
# Contratos de *E-Banking* e a Responsabilidade nas Operações não Autorizadas:

# o Caso do *MBWay*

Mestrado em Solicitadoria de Empresa

Rita Bernardino Lopes

Leiria, setembro de 2023

escola superior de tecnologia e gestão
instituto politécnico de leiria

# Contratos de *E-Banking* e a Responsabilidade nas Operações não Autorizadas:

# o Caso do *MBWay*

Mestrado em Solicitadoria de Empresa

Rita Bernardino Lopes

Dissertação sob a orientação da Professora Doutora Susana Catarina Simões de Almeida

Leiria, setembro de 2023

# Originalidade e Direitos de Autor

A presente dissertação é original, elaborada unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para a elaborar.

*Aos meus pais e irmão, Luís Henrique*.

# Agradecimentos

A elaboração da presente dissertação apenas foi possível realizar com o apoio daqueles que foram indispensáveis para o contributo da sua conclusão.

Primeiramente, dirijo uma palavra de profundo agradecimento à Professora Dra. Susana Almeida que, perante uma caminhada tão longa, sempre esteve presente, com disponibilidade e prontidão para que este estudo pudesse ser concluído com o rigor exigido.

Aos meus pais, pela permanente dedicação e inspiração que fizeram com que fosse possível levar a cabo mais um desafio.

Ao Luís Henrique, irmão, mas acima de tudo amigo, pela motivação, companheirismo e alegria, que se tornou força por tantas vezes.

A toda a minha família e amigos, pois, também, sem eles nada disto seria possível.

A todos, o meu muito obrigado.

# Resumo

O mundo encontra-se em mudança e estas ocorrem de "mãos dadas" com a evolução.

Uma das principais evoluções nas últimas eras foi a sociedade de informação e, em especial, a área financeira, que foi aquela que, talvez, mais acompanhou a mudança da nova era digital. O progresso, seja em que área for, está sempre associado a novos riscos e, neste caso, a novos crimes, os informáticos.

Durante o presente estudo será feita uma análise à evolução dos sistemas bancários ao longo dos últimos anos, nomeadamente do melhoramento dos serviços que originaram a possibilidade de aceder ao banco de forma completamente digital. Associado a este desenvolvimento digital foram surgindo novas formas de crime informático, onde consideraremos como principais o *phishing*, *pharming* e *spyware*.

De tal fraude, surgem prejuízos, e será precisamente sobre eles e sobre quem sai responsabilizado pelos mesmos que nos focaremos ao longo de uma grande parte do presente trabalho. A que direitos e deveres estão as partes desta relação adstritas e de que modo o seu incumprimento alterará o curso desta responsabilidade.

Ressalvar que estes direitos e deveres, a par com a segurança na utilização do serviço de pagamento, são das principais alterações do novo Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica.

O presente estudo servirá, essencialmente, para perceber sobre quem incorrem as responsabilidades nos casos de fraude no *E-Banking* e, ainda, de que forma esse ato ilícito é gerido ao nível das aplicações de pagamento, mais concretamente, no caso do MBWay.

**Palavras-chave:** *E-Banking*; responsabilidade por fraude informática; *phishing*; *pharming*; *MBWay*.

# Abstract

The world is changing and this is happening hand in hand with evolution.

One of the main developments in recent eras has been the information society and, in particular, the financial sector, which has perhaps kept pace with the changes of the new digital age. Progress, in whatever area, is always associated with new risks and, in this case, new crimes, informatic crimes.

This study will analyze the evolution of banking systems over the last few years, in particular the improvement of services that have led to the possibility of accessing the bank in a completely digitally way. Associated with this digital development, new forms of computer crime have emerged, the main ones were the phishing, the pharming and the spyware.

Such fraud leads to damage, and it is precisely this damage and who will be held responsible for it that we will focus on for a large part of this work. What rights and duties are attached to the parties in this relationship and how their failure to comply will change the course of this responsibility.

It should be noted that these rights and duties, along with security in the use of the payment service, are among the main changes in the new Legal Framework for Payment Services and Electronic Money.

This study will essentially serve to understand who is responsible for cases of fraud in E-Banking and also how this illegal act is managed in payment applications, more specifically in the case of MBWay.

**Keywords:** *E-Banking*; responsibility for computer fraud; *phishing*; *pharming*; *MBWay*.

# Índice

# Lista de siglas e abreviaturas

| | |
|---|---|
| Ac. | Acórdão |
| ACEPI | Associação da Economia Digital |
| al. | alínea |
| APWG | Anti-Phishing Working Group |
| art. / arts. | artigo / artigos |
| BP | Banco de Portugal |
| CC | Código Civil |
| CCG | Cláusulas Contratuais Gerais |
| cf. | conferir |
| CP | Código Penal |
| DL | Decreto-Lei |
| DSP | Diretiva Serviços de Pagamento |
| ed. | edição |
| ESTG | Escola Superior de Tecnologia e Gestão |
| IBM | International Business Machines Corporation |
| LC | Lei do Cibercrime |
| n.º | número |
| PNB | Produto Nacional Bruto |
| *Op. cit.* | Obra citada |
| p. | página |
| RGPD | Regulamento Geral sobre a Proteção de Dados |
| RGICSF | Regime Geral das Instituições de Crédito e Sociedades Financeiras |
| RJSPME/DSP2 | Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica/ Diretiva de Serviços de Pagamento 2 |
| ss. | seguintes |
| STJ | Supremo Tribunal de Justiça |
| TIC | Tecnologias da Informação e Comunicação |
| TRC | Tribunal da Relação de Coimbra |
| TRG | Tribunal da Relação de Guimarães |

| | |
|---|---|
| TRL | Tribunal da Relação de Lisboa |
| TRP | Tribunal da Relação do Porto |
| UE | União Europeia |
| Vol. | Volume |
| WWW | World Wide Web |

# Introdução

Os novos vintes, e com isto referimo-nos aos últimos três anos aproximadamente, implicaram uma evolução de fenómenos sociais nas mais diversas áreas, entre outros, encontra-se uma aceleração considerável no que toca ao *e-commerce* e aos pagamentos à distância, que inevitavelmente acabam por estar quase sempre relacionados.

Foram vários os estudos realizados em Portugal[1], e não só, que demonstraram o impacto que a Covid-19 veio a ter no impulsionamento deste crescimento de comércio *on-line* e meios de pagamentos alternativos, abrindo assim novas possibilidades aos consumidores. Não obstante este desenvolvimento, junto com uma epidemia na área da saúde veio também uma epidemia de fraudes informáticas que são, atualmente, uma das maiores preocupações dos nossos reguladores, tribunais e demais entidades de controlo. Cresce assim a atenção da cibersegurança e proteção dos direitos e deveres dos consumidores digitais.

Pese embora o *e-commerce* e *E-Banking* não sejam temas recentes, facto é que nos últimos três anos o crescimento de ambos foi completamente inesperado, sendo a área bancária aquela que mais se destacou no que toca à digitalização[2]. Antes de maiores desenvolvimentos, cumpre esclarecer que ao longo do presente estudo o banco *on-line* será designado por nós como *E-Banking*, expressão que decidimos adotar face ao crescimento exponencial do conceito do "E" enquanto denominador comum entre os termos relacionados com o formato *on-line* e com o qual mais concordamos.

É precisamente quanto ao fenómeno do *E-Banking*, bem como quanto à responsabilidade pelas operações fraudulentas que ocorrem associadas a este, que nos debruçaremos ao longo da presente dissertação.

[1] Veja-se neste sentido, por exemplo, o estudo da SIBS que analisa o crescimento do consumo online em 365 dias de pandemia. Disponível para consulta em https://www.sibsanalytics.com/noticias/relatorio-365-dias-de-pandemia/ , consultado a 22-09-2023.

[2] Conforme notícia no site sapo - marketeer intitulada "Pandemia acelera digitalização da banca: mobile é o canal que mais cresce em Portugal. Disponível para consulta em https://marketeer.sapo.pt/pandemia-acelera-digitalizacao-da-banca-mobile-e-o-canal-que-mais-cresce-em-portugal/, consultado em 22-09-2023.

Desta feita, o presente trabalho versará sobre cinco grandes capítulos, inicialmente será analisada a evolução da sociedade digital, com enfoque na evolução do Direito Bancário, sendo posteriormente feita uma caracterização destes contratos de *E-Banking*.

Posteriormente, teremos a oportunidade de aprofundar a temática da fraude informática no âmbito do *E-Banking*, em concreto o *phishing*, o *pharming* e, finalmente, o *spyware*.

No seguimento do estudo destes esquemas ilícitos, aprofundaremos a responsabilidade por estes atos, nomeadamente, sobre quem recaem as responsabilidades de fazer prova e de reembolsar os prejuízos decorrentes de tais utilizações indevidas.

Num curto espaço de tempo, a par com o melhoramento e crescimento dos meios de pagamento à distância, rapidamente foram surgindo aplicações, geridas por terceiros – ou seja, não pela entidade bancária –, que foram ganhando força entre os consumidores. Assim, de forma brusca, uma dessas aplicações, no caso o MBWay, passa a figurar nos nossos dias como um meio "normal" de pagamento. Será precisamente sobre esta forma alternativa de pagamento à distância, que nos dedicaremos no último capítulo deste trabalho. Ali, para além de uma noção geral desta aplicação, analisaremos, igualmente, a responsabilidade pelos atos fraudulentos decorrentes da sua utilização.

Para realizar o presente trabalho, socorremo-nos da revisão de doutrina relevante neste domínio, da análise e reflexão crítica de legislação, bem como da consulta de jurisprudência.

Importa referir, sem mais delongas, que o presente estudo abarcará uma análise civil e não penal.

# 1. A Sociedade Digital e o Direito Bancário

## 1.1. Resenha Histórica

Vivemos, atualmente, na era da *World Wide Web*, onde, a cada momento, se verifica uma nova evolução a nível tecnológico. Em bom rigor, e de acordo com Macedo (Macedo, 2005, p. 897), um Estado que não consiga acompanhar o contínuo desenvolvimento das tecnologias será, inevitavelmente, um Estado mais fraco, pois é, precisamente, na capacidade de acompanhamento e utilização destas que se encontra a sobrevivência e destacamento de cada país[3].

Várias têm sido, ao longo das décadas, as revoluções na sociedade da informação. No entanto, aquela a que se dará mais enfoque, neste trabalho, será a sua quarta, momento em que existe um incessante avanço na conversão da tecnologia "habitual" para uma revolução digital (Amaral, 2007). Este "novo" formato tem uma maior visibilidade a partir da década de 70, altura em que esta se revela ser, essencialmente, um modelo de desenvolvimento económico. A sua aplicação tem conduzido à transformação das atividades ditas tradicionais, como, por exemplo, o "…correio, o comércio, a publicidade ou o ensino, em atividades realizadas em ambiente virtual…" (Macedo, 2005, p. 893), o que leva a que, consequentemente, se tenha vindo alterar, também, a forma de contratar.

Uma área que em nada ficou indiferente a esta transição foi o sector bancário, que também sofre uma verdadeira mutação de relações que passam a envergar as vestes do mundo virtual. Ora, é precisamente nesta conjuntura que nos debruçaremos neste primeiro ponto de estudo, ou seja, perceber em que consiste esta dita sociedade da informação e de que forma esta, com o correr dos tempos, foi alterando o procedimento bancário até chegarmos ao momento atual, momento em que somos dominados pelas tecnologias e passamos a travar as relações à distância. Importa referir, antes de mais extensos desenvolvimentos, que atualmente esta "forma" de sociedade é defendida por alguns autores[4], posição com a qual concordamos, como sociedade digital, sendo que, em bom rigor, é devido à evolução

[3] Para maior aprofundamento sobre o tema, veja-se Bóia, J. (2003). *Educação e Sociedade: Neoliberalismo e os desafios do futuro*. Lisboa: Edições Sílabo.
[4] Por exemplo, Schwalbach, J. G (2021). *Direito Digital.* Coimbra. Almedina.

tecnológica e ao mundo digital que hoje temos acesso a quantidades, outrora inimagináveis, de informação em curtos espaços de tempo.

Toda esta evolução e desenvolvimento fizeram com que vários pensadores da comunidade científica criassem modelos teóricos que permitiram compreender, de uma melhor forma, este mundo novo que se edificava perante nós[5]. Foram, então, surgindo ao longo das décadas, várias denominações relativas ao tema, tais como o "informatismo", a "informacionalização", a "economia da informação" ou a "sociedade da informação" (Macedo, 2005, p. 893). Como reforça Lurdes Macedo, o conceito de sociedade da informação era aquele que parecia ter um maior alcance, uma vez que, numa só conceção, se consegue abranger cada um dos restantes, é, talvez, por esta razão que por largos anos tenha sido este o conceito adotado pela generalidade da comunidade (Macedo, 2005, p. 893). Presentemente muitos ainda a invocam com essa mesma expressão, outros, como já enunciado, preferem apelidá-la como digital. Verdadeiramente, o que temos é uma sociedade da informação, caracterizada pela sua revolução a nível de transmissão de informação, associada à tecnologia, o que só veio privilegiar, tornando assim a sua transmissão mais rápida e acessível para todos.

