gomes, Paulo Cesar Conrado, coordenação. 1. ed., São Paulo: Thomson Reuters Brasil, 2022, RB-6.1 - grifou-se)

Há consenso de que o uso da tecnologia *blockchain,* por exigir a validação de toda a rede e de seus usuários, traz inúmeras vantagens no que diz respeito à segurança das transações oficialmente realizadas.

No entanto, por se tratar de inovação tecnológica ainda em desenvolvimento, com riscos desconhecidos e imprevisíveis, e que ainda não foi completamente introduzida no dia-a-dia da maioria das pessoas, acaba sendo terreno fértil para fraudes perpetradas por terceiros.

As transações de criptoativos, não obstante a possibilidade da negociação direta entre pessoas (*Peer-to-Peer*), são normalmente realizadas por intermédio das Sociedades Prestadoras de Serviços de Ativos Virtuais (SPSAVs), popularmente conhecidas como *exchanges*.

As *exchanges* exercem papel fundamental nesse tipo de operação, permitindo aos usuários a **compra**, **venda** e **troca** de criptoativos com maior segurança, sendo que muitas delas também oferecem serviço de **custódia**, armazenando os criptoativos de seus clientes em carteiras digitais (*wallets*).

Nesse aspecto, essa nova tecnologia também difere do modelo tradicional de guarda e circulação de riquezas, visto que os criptoativos não ficam vinculados a pessoas, mas a **chaves específicas protegidas por criptografia** (*tokens*).

Os criptoativos também não ficam "guardados" dentro das carteiras virtuais como arquivos ou moedas digitais armazenadas localmente. Na verdade, eles existem como registros na própria *blockchain.* O que define a posse de um criptoativo é a associação dele a um endereço específico dentro dessa rede, sendo esse endereço derivado de chaves criptográficas.

As carteiras virtuais (*wallets*), portanto, não armazenam os criptoativos em si, mas sim as **chaves públicas e privadas** que permitem ao usuário movimentá-los na *blockchain*. A chave pública gera o endereço que pode ser compartilhado para receber valores, semelhante ao número de uma conta bancária, enquanto a chave privada funciona como uma assinatura digital (senha) que autoriza transações.

Assim, quem controla a chave privada controla os ativos vinculados àquele endereço. Por isso, a segurança de uma carteira está diretamente relacionada com a proteção dessas chaves, que podem ser armazenadas em dispositivos físicos, mídias digitais, aplicativos ou até mesmo em formato impresso.

A partir dessa variedade de formas de armazenamento, surgem as seguintes classificações, que **podem também influir na definição da responsabilidade das *exchanges***:

Quanto à conexão com a *internet*, as carteiras digitais (*wallets*) estão divididas em *Hot Wallets* (quentes) e *Cold Wallets* (frias), sendo as primeiras mais práticas para o uso diário em movimentações frequentes e de pequenos valores, porém mais expostas a ataques cibernéticos, por estarem constantemente conectadas à rede mundial de computadores, e a segunda mais indicada para guardar grandes quantias a longo prazo, sendo muito mais seguras contra ataques *hackers*.

A normatização aplicável aos criptoativos, que será introduzida mais a frente, ainda traz o conceito de "carteira morna", tipo de carteira de ativos virtuais que

representa uma categoria intermediária entre as carteiras fria e quente, sendo mantida conectada à rede mundial de computadores com acréscimo de camadas de segurança.

Quanto à custódia das chaves privadas, tem-se as chamadas *Wallets Custodiais*, em que a chave é controlada somente pela empresa custodiante, e as *Wallets Non-Custodiais*, em que o próprio usuário controla a chave privada.

Quanto ao formato, são três os tipos de carteiras digitais: as *Software Wallets*, acessadas mediante aplicativo específico ou extensão de navegador na internet, as *Hardware Wallets*, nas quais as chaves são guardadas em um dispositivo de armazenamento físico *off line*, e as *Paper Wallets*, em que a chave privada é impressa em um papel.

Quanto à assinatura, existem as *Single-Signatures* e as *Multi-Signatures*, a depender do número de assinaturas necessárias para acesso e movimentação de fundos.

As carteiras digitais também pode ser divididas **quanto ao tipo de *blockchain* utilizado**: as *Wallets específicas* funcionam apenas em uma rede e para um tipo específico de criptoativo (ex.: Bitcoin), enquanto as *Wallets multi-chain* suportam várias redes.

