Google deve indenizar roubo de criptoativos decorrente de invasão ao Gmail?

Pode o Google ser responsabilizado por indenizar um usuário que teve suas criptomoedas após a invasão ao Gmail?

Para responder esta pergunta, vamos primeiramente tratar de aspectos técnicos relacionados ao funcionamento de tais carteiras de criptoativos **(1)**, para na sequência analisar um precedente recente e favorável da 3ª Vara Cível de Penha da França, na cidade de São Paulo, **(2)** e um precedente desfavorável do STJ **(3)**. Ao final, nossas considerações **(4)**.

Aspectos técnicos relacionados ao funcionamento das carteiras de criptoativos

Dada a natureza descentralizada, o responsável pela custódia dos criptoativos é o próprio usuário, o qual depende apenas de sua chave privada [1] para movimentar seu saldo. No entanto, em *exchanges* e em algumas carteiras online, quem possui a chave privada não é o usuário, mas o próprio provedor do serviço, o qual centraliza o acesso e as movimentações. Nesses casos, o usuário normalmente possui um login e senha de acesso perante o provedor de serviço, bem como fatores de autenticação adicionais (Tokens, SMS, etc.).

Porém, além das *exchanges* e carteiras online, também existem outros intermediários, como os provedores de e-mail e de aplicativos geradores de códigos de autenticação, a exemplo do Google, com o Gmail e o Google Authenticator. A depender do provedor de serviço de ativos virtuais (VASP) em questão, e do grau de proteção configurado pelo usuário, é possível que terceiros mal intencionados consigam, através do acesso ao e-mail cadastrado na *exchange*, entrar na conta da *exchange* e movimentá-la — tal qual também acontece em contas bancárias, redes sociais e aplicativos diversos.

Precedente 12/5/2025: 3ª Vara Cível de Penha da França (1005407-15.2024.8.26.0006) [2]

Neste caso, fraudadores invadiram a conta de e-mail do usuário na plataforma Gmail, na sequência alteraram a forma de autenticação de dois fatores do e-mail — retirando a autenticação via Token para e-mail da esposa do usuário para autenticação via Token em dispositivo físico, impossibilitando a recuperação pela vítima —, já com acesso ao e-mail, também obtiveram acesso ao Google Authenticator e, posteriormente, invadiram contas em *exchanges* de criptomoedas se utilizando da redefinição de senhas de acesso através de link para o e-mail hackeado.

Tal violação serviu como vetor para que os criminosos obtivessem acesso não autorizado a contas vinculadas a corretoras de criptoativos, culminando na movimentação fraudulenta e consequente esvaziamento do saldo em ativos digitais do titular.

A juíza Luciana Antunes Ribeiro Crocomo, da 3ª Vara Cível de Penha da França, na cidade de São Paulo, consignou na **sentença** que a requerida, embora dispusesse de ferramentas tecnológicas aptas à prevenção de acessos indevidos, não garantiu, de forma eficaz, a proteção da conta eletrônica do usuário, restando configurada a falha na prestação do serviço.

Em síntese, a decisão reforça a tese de que os provedores de serviços de internet, ainda que não atuem diretamente na operação ou custódia de criptoativos, podem ser responsabilizados civilmente quando sua conduta omissiva ou falhas sistêmicas contribuam de maneira substancial para a concretização do dano.

A controvérsia jurídica reside na possibilidade de imputar ao Google responsabilidade pelas deficiências de segurança que resultam, ainda que indiretamente, em prejuízos sofridos em plataformas de terceiros. A análise de precedentes semelhantes demonstra que a caracterização do dever de indenizar está intrinsecamente vinculada à forma de acesso e ao grau de relevância da plataforma de e-mail no iter criminis. Nesse sentido, compara-se com o julgado abaixo do STJ.

Precedente 25/11/2021: 3ª Turma do STJ (REsp 1.885.201/SP) [3]

No âmbito da 3ª Turma do Superior Tribunal de Justiça (REsp 1.885.201/SP), em 25 de novembro de 2021, restou decidido que o Google não deveria ser responsabilizado pelos danos materiais decorrentes da subtração de 79,2 *bitcoins* (à época avaliados em R$ 1 milhão), realizada por meio de acesso indevido à conta de e-mail da vítima em 2017.