Frank Webster acredita que a necessidade de delimitar estes conceitos se foi devendo ao facto da abrupta ascensão das TIC e a informatização da vida social no geral. É, por essa razão, que na sua obra enuncia cinco critérios de identificação de existência de uma sociedade da informação, sendo esses o critério tecnológico, económico, ocupacional, espacial e cultural (Webster, 1995, p. 8).

Segundo o autor, o critério tecnológico assenta na já anteriormente referida expansão das TIC, onde o desenvolvimento, armazenamento e transmissão de informação em todos os campos da vida social (escola, lojas, fábricas, bancos, etc.) nunca estiveram tão avançados, sendo assim estabelecido um paradigma técnico-económico para o século XXI.

Já o critério económico vem na senda do anterior, sendo que se prevê que a informação e o conhecimento se encontrem na base da economia moderna, quer isto dizer que cada vez mais as indústrias da informação contribuem para o Produto Nacional Bruto (PNB), ou seja, quanto maior for a percentagem destas indústrias no PNB, mais perto um país se encontra de uma dita sociedade da informação.

[5] *Vide* Webster, F. (1995) *Theories of Information Society* (4ª ed.). London: Routledge.

Outra forma de avaliarmos a existência de uma sociedade como a estudada será observando o critério ocupacional, segundo o qual estaremos perante a mesma quando os trabalhos relacionados com a informação forem em maior quantidade do que aqueles em que esta não é primordial. Tomemos como exemplo disso os agricultores. Webster define tal critério como: "The decline of manufacturing employment and the rise of service sector employment is interpreted as the loss of manual jobs and its replacement with white-collar" (Webster, 1995, p. 14). Fazendo uma análise deste critério em Portugal, podemos, desde já, concluir que tal já se verifica entre a maioria dos nossos trabalhadores[6].

A conceção espacial contém em si uma "diferente" noção geográfica de "espaço", enfatizando a importância das redes que vêm ligar, em tempo real, locais que podem ser geograficamente distantes num só espaço, facilitando assim a comunicação, o comércio e, inevitavelmente, a economia.

A última dimensão apresentada pelo autor é relativa à definição cultural. Segundo Webster, esta será provavelmente a dimensão mais facilmente reconhecida por todos. No entanto, é, simultaneamente, a de maior apreensão (Webster, 1995, p. 19). Nesta última interpretação, pretende-se destacar a quantidade de informação que corre nos dias de hoje, nunca, em qualquer outro momento, existiu uma tamanha dimensão de informação disponível a todos, e é, precisamente, relativamente a esta possibilidade de acesso a que este último critério dá relevância.

Em suma, apesar de todas as possíveis conceções serem de possível aplicação, cada uma delas, à sua maneira, tem algum ponto em que pode ser discutível[7], dificultando assim uma afirmação perante apenas uma das sugeridas. De entre as várias dúvidas enunciadas, destacamos aquela que mais nos suscitou, também a nós, e que consideramos atual, não obstante tantos anos terem volvido, ser uma certa incerteza: será que uma sociedade da

[6] Uma forma de conseguirmos chegar a esta conclusão será fazendo uma avaliação dos cursos superiores que vão tendo um maior número de alunos inscritos. Posteriormente, e após essa avaliação faz-se uma análise relativa ao número de licenciados desempregados e quais as suas áreas. De acordo com uma notícia no "O Jornal Económico", datada de 18 de julho de 2020, os cursos que continuam com um maior grau de ingressos e empregabilidade são referentes à área da saúde seguidos das áreas das engenharias, em especial da informática (Disponível para consulta em https://jornaleconomico.sapo.pt/noticias/conheca-os-cursos-com-mais-saida-em-portugal-614978 , consultado a 11-02-2021). Todos os anos o site http://infocursos.mec.pt/ faz uma retrospetiva das áreas com maior empregabilidade, provando assim que cada vez mais estamos perante uma sociedade da informação.

[7] Ao longo do seu estudo, Webster faz ainda referência a vários autores que merecem, igualmente, relevo no estudo desta matéria. Destacamos Daniel Bell e Manuel Castells.

informação, ou digital como preferimos designar, resultará, indiscutivelmente, em pessoas mais informadas?

Assim, e após o anteriormente apresentado, como forma de uma breve resenha histórica, podemos retirar várias ilações: uma das mais relevantes será a velocidade do avanço das novas tecnologias e em como vários conceitos foram, como já enunciado, alterados.

Não nos é permitido avançar sem, ademais, fazer uma referência de sobeja importância aos tempos de pandemia recentemente vivenciámos e que, de alguma forma, ainda se fazem sentir. Foi a 11 de março de 2020 que a Organização Mundial da Saúde veio decretar que o vírus SARSCOV-2, que provoca a doença de Covid-19, se tornava numa pandemia mundial. Com esta determinação várias foram as alterações que cada país teve de promover para tentar mitigar a expansão da doença. Podemos aqui elencar algumas das mais notórias: para além dos encerramentos dos espaços públicos, a passagem para os regimes de telescola e teletrabalho, a interação social que passou a realizar-se maioritariamente, para não dizer totalmente, através de meios eletrónicos e, consequentemente, o crescimento abrupto da utilização do e-commerce, bem como do *E-banking*, o ponto fulcral do nosso trabalho. Em Portugal, tal como no resto do mundo, verificou-se um aumento exponencial da utilização das tecnologias, que, por certo, se viram obrigadas – não as próprias mas as pessoas que com elas trabalham e as desenvolvem –, também elas, a renovarem-se e estarem o mais atualizadas e funcionais possíveis, uma vez que a Covid-19 impulsionou o uso do digital, introduzindo novas faixas etárias na sua utilização. De acordo com um estudo realizado pela Anacom, Portugal teve um crescimento na ordem do 55% desde que começou a pandemia, algo completamente inédito para Portugal[8]

Um exemplo de todo o avanço – aqui focando não só nos derivados da pandemia, mas todos aqueles que foram surgindo ao longo das décadas – são serviços que esta nova sociedade nos oferece, estes vão muito além daqueles a que a sociedade estava acostumada, sendo que, hoje, estas novas abordagens estão totalmente direcionadas para o cliente, para a sua satisfação e posterior fidelização (Meirelles, 2006). Desta feita, o conceito de serviço tem vindo a ser, inevitavelmente, alterado, sendo este definido, pela al.

[8] Dados retirados do *site* da Anacom, disponível para consulta em https://www.anacom.pt/render.jsp?contentId=1603793, consultado em 11-03-2021.

g) do artigo 3º do Decreto-Lei n.º 30/2020, de 29 de junho[9], como: "qualquer prestação de atividade à distância, por via electrónica e mediante pedido individual do seu destinatário, geralmente mediante remuneração…". Ora, da presente definição podemos retirar três elementos essenciais (1) "à distância", (2) "por via electrónica", (3) "mediante pedido individual de um destinatário de serviços", que são também estes melhor especificados nas subalíneas da al. g) do pré-referido artigo. Assim, de acordo com o artigo anteriormente enunciado, significará o conceito de "à distância" como os serviços prestados sem que haja a necessidade de presença simultânea das partes. Já no que tange à utilização da "via eletrónica", quererá isto dizer que o serviço deverá ser enviado da origem e recebido no destino através de meios eletrónicos de processamento e de armazenamento de dados, que sejam inteiramente transmitidos e recebidos por cabo, rádio, meios óticos ou qualquer outro meio eletromagnético. Por fim, o último destaque vai para a menção da expressão "mediante pedido individual do seu destinatário", que significa um serviço fornecido por transmissão de dados mediante um pedido individualizado. Estas definições encontram-se, respetivamente, mencionadas nas alíneas i), ii) e iii). Destacamos ainda um quarto elemento destes serviços, apesar da ressalva para a sua natureza não essencial, que é a prestação de um serviço mediante uma remuneração, tal como refere a própria caracterização de "serviço".

Com o enquadramento supra, é-nos, então, possível entender em que consistem os designados serviços da sociedade digital e o quanto estes abrangem um sem número atividades económicas na sua rede. Enfatizar que, de entre as variadíssimas atividades que estes compreendem, e fazendo aqui um paralelo com o último elemento – os serviços mediante remuneração – destacado na disseminação anterior –, existem ainda aqueles que não são remunerados pelo destinatário, como é o caso do fornecimento de informação em linha (Pereira, 2001, p. 9), ou seja, o acesso a bases de dados eletrónicas em linha[10].

[9] Este Decreto-Lei transpõe para o ordenamento jurídico português a Diretiva da União Europeia n.º 2015/1535 do Parlamento Europeu do Conselho, de 09 de setembro de 2015, relativa a um procedimento de informação no domínio das regulamentações técnicas e das regras relativas aos serviços da sociedade da informação.

[10] Urge referir que existe uma proteção de dados eletrónicos através da designada propriedade intelectual, cf. Decreto-Lei n.º 252/94, de 20 de outubro, que vem regular o regime de proteção jurídica dos programas de computador, transpondo assim para o nosso ordenamento jurídico a Diretiva n.º 91/250/CEE, do Conselho, de 14 de maio. No que tange à proteção das bases de dados, encontramos o Diretiva 96/9/CE do Parlamento Europeu e do Conselho de 11 de março de 1996, alterada pela Diretiva 2019/790 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, porquanto, atualmente, podemos também socorrer-nos do estabelecido no Regulamento da União Europeia de 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016, vulgarmente conhecido como RGPD. Importa referir que este regulamento é assegurado a nível

## 1.2. "O E-commerce"

Com o decorrer dos tempos, e com todo desenvolvimento tecnológico, vários conceitos a que as gerações passadas[11] estariam habituadas foram sendo modificados, ou melhor dizendo, readaptados ao novo mundo digital. É aí que ganha destaque o tão já conhecido "e", que nos acompanha diariamente no momento atual. Destaque para o *e-service*, que foi já parcamente estudado anteriormente, e *e-commerce*, também conhecido como comércio eletrónico.

Thais Zaninelli admite que o *e-commerce* e *e-business* estarão na origem dos ditos *e-services*, pois são estes que desafiam o modelo tradicional, otimizando assim o espaço *on-line*, criando, posteriormente, lucros mais elevados (Zaninelli, 2007, p. V).

*E-commerce* foi definido por Fernando Ferrão genericamente como *"*o fornecimento relativo a produtos/serviços/pagamentos através de linhas telefónicas, redes de computadores, ou outros meios de comunicação" (Ferrão, 2000, p. 35).

Já para Alexandre Pereira, esta forma de comércio poderá ser traduzida "na negociação realizada por via eletrónica, isto é, através do processamento e transmissão eletrónicos de dados, incluindo texto, som e imagem"[12] (Pereira, 2001, p. 4). De acordo com o mesmo autor, deverá ser feita uma distinção de modalidades relativas ao comércio eletrónico, existindo assim um comércio que se designa indireto e um outro denominado direto. O primeiro está relacionado com a encomenda eletrónica de bens, onde, ainda assim, será necessário recorrer aos meios tradicionais (como serviços postais, privados ou correio) para a sua correta entrega. Por outro lado, a segunda modalidade, está associada aos negócios totalmente *on-line*, onde a encomenda, pagamento e entrega são feitas em linha de forma informática (são exemplo programas de computador ou conteúdos de diversão).

nacional através da Lei 58/2019, de 8 de agosto, vulgarmente conhecida como Lei da Proteção de Dados Pessoais, bem assim como pela Diretiva 2019/770 do Parlamento Europeu e do Conselho, de 20 de maio de 2019 – sobre certos aspetos relativos aos contratos de fornecimento de conteúdos e serviços digitais, de notar que esta tem em vista, igualmente, a sua transposição para o ordenamento jurídico português.

[11] Por gerações passadas entendam-se aqueles nascidos antes dos anos 70, aproximadamente. Ricardo Santos faz um estudo, na sua dissertação de mestrado, relativo aos jovens *Millennials*, no qual assume que esta geração está compreendida entre os nascidos em 1977 e 1997. De acordo com o autor, estes são definidos como os "nativos digitais", uma geração que busca o novo e diferente e que, consequentemente, se encontra muito mais "aberta" a novos conceitos. Veja-se: Santos, R. P. H. (2017). *As Fintech na geração Millennials.* (Dissertação de mestrado, não editada). Escola Superior de Gestão, Lisboa. Disponível para consulta em https://comum.rcaap.pt/bitstream/10400.26/23184/1/RicardoSantos_ISG.pdf.

[12] O autor enfatiza como principais atividades do comércio eletrónico, o de bens e serviços, a entrega em linha de conteúdo digital, as transferências financeiras eletrónicas, o comércio eletrónico de ações, leilões comerciais, contratos públicos, entre outros. *Vide* p. 4 (Pereira, 2001).