Na aferição da responsabilidade das *exchanges* por eventuais fraudes, é sempre importante definir qual o tipo de carteira digital utilizado, seja para confirmar ou não a existência de nexo causal entre a conduta do prestador de serviço e o dano, seja para constatar a existência ou não de vício no serviço prestado.

Para os fins que aqui interessam, importa registrar, por último, que **as operações relacionadas com a compra, venda, troca e custódia de criptoativos podem envolver uma só prestadora (*exchange*) ou várias plataformas distintas, cada qual atraindo, nessa segunda hipótese, a responsabilidade por vícios porventura existentes nos serviços que cada uma prestou**, a ser aferida a partir das incumbências legalmente atribuídas a cada uma delas.

Não se trata de exceção à regra da reponsabilidade solidária de todos os integrantes da cadeia de consumo, consagrada no Código de Defesa do Consumidor, tendo em vista que, no mais das vezes, há **absoluta independência entre os serviços prestados**.

No tocante às incumbências legais das *exchanges*, o art. 8º da Lei nº 14.478/2022, em conjunto com o art. 1º do Decreto nº 11.563/2023, atribuíram ao Banco Central do Brasil a competência para regulamentar o setor.

No exercício desse mister, foram editadas a **Resolução BCB nº 519/2025**, que **disciplina os processos de autorização relacionados ao funcionamento** das sociedades prestadoras de serviços de ativos virtuais, e a **Resolução BCB nº 520/2025**, que **disciplina a constituição e o funcionamento** das sociedades prestadoras de serviços de ativos virtuais, ambas em vigor a partir de 2 de fevereiro de 2026.

De acordo com esse segundo ato normativo, as SPSAVs são classificadas de acordo com os serviços de ativos virtuais prestados, podendo desempenhar as seguintes atividades: "(...) *I* - ***intermediárias de ativos virtuais***; *II* - ***custodiantes de ativos virtuais***; *e III* - ***corretoras de ativos virtuais***" (art. 4º, § 1º - grifou-se).

A **intermediação** de ativos virtuais, ainda de acordo com a norma citada, compreende a realização, exclusivamente, das seguintes atividades, por conta de terceiros, de forma individual ou cumulativa:

> *"Art. 7º (...)*
> *I - subscrever, isoladamente ou em consórcio com outras sociedades autorizadas, emissões de ativos virtuais;*
> *II - comprar, vender e trocar ativos virtuais;*
> *III - administrar carteiras de ativos virtuais ou carteiras compostas por ativos virtuais, valores mobiliários, ativos financeiros e outros instrumentos financeiros admitidos na regulamentação específica;*
> *IV - exercer funções de agente fiduciário nas operações do mercado de ativos virtuais;*
> *V - realizar operações de staking de ativos virtuais;*
> *VI - praticar operações de prestação de serviços de ativos virtuais no mercado de câmbio; e*
> *VII - exercer outras atividades expressamente autorizadas pelo Banco Central do Brasil."*

Já a **custódia** de ativos virtuais compreende a realização, exclusivamente, das seguintes atividades, de forma individual ou cumulativa:

> *"Art. 8º (...)*
> *I - a guarda e o controle dos instrumentos que afetam o exercício dos direitos e benefícios relacionados ao ativo virtual, a exemplo das chaves privadas;*
> *II - a descrição, tempestivamente atualizada, da posição do ativo virtual, de cada tipo de ativo do cliente ou usuário do contrato de custódia, bem como a conciliação tempestiva dessa posição com as informações pertinentes disponíveis nos sistemas baseados nas tecnologias de registros distribuídos ou similar;*
> *III - o atendimento das instruções de movimentação emitidas pelo titular do ativo virtual ou da pessoa ao qual foi delegado o poder de agir no interesse do titular, bem como a conservação dessas instruções;*
> *IV - o tratamento dos eventos incidentes sobre o ativo virtual; e*
> *V - a administração de dados e de informações relevantes ao exercício de alguma das atividades descritas nos incisos I a IV a respeito do titular e dos seus ativos virtuais custodiados."*

Finalmente, nos termos do art. 10 da Resolução BCB nº 520/2025, as **corretoras** de ativos virtuais têm por objeto social a intermediação e a custódia de ativos virtuais.