123RF

Copyright © 2026 Consultor Jurídico

A vítima alegou que detinha conta na "Blockchain.com" cujo e-mail era o mesmo que havia sido hackeado, e que era possível solicitar um link temporário de acesso sem que fosse necessário se ter conhecimento da senha. De modo que o hacker teria invadido seu e-mail, ingressado na Exchange Blockchain.com através do link temporário de acesso, sacado todos os fundos, e deletado todos os e-mails.

A sentença, em sentido diverso do que defendido pelo autor, consignou que o requerente *"deixou de excluir arquivos que contivessem a senha para o acesso à carteira de bitcoins, já que tais e-mails são recebidos sempre que realizada movimentação no sistema ou nas corretoras, revelando desídia com quantia tão elevada"*.

O autor contestou tais fatos, sustentando inclusive que teria havido nulidade no julgamento diante da não apreciação de seu pedido de produção de prova pericial.

No entanto, o STJ manteve o posicionamento do juízo de primeiro grau, entendendo que o hacker somente poderia ter acessado a *exchange* na ocasião em que, além de ter acesso ao link de acesso enviado ao e-mail, também tivesse conhecimento do e-mail de acesso e da chave privada. Nesse sentido, concluiu a ministra Nancy Andrighi que não haveria nexo de causalidade no caso concreto, visto que seria provável que o invasor tivesse obtido acesso a chave privada (também por vezes referida pelo STJ por "senha") por outros meios, como ter fornecido a chave privada a terceiros, armazenado no e-mail ou por conta de eventual falha na *exchange*:

> *"52. Ocorre que, conforme esclarecido no tópico anterior, o acesso à carteira de criptomoedas exige, necessariamente, a indicação da chave privada. Ou seja, ainda que a gerenciadora adote o sistema de dupla autenticação afirmado pelo recorrente, qual seja, digitação da senha e envio, via e-mail, do link de acesso temporário, a simples entrada neste é insuficiente para propiciar o ingresso na carteira virtual e, consequentemente, viabilizar a transação das cryptocoins. (…).*
>
> *53. Nesse contexto, como assentado na origem, é provável que o invasor tenha obtido a senha do recorrente, seja porque ele tinha armazenado-a no e-mail, forneceu a terceiro ou até mesmo em razão de eventual falha apresentado no sistema da gerenciadora.*
>
> *54. Nenhuma dessas circunstâncias guarda relação com a conduta da recorrida ou com o risco do serviço por ela desenvolvido, razão pela qual não está configurado o nexo de causalidade. Logo, é descabida a pretendida atribuição à recorrida da responsabilidade pelo prejuízo material experimentado pelo recorrente."*

Data maxima venia, e sem a pretensão de realizar uma análise exaustiva do caso, considerando que parte dos autos estão em sigilo, entende-se que o acórdão pode ter incorrido em confusão quanto ao funcionamento de exchanges e wallets de criptoativos.

Vê-se que o STJ assentou o argumento no sentido de que o mero acesso ao e-mail não seria suficiente para ingressar e sacar os ativos digitais na Blockchain.com, pois ainda faltaria ciência do e-mail e da "chave privada" (também referida no acórdão por senha) que possibilitassem o acesso.

Ora, o e-mail presume-se ser o mesmo da conta hackeada. E a chave privada de fato não seria necessária, eis que a Blockchain.com, como qualquer outro provedor de serviços que oferece os serviços de *exchange* e também de carteira privada, não exige necessariamente o conhecimento da chave privada para realizar as transações. Embora possa permitir ao usuário ter conhecimento da chave privada, tal provedor de serviço também possui, de modo que o controle não reside apenas com o usuário.