Temos então uma modalidade indireta que dependerá sempre de terceiros para a sua correta execução, ao passo que, numa modalidade direta esses terceiros não existem, explorando-se assim na totalidade o potencial de um mercado digital, sem fronteiras geográficas.

A nível nacional, é com o Livro Verde para a Sociedade da Informação em Portugal[13], elaborado pela Missão para a Sociedade da Informação, que urge, pela primeira vez, a necessidade de se viabilizar o comércio eletrónico, baseado numa economia digital.

## 1.3. "Evolução digital na Banca"

Todo o progresso tecnológico ao longo dos anos está hoje evidente um pouco por toda a indústria mundial, e facto é que a financeira não é exceção. Antes pelo contrário. Este é um dos setores que desde cedo sofre maior desenvolvimento e que, pela sua importância na economia dos países, mais rápida e facilmente se ajusta ao que há de novo. Desde cedo que a área bancária está em contacto com a tecnologia. Segundo Artur Agostinho, remonta ao período entre 1886 e 1897 o momento em que começam a ser utilizadas infraestruturas tecnológicas para suportar a globalização dos serviços financeiros, tais como o telégrafo e o cabo submarino transatlântico (Agostinho, 2016, p. 10). É com a criação da *Automated Teller Machine* (ATM), em 1967 no Reino Unido, que se dá a expansão da história evolutiva e é com esta criação que se inicia a libertação dos clientes de se deslocarem ao balcão sempre que necessitavam de acesso às suas contas, sendo que, com isto, esta torna-se na segunda fase de introdução de tecnologia no sistema financeiro, que se alargou até aos meados de 2008, altura em que se dá uma das grandes crises financeiras mas que, ao mesmo tempo, fica marcada pela transformação e inovação levadas a cabo pela área bancária (Agostinho, 2016, p. 10).

Entretanto, entre os anos de 1997 e 2008, o sistema financeiro sofre uma das suas maiores alterações a nível tecnológico, com destaque para o *on-line banking* e as *satart-ups.* Dá-se então início à possibilidade de aceder aos serviços através da internet, telefone e, mais tarde, através de aplicações para *smartphones* (Agostinho, 2016, p. 10). Hoje em dia, a

[13] Este livro surge com a preocupação de acessibilidade aos *sites*, tentando ao máximo clarificar no que consistiam as tecnologias de informação, bem como de que forma estas poderiam ser importantes para uma necessária inovação a nível nacional, mas, e acima de tudo, uma regulamentação a nível legislativo para a possibilidade de uma correta expansão do comércio eletrónico. Disponível para consulta em http://homepage.ufp.pt/lmbg/formacao/lvfinal.pdf, consultado a 16-03-2021. Este estudo foi de tal forma bem conseguido que apenas em 2006 existiu a necessidade de rever o plano do Livro Verde, de notar que o mesmo é publicado em 1997.

indústria financeira apresenta desenvolvimentos tecnológicos de excelência ao nível de empréstimos, assessoria financeira e de seguros mas, essencialmente, a nível de pagamentos (Vives, 2017, p. 99).

Em suma, com o avanço do mundo novo da sociedade digital temos acesso a novos serviços a que, outrora, não tínhamos acesso, culminando assim num novo tipo de comércio e que, como vimos, dá origem às maiores revoluções digitais, nas mais diversas áreas económicas. No presente estudo, importa-nos a área financeira, mais concretamente este novo sistema designado de *E-banking*. Será nele que nos focaremos, de forma detalhada, no ponto seguinte do trabalho.

# 2. Os Contratos de E-banking

## 2.1. *Nomen iuris* e noção

O *E-banking* pode ser considerado, a nosso ver, como o apogeu/auge da evolução bancária, pois foi através deste que toda a tradicional metodologia organizativa sofreu a sua maior alteração. No momento presente, e muito graças à pandemia que se viveu, e que certa forma ainda se encontra presente no quotidiano de todos, mas, com especial relevo, nos períodos de Estado de Emergência (09-11-2020 e 30-04-2021) e de Calamidade (01-05-2021 e 22-08-2021), vários foram os hábitos a que a população teve de se adaptar, não só a nível nacional, mas a nível mundial e, indubitavelmente, a utilização dos meios alternativos de pagamento foi, a par com o comércio eletrónico, bem como as plataformas de comunicação (Zoom ou Microsoft Teams), daqueles que sofreram um maior aumento[14].

Num estudo feito pela ACEPI, relativo ao estudo da economia digital em Portugal no ano de 2022, foi possível apurar que o crescimento do e-commerce no ano de 2021 foi de 40%, sendo que, a título de curiosidade, 27% das pessoas até ao momento nunca tinham realizado compras *on-line*. Ora, estes dados mostram que Portugal teve um crescimento na ordem dos 66% superiores ao crescimento da União Europeia, passando da 24ª para a 21ª posição no que respeita à percentagem de cidadãos que realizam compras *on-line*. Também a nível bancário esta readaptação societária teve impactos, atualmente, e de acordo com o estudo, 64% dos indivíduos utilizam hoje as plataformas bancárias através dos meios eletrónicos.

Vulgarmente denominado como banco *on-line*, banco internético (esta designação proveniente da expressão inglesa *Internet Banking*), passando pelo *home banking*, banca eletrónica ou *E-banking*, designação que decidimos acolher para esta dissertação, várias são as denominações que vão sendo utilizadas para abordar o tema. No entanto, tal como refere Carolina Barreira, entre a nossa doutrina e jurisprudência as expressões elegidas são, maioritariamente, a banca eletrónica e *home banking* (Barreira, 2015, p. 7).

[14] Dados retirados do site ACEPI, disponíveis para consulta em https://www.acepi.pt/media/a5afiwhq/estudo-economia-digital-2022.pdf, consultado em 20-02-2023.

Caracterizado pela possibilidade atribuída pelo banco, aos seus clientes, mediante a aceitação de determinados condicionalismos, de utilizarem um sem fim de operações bancárias *on-line*, relativamente às contas a que os mesmos sejam titulares, utilizando para o efeito canais telemáticos – que conjugam os meios informáticos com os meios de comunicação à distância[15] –, por meio de uma página seguramente assegurada pela entidade bancária[16], é, desta forma, que a generalidade da jurisprudência se pronuncia quanto à definição do referido serviço bancário. Em bom rigor, não existirá uma definição concreta relativa a esta forma de utilização do serviço bancário. Sabemos, pois, que terá de cumprir os requisitos acima enunciados para que possa ser considerado como tal.

Com uma simples pesquisa *on-line* relativa ao tema, vários são os resultados à disposição para consulta. Na sua grande maioria, são entidades bancárias que procuram, através da pesquisa dos mais curiosos, encontrar ali potenciais clientes. Desta forma, através desta procura, aquilo que obtemos é, em regra, uma típica venda de um produto, no caso, um serviço de pagamento[17], sendo o utilizador então exposto a todas as funcionalidades destes meios, bem como ao processamento necessário para a instalação e adesão do mesmo. Podemos, de acordo com estas buscas, efetuar operações de consulta de saldos e movimentos, ter uma visão geral das receitas e despesas[18], realizar transferências através da lista de contactos de telemóvel[19], fazer pagamentos de serviços e/ou compras, transferências de valores depositados para contas próprias ou de terceiros, para a mesma ou para diversa instituição de crédito[20], entre tantas outras coisas. O *E-banking* permite fazer praticamente todas as operações que se fazem num balcão e, em via de regra, com um

[15] Para mais desenvolvimentos relativamente aos meios telemáticos *vide* (Marques G. &., 2006) p. 748 e ss.

[16] Definição retirada do Ac. do STJ de 18 de dezembro de 2013, onde foi relatora Ana Paula Boularot, Processo nº 6479/09.8TBBRG.G1.S1, disponível para consulta em www.direitoemdia.pt, consultado e, 22-05-2021.

[17] De acordo com o artigo 2º, alínea vv, do DL n.º 91/2018, de 12 de novembro (vulgarmente denominado por RJSPME ou DSP2 – designação que adotaremos no presente estudo), serão serviços de pagamento as atividades enumeradas no artigo 4º do mesmo diploma legal.
Importa, ademais, referir que esta transposição surge da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro (DSP2), uma vez que, a DSP1 se reporta à Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro, esta, anteriormente transposta para o nosso ordenamento jurídico através do DL n.º 317/2009, de 30 de outubro.

[18] Informação retirada do site do banco BPI, disponível para consulta em: https://www.bancobpi.pt/particulares/servicos-24-7/bpi-net, consultado em 22-05-2021.

[19] Informação retirada do site da Caixa Geral de Depósitos, disponível para consulta em: https://www.cgd.pt/Institucional/Sala-de-Imprensa/2018/pages/caixa-lanca-nova-aplicacao-homebanking-para-smartphone.aspx, consultado em 22-05-2021.

[20] De acordo com Santos, V. (2018) p. 12.

custo muito mais reduzido[21] (pensemos não só, mas, por exemplo, que não existirá consumo na deslocação, ou que certas taxas podem sofrer uma redução de valores).

O serviço de *E-banking* inicia-se com a entrega, por parte da entidade bancária, das chaves de acesso ao serviço *on-line*. Em regra, essas chaves consistem no número do contrato, um código secreto e um cartão matriz[22] de coordenadas. Destarte, bastará ao cliente/utilizador dirigir-se à página de internet do seu banco, selecionar a área destinada ao registo e autenticar-se através dos dados que lhe foram anteriormente fornecidos (Barreira, 2015, p. 31)[23].

Nos casos em que o utilizador pretenda apenas fazer a consulta informativa da sua conta bancária, serão apenas necessários os passos anteriores, a saber, os de autenticação. Não obstante, se este, por sua vez, pretender realizar outro tipo de operações, como por exemplo uma transferência bancária para uma outra conta, aqui, a entidade bancária exigirá um maior número de confirmações, que poderão passar pela entrega de dígitos que constam do seu cartão matriz, estes escolhidos de forma aleatória pela plataforma, ou poderá ser ainda solicitado, como opção ou complemento, um código de confirmação que é enviado para o número de telemóvel que estará associado à sua conta bancária (Barreira, 2015, p. 31).

Urge referir que atualmente, e de acordo com o disposto no RJSPME/DSP2, os prestadores de serviços são obrigados a aplicar uma forma de segurança extra de proteção do cliente, sendo esta designada de autenticação forte. Esta regra entrou em vigor a partir do dia 14 de setembro de 2019, sendo que teve um período de transição que se estendeu até ao final do ano de 2021, querendo isto dizer que, foi a partir do início do ano de 2021 que se fez sentir com maior frequência a presença desta nova forma de proteção nos serviços de pagamento. De acordo com o *site* do Banco de Portugal, a autenticação forte caracteriza-se pelo procedimento do prestador de serviços em identificar/validar um cliente da utilização de um instrumento de pagamento específico. Esta autenticação será baseada em dois ou mais

[21] Afirmação emitida pela GAS DECO, a 10 de fevereiro de 2017, na sua página *on-line* numa publicação subordinada ao tema: "*Home Banking*: o que é?", disponível para consulta em https://gasdeco.net/literacia-financeira/trocar-por-miudos/banca-digital/, consultado a 22 de maio de 2021

[22] Conforme explica (Barreira, 2015), p. 19.

[23] A autora, Carolina Barreira, faz ainda um interessante paralelismo entre os códigos de acesso ao *E-banking* e a assinatura de um documento particular autenticado, consoante o preceituado no artigo 374º do CC Ora, de acordo com a lei, é considerada válida uma assinatura que tenha sido aposta e reconhecida num documento particular, ou, por sua vez, que não tenha sofrido quaisquer impugnações por parte daqueles contra quem o documento é apresentado. Quer então isto dizer que, nos contratos de *E-banking*, os códigos introduzidos, como os de acesso, desempenham as funções de assinatura do cliente, substituindo as mesmas

elementos, que poderão pertencer a uma das seguintes categorias: (i) conhecimento – algo a que apenas aquela pessoa terá acesso, como uma palavra passe –, (ii) posse – um elemento que só o utilizador possua – e (iii) inerência – que, tal como o nome indica, seja algo inerente ao usuário, algo que o possa identificar, como a impressão digital ou retrato facial[24].

A autenticação forte é, em regra, aplicada sempre que um cliente aceda à sua área *on-line*, e consequentemente inicie uma operação de pagamento, mas não só, basta que o mesmo realize a operação através de um canal remoto e a mesma possa envolver riscos de fraude. No entanto, como toda a regra tem a sua exceção, de acordo com o Banco de Portugal, os pagamentos de valores inferiores a 30 € (trinta euros), bem como o pagamento de portagens através da Via Verde são excluídos da utilização deste tipo de autenticação, sendo que o mesmo é justificado pela previsão do risco associado à operação[25].

