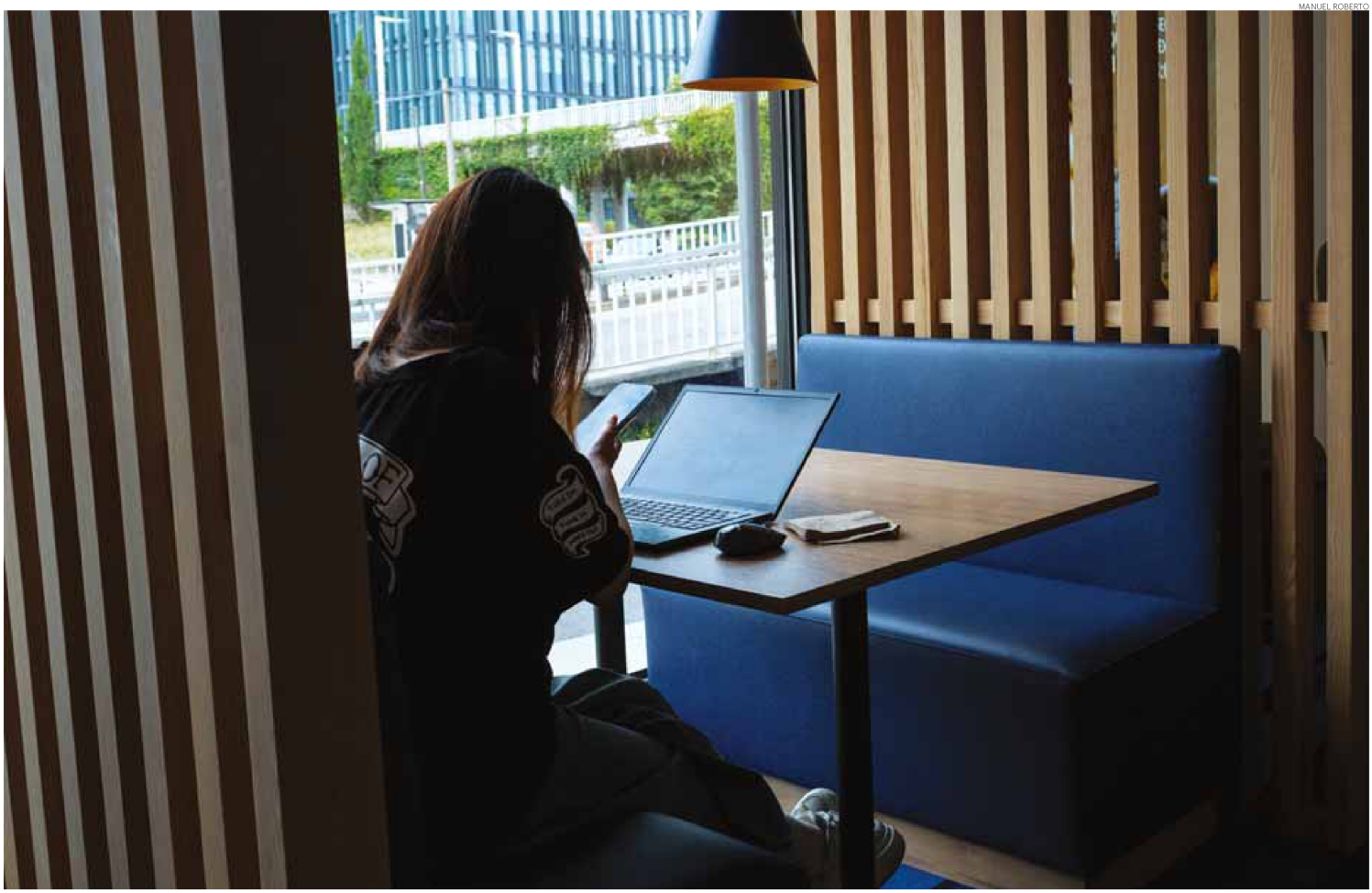
Fraudes digitais

Bancos têm de repor dinheiro antes de provar negligência

As vítimas de fraudes digitais vão estar mais protegidas na reposição de verbas que saem das suas contas bancárias Economia, 22/23


MANUEL ROBERTO

Bancos obrigados a repor dinheiro antes de provar negligência de clientes

A devolução imediata só pode ser recusada se houver suspeita (razoável) de actuação fraudulenta dos clientes, com comunicação às autoridades

