ULP LAW REVIEW
REVISTA DE DIREITO DA UL-P

VOL. 17 N. 2 [2023]

VARIA

Ana Isa Meireles

A Minha E-Wallet: uma análise do Regime de Serviços de Pagamento Comentário ao acórdão do Supremo Tribunal de Justiça 379/21.0t8far.e1.S1 datado de 23.01.2024 cujo relator foi o senhor juiz conselheiro Nelson Borges Carneiro

ULP LAW REVIEW
REVISTA DE DIREITO DA UL-P
BI ANUAL | BI ANNUAL

CEAD FRANCISCO SUÁREZ
Fdcp Faculdade de Direito e Ciência Política
UNIVERSIDADE LUSÓFONA | CENTRO UNIVERSITÁRIO PORTO
ULPLR

A MINHA E-*WALLET*: UMA ANÁLISE DO REGIME DE SERVIÇOS DE PAGAMENTO

Comentário ao acórdão do Supremo Tribunal de Justiça 379/21. 0t8far.e1.S1 datado de 23.01.2024 cujo relator foi o senhor juiz conselheiro Nelson Borges Carneiro

ANA ISA MEIRELES[1]

DOI: 10.60543/UL-PLR-RDUL-P.V17I2.9731

RESUMO

Se, em tempos áureos, tudo ficava mais simples com uma simples carteira onde tínhamos um cartão multibanco, pensando que, na ousadia de comprar alguma coisa pelo computador teríamos que usar um cartão matriz agora nada disso é comum. O advento da tecnologia desafiou-nos e, com esses desafios, também a legislação teve que acompanhar a mudança. Os anglicismos parecem dificultar a nossa realidade e queremos tratar como presencial aquilo que, muitas vezes, está só camuflado: o facto de usarmos uma e-wallet não significa que estejamos a contratar presencialmente (muito pelo contrário!).

SUMMARY

If, in golden times, everything was simpler with a simple wallet where you had an ATM card, thinking that, if you dared to buy something on the computer, you would have to use an ATM card, now none of this is commonplace. The advent of technology has challenged us and, with these challenges, legislation has also had to keep pace with change. Anglicisms seem to hinder our reality and we want to treat as face-to-face what is often just camouflaged: the fact that we use an e-wallet doesn't mean that we are contracting in person (quite the opposite!).

1 Nascida em Davos-Platz na Suiça é, hoje, Advogada, Mestre em Direito dos Contratos e da Empresa e Doutora em Ciências Jurídico-Privatísticas. Além disso é Professora Auxiliar na Universidade Lusófona (Porto), Professora Convidada na Escola de Direito da Universidade do Minho, investigadora no CEAD e no JUSGOV, e formadora. Email: isa.meireles@ulusofona.pt ORCID: https://orcid.org/0000-0002-8942-3768.

1. O REGIME JURÍDICO DOS SERVIÇOS DE PAGAMENTO E DA MOEDA ELETRÓNICA

O modo com que nos relacionamos e, também, fazemos pagamentos está cada vez mais facilitado. Esta facilidade, com termos como NFT e tokenização, transporta-nos para vinculações quase por osmose, impondo conhecimento técnico e informático (bem como consciencialização) que tudo o que é fácil (aparentemente) trás muitos desafios.

O DL n.º 91/2018, de 12 de Novembro regula o regime jurídico dos serviços de pagamento e da moeda eletrónica.

Importante será refletir que este regime jurídico implica uma noção de consumo (ou seja, de uma relação jurídica de consumo) com um conceito de consumidor restrito, a saber "[uma] pessoa singular que atua, nos contratos de serviços de pagamento e nos contratos celebrados com os emitentes de moeda eletrónica abrangidos pelo presente Regime Jurídico, com objetivos alheios às suas atividades comerciais, empresariais ou profissionais", conforme artigo 2.º alínea f) do referido DL. Nessa medida, o uso predominantemente aos contratos celebrados com os emitentes de moeda eletrónica terão que ser de uso pessoal: aferir-se a razão da compra e/ou da transação é o *quid* que soluciona a aplicação.

Este artigo 2.º contém, também, mais definições, no qual encontramos a definição de *moeda eletrónica*, dizendo-se, na alínea ff), que é "[o] valor monetário armazenado eletronicamente, inclusive de forma magnética, representado por um crédito sobre o emitente e emitido após receção de notas de banco, moedas e moeda escritural, para efetuar operações de pagamento na aceção da alínea ii) e que seja aceite por pessoa singular ou coletiva diferente do emitente de moeda eletrónica".