Além das normas regulatórias citadas, a autorregulação é um outro fator que pode ser levado em consideração para a responsabilização das *exchanges*. Por autorregulação, segundo artigo doutrinário de autoria de Tiago Misael de Jesus Martins, se entende

> *"(...) o* ***conjunto de medidas adotadas voluntariamente por prestadores de serviços de ativos virtuais (corretoras ou* exchanges*) com o objetivo de cumprir as normas de combate à lavagem de dinheiro (antilavagem) nos países onde estão sediados****. Essas medidas incluem notadamente a* ***adoção de devida diligência ao cliente (*know your client*, KYC)****, a* ***identificação das transações (*know your transaction*, KYT)*** *e a comunicação voluntária das operações suspeitas à Unidade de Inteligência Financeira.*
> *Tais normas antilavagem são obrigações impostas às instituições do mercado financeiro tradicional por* ***tratados internacionais*** *(convenções de Viena, Palermo e Mérida), por recomendações do FATF-GAFI (Recomendações nº 10, nº 11, nº 16 e nº 20) e por legislação nacional de*

cada país. No Brasil, elas foram impostas às entidades do Subsistema da Intermediação Financeira por meio dos arts. 10 e 11 da Lei de Lavagem de Dinheiro (Lei nº 9.613/98) e de normas regulamentares expedidas por órgãos estatais de supervisão (Subsistema Normativo de Regulação e Fiscalização) de mercados financeiros. Apenas com a Lei nº 14.478/2022, o Brasil positivou medidas antilavagem a cargo de prestadoras de serviços de ativos virtuais.

Ocorre que, ***mesmo antes de legislações nacionais,*** **exchanges** ***começaram a adotar, por vontade própria e como compromisso ético de não compactuar com atividades ilícitas, medidas de cooperação com o Estado*** *para rastreio de lavagem de capitais. No Brasil, as maiores corretoras de criptoativos se reuniram em 2017 em torno da Associação Brasileira de Criptoeconomia (ABCripto) e adotaram, em 2020, um* ***código de autorregulação*** *com vistas a prevenir fraudes, combater a lavagem de dinheiro e privilegiar medidas anticorrupção, aumentando a confiabilidade nos agentes do mercado.*

O código prevê procedimentos de coleta, verificação, validação e atualização de informações cadastrais, visando a conhecer clientes, funcionários, parceiros e prestadores de serviços terceirizados; procedimentos de registro de operações e de serviços financeiros; e procedimentos de monitoramento, seleção e análise de operações e situações suspeitas, com a comunicação ao Conselho de Controle de Atividades Financeiras (Coaf)." (Regulação de criptoativos e dados aproveitáveis em investigações criminais no Brasil, *in* Investigação com criptoativos, Brasília: MPF, 2024 - págs. 14-15 - grifou-se)

Assim, para fins de responsabilização das SPSAVs por eventuais falhas na prestação de serviço é preciso inicialmente delimitar qual o tipo de serviço por ela prestado para, em seguida, verificar se foram observadas as normas a elas aplicáveis.

Fixadas todas essas premissas, passa-se ao exame do caso concreto.

No caso em apreço, o próprio autor afirma que a fraude ocorreu no momento em que ele transferiu os valores, por ele previamente depositados e convertidos para criptoativos dentro da plataforma ré (Bitso), para uma carteira digital (*wallet*), tendo, para tanto, informado ao réu uma **chave de acesso pública**, na forma de endereço eletrônico, **fornecida pela própria carteira digital**.

Confira-se:

"(...)

De uma forma resumida, ***o autor realiza depósito em moeda nacional (real) dentro da plataforma do réu*** *e* ***em seguida adquire criptomoedas, no caso USDT, e dentro da mesma plataforma transfere as criptomoedas para uma carteira digital*** *(wallet) pertencente ao autor.*

Exsurge esclarecer que ***para realizar a transferência de criptoativos para a carteira digital é informado ao réu uma chave de acesso na forma de endereço eletrônico fornecido pela própria carteira digital (wallet) para tal finalidade****.*

O endereço fornecido pela carteira, funciona como uma espécie de conta bancária, se compararmos a um banco tradicional.