Ora, através desta revolução de prestação de serviços, o banco assume inerentemente um maior compromisso para com os seus clientes, pressupondo-se assim que as suas respostas, para além de mais rápidas, sejam mais desenvolvidas e aperfeiçoadas[26]. Mas não só, importa referir que o recurso à informática fez com que estas entidades conseguissem prosseguir um princípio de sobeja importância, o princípio da simplicidade, que, como enuncia Menezes Cordeiro, se caracteriza pela redução ao mínimo de qualquer diligência dispensável, de forma a assim diminuir os custos e aumentar ao máximo o lucro (Cordeiro, 2008, pp. 147-150) e, mais uma vez, será de enunciar as vantagens de não existir a necessidade de deslocação que aqui consistirão na comodidade do cliente, incluindo-se igualmente neste princípio.

Enquanto a sua noção é relativamente simples e de fácil entendimento, o mesmo não se poderá dizer quanto à sua inserção numa relação negocial, que tende a ser caracterizada como complexa. Este serviço revela-se, segundo Maria Raquel Guimarães, no plano jurídico como uma teia de contratos que entre si interligados criam uma série de relações jurídicas complexas (Guimarães, 2011, p. 174).

[24] Seguimos aqui o entendimento do Banco de Portugal, disponível para consulta em https://www.bportugal.pt/perguntas-frequentes/8526, consultado em 13-07-2021.
[25] *Ibidem.*
[26] Não obstante a celeridade nas respostas, o prestador de serviços deverá sempre atentar nos deveres de informação, lealdade, diligência e transparência, tal como figura nos artigos 74º e 77º do Decreto-Lei n.º 298/92, de 31 de dezembro (RGICSF).

## 2.2. Caracterização dos Contratos de *E-banking*

Retomando a linha de pensamento de Maria Raquel Guimarães e, dando aqui enfoque à sua, a nosso ver, correta associação dos serviços de *E-banking* a uma relação jurídica complexa, não poderíamos deixar de mencionar que este é, igualmente, o parecer de uma parte significativa da doutrina[27], sendo mesmo adotada por muitos a expressão "relação bancária complexa" quando se pretende designar a cadeia de relações encetadas entre a entidade bancária e o cliente (Guimarães, 2011, p. 346).

Aqui chegados, a questão a que urge responder é de onde surge, então, esta relação elaborada de contratos. Ou seja, qual poderemos designar de contrato primogénito, apesar de todas as demais figuras afins a este associadas, e aqui a resposta revela-se de substancial concordância: o contrato de abertura de conta[28,29].

Ora, de acordo com Engrácia Antunes, o contrato de abertura de conta poderá ser definido como "o contrato celebrado entre um banco e um cliente através do qual usualmente se constitui, disciplina e baliza a respetiva relação jurídica bancária" (Antunes, 2009, p. 483). Contrariamente ao que acontece noutros países[30], onde existem regras comuns aprovadas pelas entidades bancárias para a elaboração deste tipo de contratos, em Portugal tal não se verifica, ou, pelo menos, de forma tão explícita como noutros ordenamentos. A nível nacional, recorre-se, em regra, às conhecidas cláusulas contratuais gerais[31]. No caso, e tal como é estipulado nos n.[os] 4,5 e 6 do art. 77º do RGICSF, o Banco de Portugal obriga a que todos os contratos celebrados entre as instituições bancárias e os seus clientes contenham neles todas as informações necessárias à boa compreensão do cliente relativamente ao contrato em causa[32], existindo, consequentemente, lugar a contraordenação quando as

[27] Vide para o efeito, a título de exemplo, (Antunes J. A., 2009), p. 484 e (Vasconcelos, 2019) p. 73 e ss.

[28] Incumbe-nos aqui fazer igualmente a ressalva de que, também, a jurisprudência nacional partilha da mesma opinião da demais doutrina. Atente-se para tal, entre outros, nos Ac. do STJ de 5 de abril de 2016, onde foi relator Martins De Sousa, Processo nº 4640/11.4TBRG.G2..S1 e Ac. do TRC de 11 de fevereiro de 2020, onde foi relator Isaías Pádua, Processo nº 8592/17.9T8CBR.C1, ambos disponíveis para consulta em www.direitoemdia.pt.

[29] Será relevante notar que alguns autores preferem a denominação de contrato bancário geral para este primeiro passo de interligação, nomeadamente (Almeida, 2015), p. 24 e 10 e ss.

[30] Como são exemplo a Alemanha e Itália, conforme refere (Vasconcelos, 2019), p. 75.

[31] Estas encontram-se reguladas no DL n.º 446/85, de 25 de outubro.

[32] Breve nota relativamente a estas informações: quando estes contratos são facultados ao cliente, vêm, na sua grande maioria, acompanhados de anexos designados de "condições gerais" que, se atentarmos, são construídos de forma comum entre todas as entidades bancárias, o que nos leva a refletir sobre o ponto acima enunciado. Ora, apesar de em Portugal não estar aprovado formalmente um conjunto de regras para realização de contratos, salvo melhor opinião, acreditamos que o Banco de Portugal, entidade máxima de referência a nível bancário, tenta de alguma forma regular aqui tal questão e, prova disso, são as referidas condições. Veja-se, para o efeito, por exemplo, as cláusulas da Caixa Geral de Depósitos

mesmas não se verifiquem[33]. Com efeito, existe sempre uma base legal que conferirá um caráter padrão a este tipo de contratos, independentemente da entidade bancária aos quais estiverem adstritos.

Desta feita, com o recurso às CCG em consonância com os elementos exigidos no art. 13º do Aviso n.º 5/2013 do Banco de Portugal – descrição detalhada das partes –, chegamos ao mencionado contrato de abertura de conta, o primogénito ou, como também o menciona Engrácia Antunes, contrato matriz[34].

A abertura de conta está dominantemente associada à constituição de depósitos bancários[35]. Este último pode ser caracterizado pela:

> "Convenção acessória do contrato de conta bancária através da qual o cliente (depositante) entrega uma quantia pecuniária ao banco (depositário), ficando este investido no direito de dela dispor livremente e no dever de restituir outro tanto da mesma espécie e qualidade nos termos acordados" (Antunes, 2009, p. 492).

Desta definição podemos, assim, identificar dois elementos essenciais ao depósito, primeiramente a entrega de uma quantia de dinheiro ao banco, que pode ser feita de forma presencial (material) ou eletrónica, sendo que com este ato o banco fica, automaticamente, responsável pelo risco da disponibilidade dos valores depositados. Já o segundo elemento prende-se com a obrigação de restituição das quantias nos moldes anteriormente acordados[36] (Antunes, 2009, p. 493). O depósito é um contrato real *quod constitutionem*[37],

(https://www.cgd.pt/Particulares/Contas/Abertura-conta/Documents/ICGD0207.pdf); do BPI (https://www.bancobpi.pt/contentservice/getContent?documentName=PR_WCS01_UCM01070682); do Banco Santander (https://www.santander.pt/pdfs/precario-banco-outros-documentos/contas/BST-IE-50003156.pdf - este relativamente à abertura de conta por parte de pessoas coletivas), consultadas em 17-07-2021.

[33] Estas contraordenações poderão ser puníveis com uma coima entre os € 3.000,00 e os € 1.500.000,00, no caso de se tratar de pessoas coletivas, e entre € 1.000,00 a € 500.000,00, caso se refiram a pessoas singulares – artigo 210º, al. h), do referido diploma.

[34] Acompanhe-se, nesta senda, o entendimento de (Vasconcelos, 2019) p. 73 e ss. bem como (Antunes J. A., 2009) p. 483 e ss. entre outros.

[35] O depósito bancário é uma matéria amplamente estudada no nosso ordenamento jurídico, vejam-se a título de curiosidade, por exemplo, (Cordeiro, 2008) *e* (Vasconcelos, 2019). Ademais, não o é só a nível doutrinal mas, como também, vastamente em jurisprudência. Neste sentido, *exempli gratia*, Ac. do TRC de 10 de setembro de 2013, onde foi relator Jorge Arcanjo, Processo n.º 6/07.9TBPNH.C1 e AC. do TRC de 17 de dezembro de 2014, onde foi relatora Maria Domingas Simões, Processo n.º 15/09.3TBPNC.C1, ambos disponíveis para consulta em www.direitoemdia.pt. Nota de relevo ainda para o DL n.º 430/91, de 2 de novembro, relativo ao regime geral das contas de depósito.

[36] Deve aqui fazer-se a ressalva de que, em regra, a restituição das quantias é acompanhada de um acréscimo de montante correspondente a juros, conforme refere (Antunes J. A., 2009) p. 493.

[37] Quer isto dizer que é um contrato real conforme a constituição. São contratos que apenas ficam celebrados com a entrega da "coisa" que é o seu objeto – art. 408º CC (São, para além do depósito, exemplo disto o contrato de comodato e mútuo).

consensual, bilateral imperfeito de prestação de serviços, que pode ser gratuito ou oneroso, conforme o estipulado nos artigos 1186º e 1158º do CC (Vasconcelos, 2019, p. 121)[38].

Apesar da praticamente constante interligação entre o contrato de abertura de conta e o contrato de depósito é imperativo esclarecer que estes são, apesar de tudo, contratos autónomos, estando regidos pelo princípio da autonomia.

Como foi anteriormente mencionado, a abertura de conta está regulada pela Lei das CCG. É este que, em consonância com o plasmado no Aviso do BP n.º 11/2005, de 13 de julho, forma a base legal deste contrato. Como consequência do exposto, constata-se que esta primeira convenção apesar de ser considerada um contrato atípico[39] é, pela sua disciplina jurídica, bem como pelo anteriormente mencionado, considerado socialmente como um contrato típico (Antunes, 2009, p. 486). Ainda na senda do seu regime jurídico, este primeiro ato de contratação deve sempre estar associado, como está, ao princípio da liberdade contratual – art. 405º do CC[40], bem como revestir a forma escrita, conservando assim a sua característica de contrato formal (Antunes, 2009, p. 481).

Do supra exposto podemos, finalmente, caracterizar os contratos de *e-banking* como contratos de adesão, bem como relacioná-lo como um contrato quadro. Desde a sua origem até ao momento atual, estes contratos são simples contratos de adesão, ou seja, através das já diversas vezes mencionadas CCG, as entidades bancárias têm elaborado uma minuta contratual com todas as necessárias informações, a qual é apresentada ao cliente dando-lhe a possibilidade de aderir aquele serviço ou não (Antunes, 2009, p. 480). Podemos dizer que são os tipos de contratos que não são avaliados caso a caso, mas sim é apresentado um modelo regra, aplicado a todos os demais.

Também nesta senda será de mencionar o enorme contributo de Maria Raquel Guimarães para o estudo destes contratos. De acordo com a autora, a contratação do serviço de *e-*

[38] A propósito do estudo destes dois contratos – a abertura de conta e o depósito – Carlos Ferreira de Almeida faz uma análise notória relativamente à necessidade da distinção de ambas as figuras, por forma a assim se evitar o equívoco entre ambas (Almeida, 2015) p. 23 e ss.

[39] Podemos definir contratos atípicos como aqueles que, como o próprio nome indica, não estão tipificados na lei.

[40] Também este é assunto pautado por alguma divergência doutrinal. Como exemplo de opiniões contrárias temos, por um lado, a favor da total liberdade contratual, (Cordeiro, 2008) p .192 e ss. Por outro lado, e com algumas questões relativamente à plenitude de liberdade, encontramos, mais uma vez, (Antunes J. A., 2009), p.479. Este último enuncia, para além do clausulado legal a que os contratos de abertura de conta estão adstritos, conforme anteriormente mencionado, o RGIC, em especial os arts. 2º e ss., como meio de limite à liberdade contratual. Não podemos deixar de mostrar a nossa compreensão pelo entendimento e ligeira filiação ao seu entender.

*banking* é equiparada ao contrato-quadro, em consonância com o disposto no artigo 2º do RJSPME/DSP2 podemos definir este como um "contrato de prestação de serviços de pagamento que rege a execução futura de operações de pagamento individuais e sucessivas e que pode enunciar as obrigações e condições para a abertura de uma conta de pagamento" (Guimarães, 2011, p. 151). É precisamente a partir desta figura contratual que se potenciam posteriormente uma multiplicidade de outros contratos que são, manifestamente, facilitados pelo recurso aos meios eletrónicos. Citando Maria Raquel Guimarães: "o contrato-quadro é, essencialmente, um contrato de contratos, um contrato que antecipa futuros contratos…" (Guimarães, 2011, p. 151). É, nas palavras de António Pinto Monteiro, uma "relação de colaboração estável, duradoura, de conteúdo múltiplo, cuja execução implica designadamente, a celebração de futuros contratos entre as partes …" (Monteiro, 2004, p. 108).

Ora, quer isto dizer que existe, na grande maioria das vezes, uma celebração paralela, ou seja, um deles existe em função do outro (um, o quadro, origina o outro, o de E-banking), sendo que funcionalmente são complementáveis, e é nesse conjunto de contratos que se reveem as vontades integrais das partes (Guimarães, 2011, p. 151 nota de rodapé 405).