Se realmente era possível ou não acessar a *exchange* e realizar movimentações com um link de acesso provisório (sem conhecimento da senha) não chegou a ser objeto direto de discussão ou de produção probatória, e é de difícil constatação considerando que os fatos ocorreram em 2017.

Copyright © 2026 Consultor Jurídico

De todo modo, o acórdão se inclinou no sentido de que a responsabilização do provedor de e-mail em casos de ataques cibernéticos envolvendo plataformas de *exchanges* ou carteiras digitais não é absoluto. O reconhecimento da obrigação de indenizar pressupõe a demonstração de nexo causal entre a conduta do fraudador e o evento danoso.

Nesse sentido, entendeu o STJ que Google não poderia ser responsabilizado por eventual desídia do usuário em salvar sua senha (chave privada) no próprio e-mail.

Tem-se com isso que o ônus da prova nas situações de furto de criptoativos poderá recair sobre a empresa, que deverá comprovar que o evento se deu por culpa exclusiva de terceiro, ou que não houve qualquer falha em seus sistemas de segurança quando da realização do ilícito.

Importa destacar que tal responsabilização pode ser compartilhada com as próprias plataformas de *exchange* ou carteiras digitais, cuja negligência na adoção de medidas preventivas também pode ensejar responsabilidade solidária.

Considerações finais

A fundamentação contida na sentença do caso da 3ª Vara Cível de Penha de França aplica claramente responsabilidade mais abrangente provedor de serviço de e-mail.

Todavia, apesar de o acórdão do STJ não ter indicado expressamente, acredita-se que o posicionamento da 3ª Turma estaria em linha com a da 3ª Vara Cível se houvesse partido do pressuposto de que o acesso ao e-mail foi suficiente para conseguir acessar a *exchange* — o que, reforça-se, aparenta ser incerto, tanto porque não se obteve acesso a parte dos autos que estão em sigilo quanto porque tal questão não chegou a ser objeto de produção de provas.

A matéria, ainda incipiente no ordenamento jurídico brasileiro, exige atualização e especialização do judiciário e dos advogados envolvidos no caso.

A rápida evolução do funcionamento e importância das plataformas digitais na segurança dos dados aumentou de sobremaneira da data dos fatos (2017) e do julgamento (2021) até os dias atuais, em que o provedor de e-mail é cada vez um prestador de muitos outros serviços além do próprio e-mail, como de backup de arquivos, fotos, gerador de códigos de autenticação, calendário, dentre outros.

Vê-se que no caso mais recente, a invasão da conta do Gmail teria permitido acesso aos aplicativo gerador dos códigos de segundo fator de autenticação, e o juízo entendeu que o provedor de e-mail teria responsabilidade pelos fatos disso decorrentes, o que a princípio denota escopo maior do que o definido pelo STJ no referido acórdão.

Assim, o desafio que se impõe ao Poder Judiciário é assegurar que as decisões judiciais proporcionem a devida prestação jurisdicional às partes envolvidas, estando tecnicamente alinhadas com as particularidades inerentes ao ecossistema das criptomoedas.

---

[1] A chave privada corresponde a um código hexadecimal de 64 caracteres, e somente com esta chave é possível movimentar uma carteira de criptoativos. Em meados de 2013, com o Bitcoin Improvement Proposal 39 (BIP-39), para facilitar o uso e a recordação das chaves privadas, o extenso código hexadecimal passou a poder ser convertido em frases mnemônicas, constituídas comumente de 12 a 24 palavras em inglês, as quais garantem igualmente a possibilidade de movimentar a carteira.

[2] TJ-SP 1005407-15.2024.8.26.0006, 3ª Vara cível de Penha da França, juíza Luciana Antunes Ribeiro Crocomo, Dje. 12/05/2025.

[3] STJ REsp 1.885.201/SP, 3ª Turma do Superior Tribunal de Justiça, min. rel. Nancy Andrighi, Dje. 25.11.2021.

Fonte: https://conjur.jumps.com.br/2025-mai-20/google-deve-indenizar-roubo-de-criptoativos-decorrente-de-invasao-ao-gmail/

Copyright © 2026 Consultor Jurídico