Pois bem, ***o autor possuía uma carteira digital (BATCOIN), vindo a descobrir posteriormente que se tratava de uma carteira falsa (fake)****, e cujos* ***endereços fornecidos por esta carteira****, como espécie de conta bancária, era informado ao réu para realização da operação de transferências de criptomoedas (USDT), ou seja, as criptomoedas eram sacadas da plataforma do réu para dentro da carteira.*

Ato contínuo, com a intermediação do réu foram transferidos 11.749,15 USDT à falsa carteira digital através 3 (três) endereços distintos ***fornecidos pela mesma carteira***" (e-STJ fls. 2-3 - grifou-se).

Na narrativa apresentada na petição inicial, portanto, é possível identificar a existência das seguintes operações: 1) transferência de valores efetuada pelo autor, em moeda corrente (reais), para a plataforma ré; 2) compra de ativos virtuais específicos (USDT - Thether) dentro da plataforma ré, e 3) transferência dos ativos virtuais para uma carteira digital (*wallet*) **vinculada a uma outra plataforma**, responsável pela custódia desses ativos.

Em tese, eventuais defeitos na prestação de serviço poderão ser identificados em qualquer uma dessas fases, a atrair a responsabilidade daquela instituição que agiu em contrariedade às normas de regência.

No caso, todavia, encerrou-se a atuação da ré no momento em que ela, **a pedido do autor e com a identificação do recebedor por ele fornecida**, efetuou a transferência dos criptoativos para uma **carteira externa custodiada por outra plataforma**, a qual ele próprio afirma ter-lhe fornecido a chave de acesso (endereço de destino) e **que não mantém nenhuma relação com a demandada**.

Em determinado trecho da contestação, afirma a ré que

> *"(...) as transações realizadas pelo Autor por meio de sua conta na Bitso, aparentemente por indução de terceiros desconhecidos, mas certamente por sua livre e espontânea vontade,* ***foram enviadas para carteiras privadas externas sem relação jurídica com a BITSO****.*
>
> *80. Neste ponto, a única informação detectada pela Ré acerca do destino dos valores depositados pelo Autor é de que as criptomoedas foram enviadas, em sua maioria, para uma carteira externa na OKX.com, uma corretora de criptomoedas"* (e-STJ fl. 120).

Vale dizer, o serviço de custódia de ativos virtuais, no qual se verificou a suposta fraude, não foi prestado pela ré, não podendo ela ser responsabilizada pela reparação do prejuízo sofrido.

Aliás, entre as atribuições dos **custodiantes** de ativos virtuais está "(...) *a adoção de medidas que mitiguem o risco de violação à integridade e a qualquer outra característica dos ativos virtuais custodiados cuja violação provoque ou possa provocar prejuízo do exercício justo dos direitos pelo titular dos ativos virtuais*" (art. 9, § 1º, da Resolução BCB nº 520/2025).

E diante de tal conclusão, de nada adiantaria determinar a inversão do ônus da prova, porquanto devidamente comprovado que não houve vício no serviço prestado pela plataforma ré.

Em tais circunstâncias, restaria ao autor a opção de voltar a sua pretensão contra a instituição mantenedora da carteira digital falsa para a qual foram transferidos os seus criptoativos, por, supostamente, permitir a abertura e manter aberta carteira utilizada para a prática de golpes, conforme já decidido, com as adequações necessárias, no seguinte julgado:

> *"RECURSO ESPECIAL. DIREITO DO CONSUMIDOR. DISPOSITIVOS CONSTITUCIONAIS. VIOLAÇÃO. ANÁLISE. IMPOSSIBILIDADE. CERCEAMENTO DE DEFESA. PREQUESTIONAMENTO. AUSÊNCIA. SÚMULA Nº 282/STF. GOLPE DO FALSO LEILÃO. INSTITUIÇÃO FINANCEIRA. CONTA DE DEPÓSITOS. CRIAÇÃO E MANUTENÇÃO. REGULAÇÃO. BANCO CENTRAL. DEVER DE OBSERVÂNCIA. SERVIÇO DEFEITUOSO. COMPROVAÇÃO. NECESSIDADE.*
> *1. A controvérsia principal dos autos resume-se a saber se as instituições financeiras depositárias de valores provenientes da prática de atividades*