Nos termos do artigo 4.º dispõe-se, concretamente, que a regulação específica recai sobre os seguintes serviços de pagamento, a saber:

a) Serviços que permitam depositar numerário numa conta de pagamento, bem como todas as operações necessárias para a gestão dessa conta;

b) Serviços que permitam levantar numerário de uma conta de pagamento, bem como todas as operações necessárias para a gestão dessa conta;

c) Execução de operações de pagamento, incluindo a transferência de fundos depositados numa conta de pagamento aberta junto do prestador de serviços de pagamento do utilizador ou de outro prestador de serviços de pagamento, tais como:

i) Execução de débitos diretos, incluindo os de carácter pontual;

ii) Execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante;

iii) Execução de transferências a crédito, incluindo ordens de domiciliação;

d) Execução de operações de pagamento no âmbito das quais os fundos são cobertos por uma linha de crédito concedida a um utilizador de serviços de pagamento, tais como:

i) Execução de débitos diretos, incluindo os de carácter pontual;

ii) Execução de operações de pagamento através de um cartão de pagamento ou de um dispositivo semelhante;

iii) Execução de transferências a crédito, incluindo ordens de domiciliação;

e) Emissão de instrumentos de pagamento ou aquisição de operações de pagamento;

f) Envio de fundos;

g) Serviços de iniciação do pagamento;

h) Serviços de informação sobre contas.

As exclusões encontram-se no artigo 5.º.

É importante, em torno de todo este DL, perceber-se o que é a autenticação forte onde, nos termos do artigo 2.º, se impõe que haja uma "[uma] autenticação baseada na utilização de dois ou mais elementos pertencentes às categorias conhecimento (algo que só o utilizador conhece), posse (algo que só o utilizador possui) e inerência (algo que o utilizador é), os quais são independentes, na medida em que

a violação de um deles não compromete a fiabilidade dos outros, e que é concebida de modo a proteger a confidencialidade dos dados de autenticação".

Mas quando é que esta autenticação forte é exigida? Afinal, olhando o artigo 104.º, quando alguém aceda em linha à sua conta de pagamento, ou inicie uma operação de pagamento eletrónico, ou realize uma ação, através de um canal remoto, que possa envolver um risco de fraude no pagamento ou de outros abusos, é exigida esta autenticação.

Diz-se exigida porque o facto de a lei o exigir, infelizmente, não significa que o prestador de serviço a aplique e, daí, se levantem tantas questões.

Esta autenticação forte é exigida, assim, em pagamentos online com cartão. Ou seja, implica-se que inexista um pagamento físico (por exemplo um terminal multibanco, designado TPA [terminal de pagamento automático]).

Pelo que falaremos destes pagamentos online, ou seja, com exigência de autenticação forte aquando de contratos celebrados à distância.

Ora, portanto, conforme até instruções do Banco de Portugal, obviamente que em situações de pagamento contactes ou MBWAY (com *qr code*) não estaremos no campo da exigibilidade de dupla autenticação.

2. *HOMEBANKING*

Antes de avançarmos será conveniente compreendermos e esmiuçarmos, concretamente, o conceito de homebanking. Segundo o Banco de Portugal, no seu campo de glossário[2] o *homebanking* ou Banco on-line é o "[canal] facultado pela maioria das instituições de crédito para interação com os seus clientes através da internet e que, mediante a adoção de medidas de segurança adequadas, possibilita o acesso aos serviços oferecidos pela instituição a qualquer hora e em qualquer lugar".

Nessa medida, estaremos a falar, então, de um website disponibilizado pela própria entidade bancária e/ou a sua aplicação.

Não podemos falar de *homebanking* de pagamentos gerais online, mas, sim, de pagamentos e transações realizadas dentro do canal oficial do banco (seja um website, seja uma APP oficial). Por isso, só por aqui, parece que caímos num erro de convicção geral.

Como reagiria a maioria da população se soubesse que os pagamentos que faz, por exemplo, numa plataforma booking, ou com a sua wallet (já chegaremos lá) ou o simples pagamento de um uber são, afinal, inseguros? Claro, não estamos a falar de situações onde se cria um mbnet ou paypall limitado de valor mas, sim, da colocação online de dados de cartão bancário (seja ele de débito ou de crédito).