Rosa Soares

As vítimas de fraudes digitais, por *phishing*, *pharming* e outras, que vêem milhares de euros desviados das suas contas bancárias em poucos minutos, passaram a estar mais protegidas na reposição dessas verbas por parte das instituições financeiras, mas isso não significa que não venham, pelo menos em parte dos casos, a suportar as perdas decorrentes desses ataques. A maior protecção decorre de um acórdão recente do Tribunal de Justiça da União Europeia (TJUE) que vem clarificar que no caso de uma operação de pagamento que os clientes aleguem "não ter autorizado", o prestador de serviços de pagamento está, em princípio, obrigado a reembolsar imediatamente esse montante, o mais tardar até ao fim do primeiro dia útil seguinte àquele em que tomou conhecimento ou foi informado da situação.

O acórdão, proferido no âmbito de um pedido de um tribunal da Polónia, na sequência de uma situação de *phishing* – envio de comunicações electrónicas que aparentam ter origem em instituições legítimas, induzindo o utilizador a introduzir credenciais de autenticação numa página com aparência do *site* oficial do banco –, vem clarificar o que já estava estabelecido na Directiva (UE) 2015/2366, transposta para a direito português pelo Decreto-Lei 91/2018, mas que as instituições financeiras não estavam a cumprir. Em síntese, o Tribunal de Justiça veio dizer que as instituições bancárias têm, primeiro, que reembolsar os clientes, mesmo que considerem que estes agiram "com dolo ou negligência grosseira". E depois, podem procurar reaver os montantes, se provarem que houve efectivamente "negligência grosseira" dos clientes, nomeadamente quando fornecem dados pessoais, como credenciais de segurança personalizadas, que acabam por permitir a concretização de transferência de saldos das contas.

A única excepção para a dispensa do reembolso imediato consta da directiva e, reforça o TJUE, verificar-se-á quando as instituições de pagamento tiverem "motivos razoáveis" para suspeitar de actuação fraudulenta do cliente, e comunicarem por escrito esses motivos às autoridades judiciárias, nos termos da lei penal e de processo penal. O prazo para esta

Um acórdão sobre um caso na Polónia vem definir novas orientações sobre fraudes digitais na banca

O acórdão pode ser invocado como um precedente judiciário e os tribunais podem segui-lo

Nuno Matos
Presidente da Associação Sindical dos Juízes Portugueses



comunicação é também até final do primeiro dia útil seguinte àquele em que tomou conhecimento.

O acórdão, já noticiado em vários órgãos de comunicação nacionais, representa, assim, uma vantagem para os clientes, particulares e empresas, ao assegurar que as suas contas não ficam totalmente desprovidas de fundos durante muito tempo, como tem acontecido em diversas situações. E, principalmente, porque esta clarificação representa, claramente, a inversão do ónus da prova. Ou seja, ao contrário do que acontece actualmente, em que são as vítimas a apresentar queixa junto das autoridades policiais, e apenas uma minoria processava judicialmente as instituições bancárias, a partir de agora terão de ser estas últimas a responsabilizar os clientes pelas perdas, recorrendo à via judicial, se for necessário.

Contudo, em relação à responsabilidade dos clientes por dolo ou negligência grosseira, importa destacar que os tribunais nacionais e europeus têm tomado decisões em sentidos opostos, ora responsabilizando-os pelas perdas ora isentando-os de culpa, com base na sofisticação e nas circunstâncias em que estas ocorrem, não existindo jurisprudência fixada.

Consequências práticas

Uma das dúvidas que se coloca neste momento é a de saber se a decisão do Tribunal de Justiça vai ser amplamente adoptada pelas instituições de pagamento em futuras burlas. E a resposta só chegará com o tempo, admite Nuno Matos, presidente da Associação Sindical dos Juízes Portugueses (ASJAP). "Arrisco-me a dizer que as coisas podem mudar um pouco", tendo em conta que o acórdão "vem impor o reembolso obrigatório e rápido", e só depois "é que se vai discutir o que é que aconteceu", adianta em declarações ao PÚBLICO.