ilícitas podem ser responsabilizadas pela abertura e manutenção de contas utilizadas para esse fim.
2. Nos termos do art. 105, III, da Constituição Federal, não compete a esta Corte o exame de suposta violação de dispositivos constitucionais, ainda que para fins de prequestionamento, sob pena de invasão da competência atribuída ao Supremo Tribunal Federal.
3. A falta de prequestionamento da matéria deduzida pela parte recorrente impede o conhecimento do recurso especial (Súmula nº 282/STF).
4. De acordo com a orientação emanada da Súmula nº 479/STJ, as instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.
5. A responsabilidade das instituições bancárias somente poderá ser afastada se comprovada a inexistência de defeito na prestação do serviço ou a culpa exclusiva do consumidor ou de terceiro, a teor do disposto no § 3º do art. 14 do Código de Defesa do Consumidor.
6. Comprovando a instituição financeira que, ao abrir e manter contas bancárias, cumpriu com seu dever de verificar e validar a identidade e a qualificação dos titulares da conta, bem como a autenticidade das informações fornecidas pelo cliente, deve ser afastada a sua responsabilidade objetiva, porquanto inexistente defeito na prestação do serviço. Precedente.
7. Necessidade de definir com precisão o conceito de conta regularmente aberta, levando em consideração o dever legal e regulamentar atribuído às instituições financeiras de garantir segurança aos usuários em todas as suas operações e o risco inerente à atividade por elas desempenhada, sem descurar, ainda, da fixação do ônus de comprovar a regularidade do procedimento de abertura e manutenção da conta, considerando a incidência das normas de proteção ao direito do consumidor (Súmula nº 297/STJ) e a possibilidade de inversão do ônus probatório (art. 6º, VIII, do CDC).
8. No processo de verificação e validação da identidade e da qualificação dos titulares da conta, bem como da autenticidade das informações fornecidas pelo cliente, podem ser detectadas diversas inconformidades que poderão ou não implicar a responsabilidade da instituição que validou a criação da conta e a manteve em plena atividade.
9. Ainda que seja regularmente admitida a abertura de contas por meios eletrônicos, sem a presença física de seus titulares ou representantes, esta deve ser encarada como uma estratégia operacional e mercadológica adotada por livre opção dos bancos, que devem suportar os riscos dela decorrentes.
10. ***A existência de contas em nome do próprio fraudador ou de outras às quais ele tenha acesso - contas essas que, bem ou mal, são abertas e mantidas pelas instituições financeiras - é o principal fator que possibilita atingir o resultado pretendido com prática dos mais variados tipos de golpes, daí exsurgindo, a depender sempre do caso concretamente examinado, a responsabilidade das entidades bancárias quando lhes faltar a necessária diligência no processo de abertura e manutenção dessas contas.***
11. A título meramente exemplificativo, são circunstâncias que implicam a responsabilidade dos bancos: i) abertura de contas com o uso de documento falso (aí incluídas todas as formas de falsidade), ou por meio de documento extraviado, sem que o verdadeiro titular tenha conhecimento; ii) movimentação de contas, regularmente abertas, por terceiros estelionatários sem o conhecimento do titular, se comprovadas eventuais falhas de segurança associadas à atuação da instituição bancária, e iii) manutenção de contas com movimentações suspeitas, se comprovada a falta de atuação dos bancos no sentido de identificá-las e de tomar as providências necessárias para evitar o seu uso para fins ilícitos.
12. Na hipótese, não tendo o autor se desincumbido de comprovar a existência de falha na prestação do serviço nem insistido no pedido de inversão do ônus probatório, deve ser confirmada a improcedência do pedido formulado na demanda, haja vista a ausência de elementos nos autos capazes de demonstrar que o serviço prestado era defeituoso.
13. Recurso especial parcialmente conhecido e não provido" (REsp 2.222.137/SP, Rel. Ministro Ricardo Villas Bôas Cueva, Terceira Turma, julgado em 7/10/2025, DJEN de 13/10/2025 - grifou-se).

No caso em apreço, não tendo o autor incluído a instituição mantenedora da carteira digital para a qual transferiu seus recursos no polo passivo da ação e não tendo comprovado a existência de defeito nos serviços prestados pela ré, não resta outra alternativa senão confirmar a improcedência da demanda.

Ante o exposto, nego provimento ao recurso especial.

Na origem, os honorários sucumbenciais foram fixados em 15% (quinze por cento) sobre o valor da causa, os quais devem ser majorados para o patamar de 20% (vinte por cento) em favor dos advogados da recorrida, nos termos do art. 85, § 11, do Código de Processo Civil, observado o benefício da gratuidade da justiça.

É o voto.