No entanto, importa ressalvar que esta complexidade contratual quando é ordenada através da Internet, isto é, sempre que um utilizador emite uma ordem pagamento a favor de um terceiro eletronicamente, é celebrado um novo contrato com base no anterior, que se rege pelas regras do já contratualmente definido num primeiro momento – no contrato quadro[41].

## 2.3. Conteúdo Contratual – As Obrigações das Partes

Ao longo do presente capítulo fomos já analisando pontualmente os serviços abrangidos pelo *E-banking*. De entre os variadíssimos privilégios que esta evolução bancária nos trouxe, podemos destacar, *exempli gratia*, a consulta de saldos e a realização de diversas operações bancárias, *maxime* pagamentos e transferências referentes às contas de que

[41] Conforme explicado por (Guimarães, 2013), p. 59.

sejamos titulares. Não obstante este ser um contrato profundamente vantajoso para o cliente, é inegável que o é, verdadeiramente, para ambas as partes contraentes[42].

Como qualquer relação duradoura de excelência, a de uma entidade bancária e do seu cliente não é diferente. Aos múltiplos benefícios, somam-se as obrigações. Assim é com um caráter, praticamente, obrigatório que esta relação (cliente – entidade bancária) tenha como princípios basilares o respeito e, acima de tudo, que sejam delimitadas quais as obrigações, direitos e deveres de cada uma das partes.

A celebração de um contrato nesta ordem de complexidade requer, para a boa prossecução do seu fim contratual, que o mesmo seja regido com base em deveres jurídicos, principais, acessórios e laterais. Atualmente, as operações realizadas através do sistema bancário eletrónico são reguladas pelo RJSPME/DSP2.

### 2.3.1. Deveres do utilizador

Se pensarmos num contexto obrigacional, um dever principal é aquele em que a parte se obriga a prestar, ou seja, em que a realização de um dado facto dá, a cada uma das partes, o fim a que se comprometeram, sendo assim constituído o vínculo obrigacional[43].

Na relação obrigacional em estudo, o cliente não deve a observância de nenhum dever principal. No entanto, muitas das vezes, o dever de correta utilização do serviço, pela sua sobeja importância, é confundido como tal. Contudo, tal associação, a nível técnico-jurídico não se encontra correta uma vez que não se consubstancia numa verdadeira prestação (Barreira, 2015, p. 17), dado que não é objetivo último da entidade bancária que o cliente utilize o serviço de *E-banking* corretamente, mas, sim, reduzir os seus custos e manter satisfeitos os seus atuais utilizadores, bem como angariar novos.

As obrigações dos clientes/utilizadores estão contempladas no art. 110º do RJSPME/DSP2.

Da análise do referido artigo, mais especificamente do n.º 1, al. a) e b), retiramos duas obrigações primordiais para a utilização do instrumento do *E-banking*: a primeira, a) "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 a segunda, b) "comunicar, logo que tenha conhecimento dos factos e sem atraso

[42] *Vide*, neste sentido, o Ac. do TRL de 26 de outubro de 2010, onde foi relatora Maria Amélia Ribeiro, Processo n.º 1943/09.1TJLSB.L1-7, disponível para consulta em https://www.direitoemdia.pt/.
[43] Para mais desenvolvimentos sobre os deveres principais, veja-se, entre outros, (Varela, 2012).

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". Já no n.º 2 do artigo em estudo, encontramos uma terceira obrigação, c) "tomar todas as medidas razoáveis, em especial logo que receber um instrumento de pagamento, para preservar a segurança das suas credenciais de segurança personalizadas".

**i. Dever de correta utilização do serviço de *E-banking***

Analisando de forma mais detalhada esta responsabilidade, como vimos acima, a mesma apesar de diversas vezes confundida, não pode ser considerada um dever principal, porquanto é um dever acessório[44]. Quer isto dizer que a boa utilização do serviço é considerada como um objetivo intermédio. Esta é uma condição *sine qua non* do seu bom funcionamento. Por outras palavras, a primeira obrigação consubstancia-se numa condição de boa utilização – isto é, dentro dos limites estabelecidos pelo contrato – que permitirá ao cliente continuar a usufruir do serviço (Barreira, 2015, p. 18).

**ii. Dever de Comunicação imediata de qualquer operação abusiva e não autorizada ou de extravio de códigos de acesso**

Também classificado como um dever acessório, esta obrigação de comunicação imediata em caso de uma utilização abusiva e não autorizada do instrumento de pagamento é, regra geral, estipulada no contrato. Contudo, no entendimento de Maria Raquel Guimarães, com o qual concordamos, mesmo que este não fosse contratualizado, decorreria sempre da relação de confiança existente entre a entidade bancária e o cliente (Guimarães, 2011, p.331).

[44] Os deveres acessórios são autónomos dos deveres principais, como é facilmente interpretado, e distintos dos deveres secundários. Estes podem surgir de uma cláusula contratual, de dispositivos da lei *ad hoc* (que, de acordo com o glossário jurídico, disponível para consulta em https://portal.oa.pt/media/134397/glossario-para-impressao_final.pdf , consultado em 10-02-2022, significa: "Para isso. Diz-se relativamente a uma pessoa ou coisa preparada para determinada função ou circunstância") ou do princípio da boa-fé (art. 762º do CC) – veja-se, neste sentido, (Varela, 2012) p. 123 e Ac. do TRC de 09 de novembro de 2004, onde foi relatora Alexandrina Ferreira, Processo n.º 2278/04, disponível para consulta em https://www.direitoemdia.pt/ .
De mencionar que, ainda no entendimento de Antunes Varela, com o qual concordamos, os deveres acessórios assumem especial relevância em contratos bilaterais, pois impõem a cada uma das partes o dever de tomar as devidas precauções por forma a que a principal finalidade seja devidamente cumprida.

Se, por um lado, de acordo com o artigo 110º do RJSPME/DSP2, esta comunicação, que deve ser feita por parte do cliente ao banco, deve ser realizada sem atrasos injustificados, logo que se tenha conhecimento da perda, roubo ou apropriação abusiva do instrumento de pagamento, por outro lado, é responsabilidade da instituição financeira disponibilizar, de acordo com o artigo 111º, n.º 1, al. c), do RJSPME/DSP2, os meios "adequados para permitir ao utilizador de serviços de pagamento proceder à comunicação prevista na alínea b) do n.º 1 do artigo 110º ou solicitar o desbloqueio nos termos do n.º 4 do artigo 108º".

Esta notificação é manifestamente decisiva, pois estabelece o momento a partir do qual o cliente deixa de ser responsável pelos resultados da operação não autorizada[45].

#### iii. Dever de confidencialidade dos dados pessoais do *E-banking*

O presente dever, explanado no n.º 2 do artigo 110º do referido Regime, reporta-se à obrigação do cliente tomar todas as medidas necessárias para preservar a confidencialidade, base da eficácia dos serviços de segurança, das senhas de acesso fornecidas pela entidade bancária, usualmente inscritas num cartão matriz[46]. Uma vez fornecidos os códigos de acesso, bem como a chave do cartão matriz, o utilizador é automaticamente considerado como titular do cartão ou conta, estando assim possibilitado de aceder a todos os erviços disponibilizados pelo *E-banking* (Alves, 2019, p. 23).

Face ao exposto – assunção da titularidade pelos códigos de acesso –, é de fácil compreensão a presente obrigação de dever de sigilo, guarda e não transmissão a terceiros daquela que é a base da confiança desta relação contratual.

### 2.3.2. Deveres do prestador de serviços

Enquanto no ponto anterior em estudo afirmámos não existir um real dever principal, por força da sua aplicação técnico-jurídica, para o utilizador de um serviço de pagamento, no presente, e relativamente ao prestador do serviço atestamos que, quanto ao mesmo, existe, sim, um dever principal. A este, cabe-lhe a aceitação dos sucessivos mandatos para pagamento, emitidos mediante a correta utilização do serviço, o que englobará, a correta autenticação, compreendendo os limites de saldo disponível – nos casos das contas à

[45] Este ponto será aprofundado adiante.
[46] (Barreira, 2015), p. 19, nota de rodapé 85, define cartão matriz como um cartão de coordenadas utilizado para validar operações bancárias suscetíveis de alterar o património detido naquele cartão ou conta.

ordem –, ou nas medidas em que tenham sido contratualizados anteriormente – nos casos das operações a descoberto ou nos casos de crédito[47].

Os deveres adstritos ao prestador de serviços encontram-se figurados no artigo 111º do RJSPME/DSP2. Pela interpretação do mesmo, podemos retirar cinco das primordiais obrigações deste, encontrando-se estas enumeradas nas alíneas: a) "assegurar que as credenciais de segurança personalizadas do instrumento de pagamento só sejam acessíveis ao utilizador…", b) "abster-se de enviar instrumentos de pagamento não solicitados, salvo quando um instrumento deste tipo já entregue ao utilizador de serviços de pagamento deva ser substituído", c) "garantir a disponibilidade, a todo o momento, de meios adequados para permitir ao utilizador de serviços de pagamento proceder à comunicação prevista na alínea b) do n.º 1 do artigo 110º...", d) "facultar ao utilizador do serviço de pagamento, a pedido deste, os meios necessários para fazer prova, durante 18 meses após a comunicação prevista na alínea b) do n.º 1 do artigo 110º…" e e) "impedir qualquer utilização do instrumento de pagamento logo que a comunicação prevista na alínea b) do n.º 1 do artigo 110.º tenha sido efetuada". Disseminando estas alíneas:

**i. Dever de entrega de códigos somente ao utilizador**

A entrega, por parte da entidade bancária, dos códigos de acesso e cartão matriz, constitui um pressuposto basilar desta relação *on-line*, uma vez que, sem os mesmos, o utilizador não conseguirá aceder ao serviço. Estamos, assim, perante um dever acessório (Barreira, 2015, p. 20).

Os códigos de acesso, bem como as coordenadas do cartão matriz, são de extrema importância na medida em que, sem os mesmos, o cliente fica impossibilitado de aceder ao *E-banking* e, mormente, realizar operações de pagamento – sendo que, é apenas através destes que uma operação é autenticada e autorizada pelo cliente, ficando posteriormente apta à execução por parte do banco. Ademais, e como analisado no título 2.1. do presente trabalho, com a nova Diretiva – o RJSPME/DSP2 – a questão da segurança foi altamente tida em conta, como o deverá, sendo que entre outras obrigações, foi imposta a obrigatoriedade da autenticação forte. Se a mesma não for exigida pelo prestador de serviço, aquando da emissão do mandato pelo ordenante, este ficará desonerado de quaisquer perdas relativas a operações não autorizadas, conforme explanado no artigo

[47] Encontramos mais desenvolvimentos sobre os deveres principais da entidade bancária em (Guimarães,2011), 282 e ss.

115º, n.º 5, do RJSPME/DSP2. Como já verificado, o utilizador será responsabilizado apenas se agir de forma fraudulenta.

### ii. Dever de correta execução de ordens de pagamento autorizadas

A contratação do serviço de *E-banking* entre o cliente e a entidade bancária não constitui *per si* uma autorização generalizada para toda e qualquer ordem de pagamento que o utilizador do serviço pretenda realizar. É necessário um conjunto de manifestações negociais – autorizações – quer da parte do cliente, quer da parte do prestador de serviços, para que a ordem de pagamento fique corretamente concluída.

Esta temática, do consentimento/autorização, é altamente abordada, pela sua importância, na nova Diretiva, mas não como algo novo, pois já o tinha sido na Diretiva anterior. Atualmente, o artigo 103º do RJSPME/DSP2 estipula que uma operação de pagamento apenas é considerada como autorizada quando existe, por parte do seu ordenante, o respetivo consentimento. Este ato de confirmação ocorre, regra geral, previamente à execução da operação, salvo quando devidamente acordado entre as partes, podendo, nestes casos, ocorrer em momento posterior, conforme indica o n.º 2 do supra mencionado artigo.

O incumprimento deste consentimento consubstancia numa falta de autorização para a operação em questão que poderá, numa situação de fraude, ser o bastante para a responsabilização da entidade bancária – art. 103º, n.º 5, RJSPME/DSP2.

Importa uma vez mais referir que o utilizador do serviço de *E-banking* identifica-se junto da entidade/plataforma através da sua identificação virtual, e quer isto dizer que é através das suas credenciais pessoais – códigos de acesso e números do cartão do cartão matriz. Assim, se uma autorização provier munida de tais dados, o Banco executará a mesma de imediato.