Mas também ressalva que, "provavelmente, os bancos podem adoptar uma posição de que isto é sempre fraude, e acabam por não devolver o dinheiro, ou que há sempre negligência grosseira, e têm de propor uma acção". Assim, aquele juiz refere que é preciso ver, "na prática, como é que os bancos e os clientes se vão comportar". Ainda assim, este juiz entende que "a ideia do acórdão é criar alguma proporcionalidade e algum equilíbrio, para que o cliente não seja sempre o lesado nestas matérias", uma vez que "o que se tem verificado é que quando as vítimas se dirigem aos bancos, o que estes lhes dizem é que devem apresentar queixa às autoridades, e depois logo se vê".

Relativamente a casos semelhantes que já se encontram a correr na justiça, o presidente da ASJP considera que "o acórdão pode ser invocado como um precedente judiciário e os tribunais podem segui-lo", salvaguardando, no entanto, que apesar de "dar algumas linhas de decisão para casos futuros", não "será uma jurisprudência obrigatória geral".

Gonçalo Guimarães, advogado associado da Antas da Cunha Ecija, defende que "a decisão do Tribunal de Justiça é vinculativa para todos os tribunais nacionais chamados a decidir uma questão semelhante. Assim, é correcto dizer que há, ou deve haver, uma aplicação imediata da interpretação fixada pelo Tribunal de Justiça aos processos nacionais em que esteja em causa a mesma questão jurídica". Ainda assim, em termos práticos, considera que "é prudente que os advogados juntem o acórdão ou invoquem expressamente a sua aplicação, explicando por que razão é relevante para o caso concreto".

Para este advogado, focado na área de União Europeia e Concorrência, a partir de agora, os clientes não deverão ter de recorrer ao tribunal para obter o reembolso imediato quando a operação não foi autorizada e foi comunicada atempadamente, considerando que o acórdão "deixou claro que a alegação de negligência grosseira do cliente não permite ao banco recusar, sem mais, esse reembolso".

Porém, "se a instituição continuar a recusar o reembolso, o cliente poderá ter de apresentar reclamação junto da própria instituição, recorrer aos mecanismos de resolução alternativa de litígios, reclamar junto do Banco de Portugal ou, em último caso, avançar para tribunal". "A diferença é que, depois deste acórdão, a posição do cliente fica substancialmente reforçada (...), acrescenta, lembrando ainda que, "normalmente, quando o cliente não seja imediatamente reembolsado e não exista suspeita razoável de fraude validamente comunicada à autoridade judiciária, são devidos juros moratórios até ao reembolso efectivo".

Sobre a influência do referido acórdão na fixação de jurisprudência em Portugal, Ana Rita Campos, sócia contratada da Abreu Advogados, entende que "terá imensa, já que a acção pendente na Polónia é exactamente igual a muitas pendentes em Portugal e que, numa decisão de reenvio, o que o TJUE faz é interpretar, de forma praticamente autêntica, o Direito Comunitário". Nessa medida, antecipa "que o modelo de litigância nestes casos vá ser profundamente alterado, deixando de ter de ser os clientes/consumidores a intentarem acções contra os bancos que, na maioria dos casos, têm vindo a ser decididas contra aqueles".

Para aquela jurista, "a diferença fundamental é que terão de ser os bancos a dar esse passo e a provar a negligência grosseira do cliente", acrescentando que "este último aspecto já era assim (e não pode deixar de ser), mas a novidade é a de que, nos casos em que obrigação de devolução imediata, os bancos terão de enfrentar uma vaga de litigância que, até agora, onerava apenas os clientes".

Acesso a contas bancárias

Bancos tornaram a excepção para não reembolso "em regra"

Rosa Soares

Atenção dos clientes e alertas dos bancos são as melhores estratégias para evitar fraudes digitais que visam roubar credenciais

O caso que chegou ao Tribunal de Justiça da União Europeia (TJUE) foi remetido por um tribunal da Polónia, partindo do caso de uma cidadã que foi vítima de burla por *phishing*, na sequência da colocação para venda de um objecto numa plataforma de leilões. Segundo o resumo apresentado no processo, fazendo-se passar por um comprador, o burlão enviou-lhe uma hiperligação fraudulenta que reproduzia o *interface* da plataforma de leilões e, em seguida, a do banco. E, enganada, a cidadã comunicou os seus dados de acesso à plataforma do banco, o que permitiu ao infractor efectuar uma operação de pagamento não autorizada a partir da sua conta bancária. No dia seguinte, apercebendo-se da fraude, a vítima contactou o banco e apresentou queixa à polícia. Em causa estava a saída da sua conta de 705 euros, que o banco se recusou a reembolsar, alegando "negligência grosseira na sua obrigação de guardar com diligência o instrumento de pagamento e de não o disponibilizar a pessoas não autorizadas".