Curioso será dizer que quando acedemos ao *homebanking* temos dois momentos chave: o momento da adesão e o momento da transação subsequente (ou seja, da efetiva utilização). Sabe-se que, claramente, no momento da adesão será aplicada autenticação forte para se perceber se o utilizador que está a aderir a este serviço de facilitismo respeita o conhecimento, posse e inerência exigidos. Mas e no momento posterior? Ou seja, após a adesão, quando utilizamos efetivamente a plataforma de *homebanking*? Exige-se esta dupla autenticação? Sim. Exige. Assim, é claro que quer o acesso à conta de pagamento através da internet, quer a realização de uma operação/transação de pagamento virtual obrigam, por aplicação da legislação, à aplicação de autenticação forte do cliente.

Não podemos, contundo, confundir *homebanking* com uma série de pagamentos online – que também nem sempre

2 Disponível em https://clientebancario.bportugal.pt/pt-pt/glossario/b, [consultado em 10.10.2024].

serão considerados feitos através da e-*wallet* tradicional e associada a dispositivos como os da *apple*.

3. CONCEITO DE E-WALLET'S

Temos, atualmente, duas realidades de e-wallets. As carteiras digitais, nada mais sendo senão isto, podem estar introduzidas no telemóvel ou num qualquer outro dispositivo (ipad, tablet, computador).

Na primeira realidade, uma carteira guardada no telefone ela terá que implicar a instalação de uma aplicação: daí que se falem em wallets Google Pay, Apple Pay e MBWay. Onde, nestas aplicações, se guardam dados de cartões bancários. A carteira digital nada mais é do que a nossa carteira física mas transporta para uma realidade digital. É lá que estão guardados os nossos cartões, com os dados dos mesmos, o que não implica que os mesmos possam ser utilizados sem limites (fisicamente, aliás, até temos o *contactless* que pode permitir pagamentos sem código até determinado montante). Com estas aplicações e através de uma simples aproximação do dispositivo a um TPA, a transação pode ser aprovada desde que o utilizador tenha um meio de autenticação forte (não a colocação do PIN, mas, por exemplo, a leitura facial [FACE ID] ou a impressão digital).

Estes pagamentos implicam uma proximidade a um TPA para ocorrerem com uma aproximação.

Coisa diferente é a carteira que ocorre no domínio totalmente digital. Ou seja, pagamentos realizados em páginas digitais através de dados guardados, por exemplo, no google – numa carteira digital existente no próprio website do google onde os cartões mais utilizados ficam guardados e armazenados (sejam eles quais forem).

Não basta estar lá o cartão para haver uma simples transação. É preciso algo mais, dado que se trata de um pagamento online.

O Banco de Portugal é muito claro ao indicar que, nestas transações "[por] se considerar que as operações de pagamento remotas implicam um maior risco de fraude do que as operações presenciais, os PSP/ bancos têm de garantir que, neste tipo de operações, a autenticação forte do cliente inclui um elemento adicional que associe de forma dinâmica a operação em causa ao montante e beneficiário específico[3]". Ora, nestas mesmos temos que voltar a verificar uma autenticação forte. E volte a realçar-se que não se exige autenticação forte só no momento de adesão a esta facilidade de pagamento mas, sim, no momento da realização concreta da operação. É uma obrigação do prestador de serviço de pagamento/banco fazê-lo para segurança e validade da operação.

4. ÓNUS DA PROVA

Existindo uma operação que não tenha sido consentida pelo titular do cartão caberá ao prestador de serviço de pagamento/banco provar que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento.

Ou seja, nos termos do artigo 113.º do DL n.º 91/2018, de 12 de Novembro, o utilizador de serviços de pagamento tem apenas que i) negar ter autorizado a operação de pagamento executada ou ii) alegar que a operação não foi corretamente efetuada.

3 Consultado no Guia de Autenticação Forte, disponível em https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/guia_autenticacao_forte.pdf, a 11.10.2024.

Caso esta operação tenha sido iniciada através de um prestador do serviço de iniciação do pagamento, nos termos do n.º2 do artigo 113.º do DL n.º 91/2018, de 12 de Novembro "[recai] sobre este último o ónus de provar que, no âmbito da sua esfera de competências, a operação de pagamento foi autenticada e devidamente registada, e não foi afetada por qualquer avaria técnica ou por outra deficiência relacionada com o serviço de pagamento por si prestado", protegendo-se, sempre, assim, o utilizador do serviço.