Não obstante essa confirmação virtual, é da responsabilidade da entidade bancária verificar que se encontram reunidos todos os pressupostos para a boa execução da ação/ordem de pagamento – respetivamente, a existência de fundos suficientes –, sendo que, caso o Banco detete alguma ação que não seja suportada pelos fundos do utilizador, este tem legítima permissão para recusar a ordem emitida (Santos V. , 2018, p. 25). Imaginemos, por exemplo, os casos em que existem levantamentos ou pagamentos sucessivos ultrapassando o valor que o cliente tinha na conta à ordem. Ora, nestes casos, o banco, por se revelarem

movimentos manifestamente incomuns, poderá e deverá bloquear as ações e assim estar à alerta para um possível caso de fraude, devendo, de imediato, contactar o titular da conta. No entanto, o Banco deverá atentar a se esses movimentos não se encontram estipulados no contrato de *E-banking*, pois, se os mesmos aquando da celebração forem acautelados, não cabe ao banco tomar a decisão de recusa de qualquer que seja a ordem bancária, conforme estipulado nos artigos 105º e 106º RJSPME/DSP2. É, ainda, responsabilidade da entidade bancária a abstinência do envio de serviços não solicitados pelo cliente.

### iii. Garantir a disponibilidade de meios para um serviço seguro e eficaz

A exigência que um serviço deste calibre – *E-banking* – requer, não se suporta só em deveres "básicos". É ainda exigido a ambas as partes, mas, em especial, à entidade bancária, que preste um serviço eficaz e seguro[48], conforme advertido sistematicamente no RJSPME/DSP2, nomeadamente no seu artigo 70º, bem como no artigo 73º do RGICSF.

O *E-banking* tem, como já amplamente referido neste trabalho, inúmeras vantagens, de entre as quais se destaca maioritariamente a sua celeridade e eficácia automática. Contudo, inevitavelmente, esses benefícios acarretam riscos elevados que são próprios da utilização de um serviço desta envergadura. Ora, isso pressupõe, não só a verificação de um alto nível de segurança, conforme mencionado supra, mas que ambas as partes utilizem o serviço de forma diligente.

Um serviço eficaz não é só aquele que é célere. Eficácia pode, também, significar confiança, sobretudo quando existe uma situação de ameaça. Nesta senda, o prestador de serviços deverá criar um sistema seguro, mas, e acima de tudo, que permita um fácil acesso em caso de ocorrência de fraude, por exemplo. Para isso, o Banco deverá garantir, a todo o momento, os meios adequados para o utilizador comunicar o ocorrido, conforme estipula o artigo 111º, n.º1, al. c), do RJSPME/DSP2.

A possibilidade que é dada ao utilizador do serviço de pagamento para fazer uma notificação nos termos do artigo supra mencionado, assume um caráter de elevada relevância, pois é a partir deste momento, com a emissão deste alerta, que o cliente se desresponsabiliza numa situação de uma operação não autorizada.

[48] Esta ideia é amplamente abordada em diversos acórdãos nacionais, tomemos como exemplo o Ac. do TRL de 12 de dezembro de 2013, onde foi relator Tomé Ramião, Processo n.º 164/11.8TBSRT.L1-6 e Ac. do STJ de 18 de dezembro de 2013 (Ana Paula Boularot), *cit.* ambos disponíveis para consulta em https://www.direitoemdia.pt/ . Esta qualidade de serviço é considerado como um dever acessório do prestador de serviços.

De acordo com o explanado no artigo 111º, n.º 1, al. d), do supra referido diploma, é ao Banco a quem compete disponibilizar os meios necessários para que o utilizador do serviço possa fazer prova de que efetuou a notificação identificada supra, apesar de ser este quem tem o dever de pedir para efetuar a mesma.

Assim, e terminando o presente ponto com a análise da al. e) do n.º 1 do artigo 111º do RJSPME/DSP2, caberá à entidade bancária impedir, logo que a notificação nos termos da alínea c) seja concretizada, qualquer utilização do serviço de pagamento assim que seja detetada qualquer suspeita de uma operação não autorizada.

### iv. Dever de informação quanto às medidas de prevenção à segurança do serviço

Desta relação bilateral entre utilizador e prestador de serviços surge um dever lateral de conduta chamado dever de informação. Este assenta na necessidade de a entidade bancária fornecer ao seu cliente todas as informações necessárias a adotar na conservação da segurança de códigos de acesso e de autenticação[49].

Pressupõe-se, com o exposto, que, com o mencionado dever cumprido, o utilizador terá total e completo conhecimento de como fazer uma utilização correta do serviço, especialmente, no que toca aos crimes de fraude informática.

Assim, e como defende Verónica Santos, posição com a qual concordamos, acabam por existir três grandes formas de dever de informação. Uma primeira aquando da celebração do contrato, uma segunda que se encontra sempre disponível para consulta no menu da página principal do banco e, por fim, os vários alertas que a entidade bancária emite quando o cliente entra na aplicação que apenas são fechados pelo próprio utilizador, quase que obrigando o mesmo a lê-los[50].

[49] O referido dever é, nas palavras de (Guimarães, 2013) p. 62, "um dever imposto à entidade bancária de explicar as situações mais comuns de fraude e os perigos específicos dos diferentes serviços que fornece, em função do tipo de utilizador envolvido e dos seus conhecimentos técnicos…".

[50] Um dos principais exemplos destes alertas são as sucessivas mensagens relativas à não entrega dos dados do cartão matriz ou quaisquer coordenadas que dele constem. Veja-se, a título de exemplo, o separador emitido pelo Novo Banco relativo à segurança *on-line*, onde faz referências não só a onde não devemos colocar os códigos mas inclusivamente denuncia diversos esquemas de fraude a que os seus utilizadores devem estar atentos, com consulta disponível em https://www.novobanco.pt/seguranca/alertas-fraude , consultado a 10-08-2023.

# 3. *E-Banking* e a Fraude Informática

O desenvolvimento digital oferece-nos inúmeras vantagens, conforme temos vindo a estudar. No entanto, nem tudo são pontos positivos. Facto é que o "facilitismo" de acesso aos sistemas permitiu que, cada vez mais, aumentasse o número de cibercrimes[51], que será a temática que aprofundaremos ao longo do presente título.

A simplicidade e celeridade das operações detonaram a segurança e dificultam, cada vez mais, a prevenção[52]. A própria criptografia[53] utilizada pelos sistemas não é impedimento bastante a estes atos ilícitos.

Não obstante esta breve introdução, é benéfico, no nosso entender, que, antes de estudarmos os vários tipos de fraude, possamos partir do entendimento técnico-jurídico, bem como quais são os elementos constitutivos associados ao conceito de fraude.

A forma mais tradicional por onde podemos começar será pela análise do Código Civil. Se conjugarmos os n.$^{os}$ 1 dos artigos 240º e 242º do predito diploma, partiremos desde logo do regime jurídico da simulação para a obtenção de uma definição de fraude, onde, legalmente, para uma ação ser considerada fraudulenta deverão ser verificados, por parte do autor da ação, dois elementos psicológicos, sendo eles, um comportamento intencionado e em segundo a pretensão de obter uma vantagem em prejuízo de uma terceira pessoa - "… no intuito de enganar terceiros…" – art. 240º, n.º 1, CC.

Já não tão tradicional, mas de sobeja importância no estudo do tema do presente trabalho, quanto ao *E-Banking*, a ação fraudulenta ocorre quando alguém, não autorizado à operação, desempenha movimentações de saldos para contas de terceiros[54]. Assim, a fraude revela-se pelo comportamento culposo do sujeito que realiza a operação de

[51] O cibercrime, de entre as várias definições, é, de acordo com o site da Caixa Geral de Depósitos, um crime cometido através de meios informáticos. Este representa os atos ilegais e ilícitos praticados *on-line*. Disponível para consulta em https://www.cgd.pt/Site/Saldo-Positivo/formacao-e-tecnologia/Pages/lei-do-cibercrime.aspx?gclid=EAIaIQobChMIxu7q3fClgQMVGJRoCR0cUglJEAAYASAAEgJYm_D_BwE.
[52] Verónica Santos, (Santos V. , 2018), p. 30.
[53] De acordo com o IBM, a criptografia é uma forma de traduzir dados simples – texto não criptografado – para um formato cifrado – mistura de dados – permitindo assim que apenas quem tenha acesso a uma chave/código de descodificação possa aceder à mensagem. Disponível para consulta em https://www.ibm.com/br-pt/topics/encryption .
[54] Veja-se, neste sentido, (Guimarães, 1999) p. 13.

pagamento não autorizada previamente pelo titular da conta, pressupondo, desde logo, que o seu acesso teve como base a criação de uma estratégia informática ilícita[55].

De acordo com a APWG[56], atualmente a fraude informática no *E-Banking* é, de todas as formas de fraude, a mais lucrativa do cibercrime. No nosso modesto entender, esta intensidade de crimes ocorre pela "facilidade" atual de acesso às demais plataformas de *E-Banking*, bem como com toda a atualizada evolução dos sistemas que, como referido supra, não conseguem acompanhar/assegurar as questões mais complexas de segurança.

No âmbito do tema em estudo, o *E-Banking*, as principais modalidades de fraude passam pelo *phishing*, o *pharming* e o *spyware*[57].

### *3.1. Phishing*

A ação de *phishing*[58] abarca um catálogo de formas destinadas à obtenção de dados ou de informações confidenciais do utilizador do *E-Banking*, que serão utilizadas para um posterior benefício ilícito por parte dos *phishers*[59,60].

O *phishing* é uma técnica fraudulenta que se traduz, num primeiro, no envio de forma massiva de *emails*[61], tendo como objetivo a obtenção de dados que permitirão o acesso indevido aos serviços eletrónicos do banco (Barreira, 2015, p. 26). Estas mensagens surgem com aparência credível e fidedigna, devidamente "camufladas", como refere Maria Raquel Guimarães (Guimarães, 1999), parecendo-se, na sua maioria, com as próprias mensagens do banco, que remetem o utilizador para um *site* com aparência extremamente idêntica ao *site* oficial do banco. Aqui é solicitado ao utilizador a introdução das chaves de

[55] Com esta afirmação não queremos proclamar a ideia de que a utilização fraudulenta não pode ser exercida pelo próprio utilizador do serviço.
[56] A APWG é uma associação a nível mundial, sem fins lucrativos, criada em 2013, que visa unificar a resposta ao cibercrime. Para mais informações consultar https://apwg.eu/ .
[57] De acordo com (Guimarães, 2013) p. 62-63, as fraudes que atingem o *E-Banking* pressupõem sempre que o pirata informático tenha acesso à conta do cliente, permitindo a movimentação dos fundos, das várias formas de acesso possíveis, sem autorização do titular da conta. No entanto, estes acessos na grande maioria das vezes são fornecidos pelos próprios lesados sem que estes deem conta.
58 A expressão de phishing surge da palavra inglesa fishing – pesca – "…uma vez que estes grupos lançam o anzol e fazem-se passar por entidades geralmente conhecidas e credíveis, para obter acesso a contas privadas", expressão retirada do *site* Internet Segura, disponível para consulta em https://www.internetsegura.pt/Phishing, consultado 26-06-2023.
[59] Os *phishers* são aqueles que praticam a ação ilícita – autor da fraude – no âmbito do *phishing*.
[60] Para um estudo mais técnico veja-se, por exemplo, (Schwalbach, 2021) p. 36 e ss.
[61] Vulgo, *spam*, que consiste no envio de mensagens não solicitadas, enviada para um grande número de destinatários, sendo o seu conteúdo substancialmente idêntico e, na maioria das vezes, têm objetivos comerciais. Informação disponível para consulta em https://www.anacom.pt/render.jsp?categoryId=346972 consultado a 26-06-2023. Para um estudo sobre o regime jurídico das comunicações não solicitadas ou *spam*, ver (Almeida, 2015).

acesso ao *E-Banking*, bem como os seus dados pessoais, permitindo assim aos *phishers* o acesso a estes dados e, por conseguinte, permitindo o acesso às suas contas e posterior realização de operações não autorizadas, sem que o utilizador se aperceba ou permita.

Este tipo de ilícito tem uma variante de denominação consoante a fonte de onde provenha a técnica. Se o contacto do *phisher* ocorrer através de mensagens de texto – SMS – encontramo-nos perante uma ação de *smishing*[62]. Por sua vez, se este contacto for realizado através de chamada de voz, passa a denominar-se *vishing*[63].

Aqui chegados, cumpre aprofundar alguns dos principais elementos no elenco de ilícitos criminais presentes no *phishing*. São eles: a falsidade informática, o dano informático e burla informática.

### 3.1.1. A falsidade informática

Este tipo de crime encontra-se plasmado no art. 3º da Lei do Cibercrime[64] e, de acordo com o mesmo, mais concretamente no seu n.º 1, consiste na falsificação de dados informáticos, consumado pela produção de dados ou documentos não genuínos. Tipicamente, os elementos objetivos deste crime são "…modificar, apagar ou suprimir dados informáticos ou por qualquer outra forma interferir num tratamento informático de dados…".