A recusa deu origem a um processo em tribunal contra o banco, que por sua vez esteve na base da remissão ao TJUE, para uma análise dos artigos 73 e 74 da Directiva 2015/2366 (que no caso da transposição portuguesa correspondem aos artigos 113 e 114, do Decreto-Lei n.o 91/2018), "quanto ao alcance da obrigação, que incumbe ao prestador de serviços de pagamento, de reembolsar imediatamente o montante de uma operação não autorizada".

Argumenta o tribunal de primeira instância que "os bancos não intentaram nos órgãos jurisdicionais polacos acções contra os consumidores relativas à obrigação de reembolsar o montante de operações não autorizadas com fundamento em negligência grosseira imputável ao ordenante".

"Em contrapartida, refere a mesma fonte, "terão sido muitas as acções intentadas por consumidores contra bancos devido ao não reembolso dos montantes das operações não autorizadas, concluindo quer "este fenómeno indica que a aplicação das excepções ao direito de reembolso pelos prestadores de serviços de pagamento [previsto para as situações em que a instituição tenha motivos razoáveis e devidamente documentados para suspeitar de fraude por parte do cliente] se tornou a regra no caso de operações não autorizadas".

Do *phishing* ao *smishing*

Com efeito, de uma forma geral, os prestadores de serviços de pagamento não procedem ao reembolso do montante das operações não autorizadas, pelo que são os ordenantes, em especial os consumidores, que se vêem obrigados a intentar uma acção judicial, refere ainda.

A decisão do TJUE relativamente aos referidos artigos da directiva vai no sentido de garantir um elevado nível de protecção dos consumidores, ao estabelecer que o prestador de serviços de pagamento está obrigado a proceder ao reembolso imediato, e num segundo momento, pode, se for o caso, reclamar junto do cliente o reembolso das perdas ocasionadas, se comprovar que estas resultam do facto de o cliente não ter cumprido, intencionalmente ou por negligência grosseira, as obrigações que lhe incumbem, designadamente a obrigação de proteger os seus dados de segurança personalizados.

Mas as burlas vão sendo cada vez mais sofisticadas, o que obriga a uma "atenção redobrada dos clientes e a uma informação ou alertas permanentes dos bancos, como já vêem fazendo", defende Nuno Matos, presidente da Associação Sindical dos Juízes Portugueses (ASJAP).

Os "ataques" mais frequentes visam, através da manipulação do cidadão, aceder ou roubar as credenciais de acesso às contas bancárias, como o cartão matriz, o acesso a códigos de confirmação de operações, muitas vezes a pretexto de actualização de dados, ou a resolução de falsos problemas nas contas.

Entre essas práticas está o *phishing*, que consiste no envio de comunicações electrónicas que aparentam ter origem em instituições legítimas, induzindo o utilizador a introduzir credenciais de autenticação numa página falsa que reproduz, com maior ou menor fidelidade, a aparência do sítio oficial do banco. Mais recentemente tem surgido o *pharming*, uma técnica em que o sistema informático do utilizador é previamente comprometido através da instalação de programas maliciosos (*malware*), sendo o cidadão redireccionado para páginas falsas, mas com aparência de autênticas.

Há ainda o *smishing*, que consiste na realização de um contacto fraudulento mediante mensagens SMS aparentemente provenientes da instituição financeira, ou o *vishing*, em que o contacto com o utilizador é efectuado por chamadas telefónicas, durante as quais o agente se apresenta como funcionário do banco ou de uma entidade pública. Ou ainda o *spoofing*, em que o agente dissimula ou falsifica elementos identificativos das comunicações electrónicas, telefónicas ou digitais, fazendo-as surgir perante o utilizador como provenientes de uma fonte legítima, com que o utilizador habitualmente se relaciona.

Ou o SIM *swaping*, que se traduz na duplicação ou clonagem do cartão SIM do utilizador, permitindo ao agente receber os códigos de autenticação enviados por SMS e concluir operações aparentemente validadas segundo os protocolos de autenticação forte. Ou, ainda mais recente, as burlas através da manipulação do WhatsApp, como aconteceu com o ministro da Defesa, Nuno Melo.

DADO RUVIC/REUTERS



Uma das burlas recentes é feita através do WhatsApp

IM. | Copyright licensed by Visapress | P. 3 of 3