Em toda a conduta do utilizador de serviços de pagamento o mesmo não poderá olvidar que tem, na sua esfera jurídica, obrigações. Nos termos do 110.º do DL n.º 91/2018, de 12 de Novembro este utilizador tem a obrigação de "[utilizar] o instrumento de pagamento de acordo com as condições que regem a sua emissão e utilização, as quais têm de ser objetivas, não discriminatórias e proporcionais; e, ainda, [comunicar], logo que tenha conhecimento dos factos e sem atraso injustificado, ao prestador de serviços de pagamento ou à entidade designada por este último, a perda, o furto, o roubo, a apropriação abusiva ou qualquer utilização não autorizada do instrumento de pagamento".

Verificadas todas estas situações é ao prestador de serviços de pagamento/banco que incumbe provar que o utilizador de serviço agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira as suas obrigações, sendo que, em todo o caso, terá que provar que cumpriu com a autenticação forte e dupla exigida.

5. O ACÓRDÃO

No acórdão em análise debatem-se questões de *home-banking* e do ónus da prova *supra* referido.

Em ação declarativa de condenação uma utilizadora de serviços de pagamento, cliente bancária, peticionou um pedido de indemnização contra um prestador de serviços de pagamento/banco, designadamente a que este último fosse condenado a pagar-lhe "[a] quantia de € 61.064,89 a título de indemnização por danos patrimoniais, acrescida de juros calculados à taxa legal, contados desde a citação e até integral pagamento, bem como o pagamento da quantia de € 3.000,00, a título de indemnização por danos não patrimoniais, acrescida de juros calculados à taxa legal e contados desde a data da citação e até integral pagamento".

A relação material controvertida foi fundamentada com a titularidade de uma conta bancária na agência do dito prestador de serviço de pagamento/banco. Foi explicado que em julho de 2020 tentou várias vezes fazer login na plataforma online disponibilizada pelo banco, sem sucesso, e, quando conseguiu, verificou que tinham sido realizados pagamentos e transferências bancárias, num total de € 56.990,00, para destinatários que lhe eram totalmente desconhecidos e, ainda, operações não autorizadas. Aquando da imediata percepção dos factos foi à agência do banco onde lhe terão indicado tratar-se de fraude e, de imediato, lhe indicaram que teria que apresentar participação criminal. O banco, ainda assim, não devolveu todo o valor, limitando-se a devolver €2.597,10.

Na referida ação o prestador de serviços/banco indicou que as transferências e pagamentos foram validados com as credenciais da utilizadora, havendo, por si, um cumprimento de todas as obrigações técnicas de segurança, imputando à utilizadora a culpa dado que utilizava nas operações um computador desprotegido e obsoleto.

Estes factos remontam a 2020, ou seja, antes das alterações ao regime jurídico dos serviços de pagamento e da moeda eletrónica.

Em primeira instância foi dada razão à utilizadora de pagamento.

Já em segunda instância, por acórdão do Tribunal da Relação de Évora[4], foi revogada a decisão e atribuída credibilidade à prova do prestador de serviço/banco.

Recorrendo-se para o Supremo Tribunal de Justiça manteve-se o acórdão do Tribunal da Relação de Évora com uma fundamentação de que, na redação, à data dos factos, do regime dos sistemas de pagamento, frisando-se que "[caso] um utilizador de serviços de pagamento negue ter autorizado uma operação de pagamento executada, ou alegue que a operação não foi corretamente efetuada, incumbe ao respetivo prestador do serviço de pagamento fornecer prova de que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência – art. 70º/1, do RSP".

Ora, o que é certo é que a utilizadora de serviços se negou a ter autorizado uma operação de pagamento.

Concluiu-se, e bem, que estávamos perante uma relação de *homebanking* e que "[para] o efeito os bancos fornecem aos seus clientes senhas de acesso pessoais, bem como cartões matriz constituídos por uma infinidade de composições numéricas, que normalmente são solicitadas no final de cada operação efetuada por meios telemáticos e por forma a autenticá-la, já que esse cartão matriz deverá apenas ser do conhecimento do cliente, único a poder utilizá-lo, não lhe sendo permitido fornecer nenhum dos dados nele insertos a terceiros, uma vez que, quer o protocolo da página bancária, quer o tráfego de toda a informação nela processada, o que inclui as sobreditas senhas de acesso, são encriptadas, tornando quase impossível um terceiro obter ou alterar a informação depois de enviada".