Por seu turno, no tocante aos elementos subjetivos, encontramos "…provocar engano nas relações jurídicas…" com a intenção de que os documentos fraudulentos por eles emitidos "…sejam considerados ou utilizados para finalidades juridicamente relevantes como se o fossem…".

O facto de nos encontrarmos no âmbito da segurança das relações jurídicas, temática de sobeja importância, implica que esta ilicitude criminal tenha natureza pública (Alves, 2019, p. 32) , facto que visa proteger a segurança das relações jurídicas enquanto interesse

[62] De acordo com a Proofpoint o *smishing* é um ciber crime em crescimento. Atualmente estima-se que as organizações tenham sofrido um aumento de 76% no ano de 2022 de ações deste tipo, que resultaram em sucesso do autor do ilícito. Veja-se https://www.anacom.pt/render.jsp?categoryId=346972 e https://www.ibm.com/br-pt/topics/smishing, consultados a 12-09-2023.
[63] Para mais desenvolvimentos, consultar https://www.ibm.com/br-pt/topics/phishing.
[64] Lei n.º 79/2021, de 24 de novembro, que transpõe a Diretiva (UE) 2019/713 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, doravante designada por LC. Esta lei provém da alteração da Lei n.º 109/2009, de 15 de setembro, que transpõe para o ordenamento jurídico português a Decisão Quadro n.º 2005/222/JAI do Conselho de 24 de fevereiro.

público, o que, conforme refere Inês Custódio Alves, é essencial que o Estado de Direito assegure[65].

### 3.1.2. Dano informático, acesso ilegítimo e interceção ilegítima

A atividade de *phishing* é conseguida através de um *malware*[66] que tanto espia o computador da vítima como pode redirecionar o seu browser para URL's falsos (Alves, 2019, p. 32).

É precisamente através da utilização de um *malware* que se dá a consumação dos três tipos de fraude anteriormente mencionadas – *phishing*, *pharming* e *spyware*. Este tópico está contemplado nos artigos 4º, 6º e 7º da LC. Analisando estes artigos de forma mais detalhada, existem alguns pontos que são necessários reter.

- Artigo 4º, n.º 1 – Aquele que sem permissão instalar um *malware* com o intuito de alterar a capacidade real de acesso à Internet, incorre num crime de dano informático, que poderá ser punido com até três anos de prisão ou pena de multa.
- Artigo 6º, n.ºs 1 e 2 – A utilização de um *malware* associada ao comportamento doloso do pirata informático, consubstancia num crime de acesso ilegítimo[67] que, de acordo com a lei, será punido até um ano de prisão ou com pena de multa até 120 dias.
- Artigo 7º, n.ºs 1 e 2 – Finalmente, a utilização de *malware* pode ainda estar associada ao crime de interceção ilegítima – "quem, sem permissão legal…interceptar transmissões de dados informáticos que se processam no interior de um sistema informático, a ele destinadas ou dele provenientes, é punido…", nestes casos com pena de prisão até três anos ou com pena de multa – n.º 1. Ainda na observância do referido artigo, o seu n.º 2, esclarece que apenas a tentativa desta interceção[68] ilegítima é punível.

65 *Vide* neste sentido, por exemplo, Ac. TRL de 30 de junho de 2011, onde foi relatora Filomena Lima, Processo 189/09.3JASTB.L1-5, disponível para consulta em https://www.direitoemdia.pt/

66 O *malware*, ou *software* malicioso é um termo que descreve um qualquer programa ou código malicioso que seja prejudicial aos sistemas. Para mais desenvolvimentos sobre a temática, *vide*, por exemplo, https://pt.malwarebytes.com/malware/ .

67 Neste sentido, veja-se, pela sua pertinência, o Ac. TRC de 17 de fevereiro de 2016, onde foi relator Jorge França, Processo 2119/11.TALRA.C2, disponível para consulta em https://www.direitoemdia.pt/.

68 De acordo com o artigo 2º, al. e), a interceção é considerada "o acto destinado a captar informações contidas num sistema informático, através de dispositivos electromagnéticos, acústicos, mecânicos ou outros".

### 3.1.3. A Burla Informática

Por fim, relativamente ao estudo das diversas formas de *phishing*, encontramos a burla informática, que se encontra prevista no artigo 221º do Código Penal[69]. Este tipo de crime surge para penalizar aquilo que temos já vindo a estudar, como as diversas formas de captação de informações alheias por meios ardilosos, sendo que com o seu manifesto acréscimo o legislador sentiu a necessidade de acautelar este novo tipo de crime (Alves, 2019, p. 34).

Por considerarmos esclarecedora, transcreve-se a definição de burla informática dada pelo Supremo Tribunal de Justiça, de 20 de outubro de 3010, onde foi relator Pires da Graça, Processo 78/07.6JAFAR.E2.S1[70]:

> "O crime de burla informática é um crime especial de burla, cuja especificidade reside no processo vinculado de execução, que assenta na manipulação do sistema informático por uma das seguintes formas: interferência no resultado ou estruturação incorrecta de programa, utilização incorrecta ou incompleta de dados, utilização de dados sem autorização ou qualquer intervenção não autorizada de processamento. A burla informática, tal como a burla geral, assenta necessariamente num artifício, engano ou erro consciente, mas, contrariamente ao tipo geral, esse expediente não se dirige à manipulação da vontade de uma pessoa, antes pela utilização (obrigatoriamente) de um daqueles procedimentos, que se traduz no uso abusivo do sistema de dados ou de tratamento informático, e consequentemente, na manipulação do funcionamento do sistema informático, em ordem à obtenção de um enriquecimento patrimonial ilícito"

Ora, esta clara definição permite-nos retirar os principais elementos, objetivos e subjetivos, deste ilícito criminal. São eles, a nível objetivo, a interferência no resultado de tratamento de dados, a estruturação incorreta e a utilização não autorizada durante o processamento. Por conseguinte, os elementos subjetivos são a intenção de obter – portanto, com dolo – benefícios de terceiro e em seu prejuízo, porquanto terá plena consciência de que o seu ato viola a lei e causará prejuízo ao lesado. (Alves, 2019, p. 35)

Ainda no âmbito do supra mencionado acórdão, esclarece-se que o crime de burla informática é primeiramente um delito contra o património, apenas secundariamente visa proteger o correto funcionamento dos sistemas informáticos.

[69] Lei n.º 54/2023, de 04 de setembro, doravante designado por CP.
[70] Disponível para consulta em https://www.direitoemdia.pt/.

## *3.2. Pharming*

Contrariamente ao *phishing*, a técnica do *pharming* é, manifestamente, mais perigosa, na medida em que, para o utilizador do *E-Banking*, é muito mais difícil de perceber que estão a ser alvos de um esquema informático, inclusivamente para os mais avançados informaticamente.

Esta dificuldade consubstancia-se no facto de este tipo de fraude ser uma técnica bem mais sofisticada do que a anteriormente estudada, na medida em que corrompe o próprio domínio da instituição financeira, levando novamente o utilizador a um *site* falso, que em tudo se assemelha ao *site* original do banco e, para que isso aconteça, basta o utilizar digite o endereço do banco no seu aparelho de acesso ao *E-Banking* (Santos V. , 2018, p. 33).

Esta técnica assenta na difusão de um vírus via *spam* no correio eletrónico, de ficheiros ocultos que, de forma igualmente oculta, se auto instalam nos computadores ou sistemas das vítimas. Após esta instalação, os arquivos do sistema, especialmente os que constam nos "favoritos" e os registos de *cookies*[71], sofrem alterações sem que o utilizador dê conta do sucedido.

Estes ficheiros ocultos são programas que captam os códigos de pulsação do teclado, os designados *keyloggers*, e permitem que, sempre que o utilizador digitar um endereço de determinado *site*, este seja transportado para outra página que não aquela que efetivamente pretendia aceder, tendo acesso a tudo o que for digitado pelo utilizador no teclado, nomeadamente, palavras-passe e nomes de utilizador do acesso à conta de *E-Banking* (Barreira, 2015, p. 27).

Para além do procedimento exposto, que consubstancia na instalação de um *malware* no computador do utilizador, que é inclusivamente o mais usual, o método do *pharming* não se esgota por aqui. Esta modalidade pode, igualmente, ocorrer quando o utilizador digita o endereço do banco na barra de pesquisa com erros ortográficos, sendo aqui o cliente

[71] De acordo com (Barreira, 2015) p. 27, citando Ramos Pereira (2001) Direito da Internet e Comércio Eletrónico. Lisboa. Quid Iuris. p. 245, os *cookies* são "um arquivo de texto que, via de regra, é gravado no disco do computador e utilizado pela memória RAM enquanto o internauta navega na internet. Deste modo, aquando da sua primeira visita a um *website* podem ser formuladas perguntas de caráter pessoal. Tais informações serão gravadas no *cookie* colocado no sistema para que uma futura navegação seja personalizada".

automaticamente redirecionado para um *site* falso. Ademais, este tipo de fraude, pode também acontecer quando o pirata informático se apodera da página oficial do banco, conduzindo para uma página falsa todos aqueles a que lhe tentem aceder durante aquele período (Barreira, 2015, p. 28).

Relativamente a esta comparação relativa a perigosidade entre o *phishing* e o *pharming*, o Tribunal da Relação do Porto, no seu acórdão de 7 de dezembro de 2014, onde foi relatora Ana Lucinda Cabral, relativo ao Processo 747/12.9TJPRT.P1, é bastante esclarecedor da diferença entre ambos:

> "O *pharming* opera pelo mesmo princípio do *phishing*, ou seja, fazendo os internautas pensarem que estão a aceder a um *site* legítimo, quando na verdade não estão. Mas ao contrário do *phishing*, o qual uma pessoa mais atenta pode evitar simplesmente não respondendo ao e-mail fraudulento, o *pharming* é praticamente impossível de ser detectado por um utilizador comum da Internet, que não tenha maiores conhecimentos técnicos. Nesse novo tipo de fraude, os agentes criminosos valem-se da disseminação de *softwares* maliciosos que alteram o funcionamento do programa de navegação (browser) da vítima. Quando esta tenta aceder a um *site* de um banco, por exemplo, o navegador infectado redireciona-a para o *spoof* site (o site falso com as mesmas características gráficas do site verdadeiro). No *site* falseado, então, ocorre a recolha das informações privadas e sensíveis da vítima, tais como números de cartões de crédito, contas bancárias e senhas.
>
> No crime de *pharming*, a vítima não recebe um e-mail fraudulento como passo inicial da execução, nem precisa clicar num link para ser levada ao site falso, uma vez infectado o seu computador pelo vírus, mesmo teclando o endereço correto do site a que pretende aceder, o navegador leva-o diretamente para site falseado".

### *3.3. Spyware*

Considerado como os anteriores como uma forma de fraude bancária *on-line*, este é proveniente, também de um *malware*, afigura-se como "um programa malicioso que se instala no computador ou *tablet* do cliente sem que este se aperceba. Uma vez instalado, deteta se o cliente está a aceder a uma página de internet protegida e regista os dados inseridos pelo utilizador"[72].

[72] Excerto retirado do *site* Banco de Portugal, disponível para consulta em https://clientebancario.bportugal.pt/pt-pt/noticias/proteja-se-contra-fraude-na-internet-banco-de-portugal-divulga-boas-praticas-nas-operacoes, consultado em 18-09-2023.

De certa forma, o método de atuação é ligeiramente idêntico ao do *pharming*, pois em ambos os casos existe a instalação de um *software* malicioso – *malware* – e o utilizador é enganado sem que tenha qualquer contacto com o criminoso, através do que acontece com o *keylogger*.

Lamentavelmente, este tipo de programa pode ser instalado inofensivamente pelo utilizador sem que este se aperceba, através de um simples *download* aparentemente sem riscos associados. Esta questão é extremamente relevante pelo facto de que todos nós enquanto usuários de um mundo cada vez mais digital estamos constantemente sob ameaça deste tipo de burlas. A velocidade de evolução está, como já referido anteriormente, ao mesmo nível da evolução de práticas fraudulentas, especialmente na área bancária, por ser a que mais rentável se revela para o criminoso. Neste sentido, o nosso quotidiano digital deve ser olhado com o máximo de atenção e conhecimento possível.

# 4. A Responsabilidade pelas Operações Não Autorizadas no Serviço de *E-Banking*

Aqui chegados, existem já diversos pontos sobre os quais somos conhecedores. Primeiramente, sobre a indubitável mais valia que é a evolução digital e, especialmente, na área bancária, tendo já sido vastamente enumeradas as várias vantagens que trouxe à população um serviço de *E-Banking*. No entanto, e como também somos já conhecedores, esta evolução acarreta algumas desvantagens, nomeadamente, quanto às fraudes associadas ao serviço de *E-banking*, que passam sempre pela intromissão de um terceiro sem autorização na rede pessoal do cliente (Santos V. , 2018, p. 34).