É claro que ficou claro que recaía sobre o prestador de serviços/banco o o risco das falhas e do deficiente funcionamento do sistema, destacando-se que é este mesmo que tem ónus da prova de que a operação de pagamento não foi afetada por avaria técnica ou qualquer outra deficiência.

A utilizadora alegou que não autorizou os movimentos que resultaram as operações de pagamento e, ainda, que nem sequer as realizou ou conhecia. Claro que, conforme se extrai do teor do acórdão em causa"[a] execução da ordem exige também que o cliente tenha sido autenticado pelo prestador do serviço através de um procedimento que lhe permite verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador".

Portanto "[se] o utilizador de serviços negar ter autorizado a operação, ou alegar que ela foi incorretamente efetuada, cabe ao prestador dos serviços de pagamento provar que a operação de pagamento foi autenticada, devidamente registada e contabilizada e que não foi afetada por avaria técnica ou qualquer outra deficiência do serviço prestado pelo prestador de serviços de pagamento".

O que é certo é que o resultado atingido está, de facto, na prova, dado que, no libelo dos factos dados como provados, concluiu-se positivo "[que] os pagamentos e transferências foram efetuados com utilização do Código de Utilizador da autora, confirmados com duas posições aleatórias do NIF e com a introdução dos Códigos de Autorização enviados por "SMS" para o telemóvel n.º 962 (facto provado n.º 23), número esse que fora indicado pela gerente da autora ao réu".

Claro que os riscos "[da] falha do sistema informático utilizado, bem como dos ataques cibernautas ao mesmo, têm de correr por conta dos bancos, por a tal conduzir o disposto no art. 796º/1, do CCivi".

4 Com o n.º 379/21.0T8FAR.E1, relatado por CRISTINA DÁ MESQUITA, datado de 12.07.2023, disponível em www.dgsi.pt.

Mais uma vez, tudo está na prova, sendo que se provou, também, "[que] *o site de homebanking do Banco não sofreu, no período em que foram feitas as transferências da conta do Autor nenhum ataque informático ou qualquer tentativa de intrusão ou utilização ilícita por parte de terceiros (facto provado nº 44)".*

6. CONCLUSÕES

Em primeira linha, no caso de *homebanking* teria também que se indagar se a utilizadora do serviço quando acedeu ao *homebanking* teve a autenticação forte aplicada devidamente e, ainda, se as referidas transações dos 90 dias estavam dentro do período em que se permite uma autenticação mais simples: sendo que após esses 90 dias é exigida nova autenticação forte.

E estes pagamentos, as operações, tiveram uma autenticação forte? É indicado no acórdão que "[que] os pagamentos e transferências foram efetuados com utilização do Código de Utilizador da autora, confirmados com duas posições aleatórias do NIF e com a introdução dos Códigos de Autorização enviados por "SMS" para o telemóvel n.º 962 (facto provado n.º 23), número esse que fora indicado pela gerente da autora ao réu". Ou seja, fala-se do cartão matriz. O cartão matriz desde 14 de setembro de 2019 só pode ser utilizado como complemento da autenticação forte e não como autenticação forte quando não se requeira esta (o que vai depender da primeira linha), isto, tudo, apenas para o *homebanking*.

Como tal, em segunda linha, havendo a alegação de não autorização nem consentimento, era sim, ao banco/prestador de serviço que cabia a prova de que: houve uma devida autenticação no *homebanking* (o que se levanta aqui em primeira linha) e, ainda, fazer prova de que não houve nenhuma avaria técnica ou qualquer deficiência do serviço prestado. Consultada a tokenização o n.º para onde foi enviada a dita mensagem correspondia ao telefone utilizado pela autora? Claro que, esses documentos, falariam por si, desconhecendo-se os meandros das provas e das alegações, compreende-se a posição sufragada pelo douto Supremo Tribunal de Justiça na medida em que só as provas podem guiar um processo.

Nas e-wallets a coisa ainda é mais complexa, dado que os anglicismos nos complicam a visão das coisas mas é simples: a e-wallet nada mais é do que a nossa carteira física, transportada para este mundo de novos desafios online.