Esta temática encontra-se regulada no RJSPME/DSP2, já anteriormente mencionado, o qual visa transpor a Diretiva (UE) 2015/2366 que veio revogar a Diretiva 2007/64/CE do Parlamento Europeu e do Conselho, de 13 de novembro[73,74], e que de ora em diante será designada DSP2.

Os pontos seguintes deste trabalho versaram, precisamente, sobre a repartição dos prejuízos resultantes da fraude informática, onde será analisado a presunção de culpa por parte do usuário, o ónus de prova, bem como a imputação das responsabilidades a estes. Debruçar-nos-emos, ainda, sobre a imputação da responsabilidade ao prestador de serviços, a importância da notificação da entidade bancária e, finalmente, quanto ao reembolso de montantes.

## 4.1. Nota Preliminar

Os esquemas de fraude bancária são, por si só, um sistema de complexa resolução, mas não se encontram sozinhos neste campo. A sua resolução é de igual modo complexa, pois existem variadíssimas condicionantes que deverão ser tomadas em consideração. É

[73] Algumas das principais alterações da nova Diretiva para a anterior são, precisamente, o aumento da segurança nos pagamentos, fortalecendo assim os direitos dos consumidores. *Vide* https://www.bportugal.pt/perguntas-frequentes/8526.

[74] De notar que a questão dos prejuízos decorrentes de operações fraudulentas são relativamente recentes nos nossos tribunais, tendo a primeira sentença relativa ao tema sido proferida em 26-10-2010, no Tribunal da Relação de Lisboa (Barreira, 2015), p. 30, assim, a grande maioria das decisões jurisprudenciais até hoje tomadas foram-no no âmbito da antiga Diretiva, pelo que o deveremos ter em atenção.
Atualmente, por razões óbvias estas sentenças, de cariz de fraude bancária, têm vindo a aumentar.

necessário verificar o cumprimento dos deveres impostos às partes, avaliar o grau de censura, aplicar as regras ao ónus da prova para, só aí, se apurar como será distribuído o risco (Guimarães, 2013, p. 69). Maria Raquel Guimarães salienta, ainda, a importância de se notar que, nos casos em que existe a presença de piratas informáticos, não existe nenhuma verdadeira relação entre utilizador do serviço e o beneficiário da operação, porquanto este último não faz parte do contrato celebrado entre usuário e prestador de serviços. Este apresenta-se como um terceiro – facto que eleva a dificuldade da repartição do risco da operação (Guimarães, 2013, p. 68).

Não obstante esta dificuldade, também se verifica que existe uma relação entre o banco e os beneficiários da operação não autorizada, tendo, por isso, o primeiro legitimidade para agir contra estes de forma a reaver os montantes reembolsados ao cliente em virtude da fraude (Guimarães, 2013, p. 69).

Assim, concluindo este ponto introdutório, podemos afirmar que este é um tema extremamente relevante e complexo pelas suas demasiadas incertezas. No entanto, deixamos um excerto de um Acórdão do Tribunal da Relação de Guimarães, 23 de dezembro de 2012, onde foi relator Filipe Caroço, Processo 305/09.5TBCBT.G1, onde a questão é ligeiramente resumida, consubstanciando num ponto de partida para os demais pontos em estudo:

> "1- A complexidade dos sistemas bancários home banking, concebidos e controlados pelos Bancos, assim como a grande exigência dos mecanismos relacionados com a segurança das operações bancárias através deles realizadas, a par da propriedade do banco sobre os valores depositados pelos seus clientes, em ambiente contratual, justificam o funcionamento da regra da presunção de culpa prevista pelo art. 799º, nº 1, do Código Civil, que recai sobre a entidade bancária na responsabilidade pela utilização fraudulenta daqueles meios.
>
> 2- Em todo o caso, o banco pode elidir aquela presunção, afastando a sua culpa ou demonstrando mesmo a culpa do cliente pela deficiente utilização daqueles meios expeditos, designadamente, alegando e demonstrando que o cliente beneficiário violou o contrato, divulgando na internet dados pessoais, secretos e intransmissíveis relativos ao seu acesso, em benefício de *hackers*.
>
> 3- No primeiro caso, o Banco pode ainda ser responsabilizado pelo risco, enquanto na segunda hipótese a responsabilidade é do cliente".

## 4.2. A Presunção de Culpa do Banco – O Ónus de Prova

O artigo 113º, n.º 1, do RJSPME/DSP2 estabelece 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 do serviço prestado pelo prestador de serviços de pagamento"

Ora, o que se pode, desde logo, retirar do predito conceito legal é que é à entidade bancária a quem compete provar que a operação de pagamento foi devidamente autorizada, nomeadamente que foram cumpridos todos os elementos de segurança, como os códigos pessoais do utilizador.

Esta assunção da obrigação por parte da entidade bancária é defendida pelo legislador através do desconhecimento normal do usuário. O homem médio não tem, *à priori*, conhecimento quanto ao funcionamento dos sistemas bancários, pela sua elevada complexidade, razão pela qual caberá ao banco, conhecedores dos seus sistemas, provar que não foi por culpa deles – entidade – que se deveu a fraude[75]. Não obstante esta prova, posteriormente o banco ainda tem de provar que foi culpa do seu cliente, sendo esta a única forma de se ilibar da responsabilidade pela operação não autorizada[76].

Sem embargo do supra exposto, de acordo com o n.º 3 do mencionado artigo do RJSPME/DSP2, se o utilizador do serviço de pagamento negar ter autorizado a operação fraudulenta, a utilização do instrumento de pagamento registada pelo prestador de serviços, incluindo o prestador do serviço de iniciação de pagamento, não é necessariamente meio de prova suficiente para provar que o pagamento foi autorizado pelo ordenante, ou que este último tenha agido de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira – termos que serão analisados em maior detalhe no próximo ponto do trabalho –,

[75] (Barreira, 2015) p. 38, reforça o entendimento de que deve ser o banco a fazer prova da sua inocência e compara, a nosso ver, pertinente, esta necessidade com a assinatura num documento particular, nos termos do art. 374º do CC, se a parte contra quem o documento é apresentado impugnar a veracidade da assinatura, cabe à parte que apresenta o documento a prova da sua veracidade – art. 374º, n.º 2.
Nos contratos de *E-Banking*, considera-se a "assinatura" os códigos de acesso introduzidos para a autorização da operação.

[76] *Vide* neste sentido o Ac. do TRL de 5 de novembro de 2013, onde foi relator Manuel Marques, Processo 9821/11.8T2SNT.L1-1, disponível para consulta em https://www.direitoemdia.pt/

ou uma ou mais das obrigações adstritas ao utilizador – referidas no art. 110º do RJSPME/DSP2 e já sumariamente referidas ao longo do presente trabalho.

Apesar deste regime de prova, fixado quer pelo RJSPME/DSP2, quer pela anterior Diretiva, em tempos verificou-se por parte de algumas entidades bancárias a inclusão de cláusulas contratuais gerais nos contratos de *E-Banking* que visavam uma ligeira alteração dos critérios de repartição dos ónus de prova, temática que foi despertando alguma atenção por parte dos nossos tribunais[77], sendo que, apesar de existirem opiniões contrárias, como boas de direito, a maioria dos tribunais superiores condenaram este tipo de cláusula, declarando-as nulas (Barreira, 2015, p. 41). Atualmente, com o RJSPME/DSP2 em vigor, notadamente no seu artigo 159º, o regime aplicável ao utilizador de pagamento – entre o contrato de *E-Banking* e o Regime Jurídico – é aquele que mais favorável for para este, tendo assim diminuindo a relevância destas cláusulas e ficando os clientes mais protegidos.

Após o breve esclarecimento relativo à presunção de culpa e obrigação de ónus de prova, analisaremos de forma mais detalhada a imputação a cada uma das partes individualmente.

## 4.3. Imputação da Responsabilidade ao Utilizador

No ponto anterior, para além de percebermos que é ao banco a quem cabe fazer prova da sua inocência, aprendemos, também, de acordo com os n.ºs 3 e 4 do art. 113º do RJSPME/DSP2, que é igualmente a ele quem cabe fazer prova de que a "culpa" da utilização indevida do serviço de pagamento ocorreu por conta do seu utilizador[78], que agiu de forma fraudulenta, ou que não cumpriu, com dolo ou negligência grosseira, alguns dos deveres a que está submisso.

Veja-se, neste âmbito, o Acórdão do Tribunal da Relação do Porto, de 10 de janeiro de 2023, onde foi relator Rui Moreira, Processo 1053/20.0T8MAI.P1[79]:

> "I - Um acto qualificável como negligência grosseira, no âmbito da utilização de um sistema bancário electrónico de pagamentos, corresponde a um erro imperdoável, a uma desatenção inexplicável, a uma incúria inaceitável, por referência ao comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes.

[77] Veja-se, entre outros, o Ac. do TRG de 23 de dezembro de 2012, cit.
[78] Importa ter em consideração, igualmente, o art. 799º, n.º 1, do CC.
[79] Disponível para consulta em http://www.dgsi.pt/

> III - Para que se exclua a classificação de uma conduta como negligência grosseira, apesar de impregnada de descuido, desatenção e incúria intoleráveis, necessário se torna apurar que a mesma é recorrente e danosa junto de um número significativo de utilizadores, o que não se basta com uma alusão genérica a que a utilização do sistema dá azo à ocorrência de situações danosas em quantidade e de tipo indeterminado."

Chegados a este ponto, é improtelável perceber o alcance das expressões dolo e negligência grosseira do utilizador, que temos até aqui vindo a enunciar, para que se possa avaliar, sempre *in casu*, se existiu, ou não, quebra dos deveres e, consequentemente, se a aquele será imputada responsabilidade.

Ora, no Acórdão mencionado supra, no ponto I é dada uma definição de negligência grosseira, pelo que, quando esta se verifique, a responsabilidade pelos prejuízos resultantes de uma ação fraudulenta incidiram sobre o ordenador.

Consubstancia-se como negligência grave, não só aquela em que o cliente fornece os códigos de acesso e credenciais disponíveis no cartão matriz, como, também, nos casos em que este aja com descuido e desatenção, pese embora o correto funcionamento dos serviços bancários esteja assegurado, bem como os alertas de segurança na página de *E-Banking*, emitidos de forma extremamente clara e elucidativa na detecção de este tipo de ilicitude. Aos olhos da nossa jurisprudência, esta situação – de negligência – é altamente condenável, posição com a qual concordamos (Alves, 2019, p. 42).

Tendo em linha de conta o exposto no artigo 115º, n.º 4, do RJSPME/DSP2, havendo negligência grosseira por parte do ordenante, e tendo a entidade prestadora do serviço provado que aquele incumpriu com as suas obrigações, será o utilizador responsável pelo prejuízos causados, ficando adstrito a um pagamento superior ao limite definido pelo n.º 1 do pré referido artigo – € 50,00 (cinquenta euros) – montante máximo para as situações de negligência leve, que deverão, igualmente, ser alvo de responsabilização.

Em suma, e pegando na letra do Acórdão do Tribunal da Relação de Lisboa, 18 de dezembro de 2019, onde foi relator A. Américo Lourenço, Processo 45/17.1PHSXL-3, podemos distinguir a negligência do dolo com base neste ideal:

> "A negligência é um juízo de censura ao agente por não ter agido de outro modo, conforme podia e devia. O traço fundamental situa-se, na omissão de um dever objectivo de cuidado

> ou diligência – isto é, não ter o agente usado a diligência exigida segundo as circunstâncias concretas do caso, de modo a obstar ao evento.
>
> Quando a realização de um facto for representada como uma consequência possível da conduta, haverá dolo se o agente actua conformando-se com aquela realização. Assim, na conformação ou não conformação com o resultado é que reside a diferença entre o dolo eventual e a negligência consciente."[80]

Pese embora toda esta análise, não podemos deixar de referir que, em muitos dos casos, a conduta pouco cautelosa deve-se ao desconhecimento por parte do cliente, uma vez que, e salvo melhor opinião, apesar de nos encontrarmos na era digital, continua a existir bastante iliteracia tecnológica, sendo que caberá essencialmente ao banco analisar o cliente casuisticamente.

## 4.4. Imputação da Responsabilidade ao Prestador do Serviços

Até ao momento, estudámos os vários direitos e deveres de ambas as partes que figuram na relação de *E-Banking*, da presunção associada ao banco para ilidir a culpa no ato fraudulento, bem como a imputação de responsabilidade ao cliente, quando este aja com dolo ou negligência. Encontra-se, assim, em falta o estudo da responsabilidade associada ao prestador do serviço de pagamento, que abordaremos em seguida.

A nossa jurisprudência, de forma consensual, decide amplamente no sentido de responsabilizar o banco no âmbito deste tema. Aqui, acreditamos, entre em prática a ótica do direito da defesa do utilizador/consumidor que é, maioritariamente, a parte mais desprotegida da relação. Ora, se o cliente não agir irresponsavelmente, a responsabilidade recairá na íntegra sobre a entidade bancária[81].

Conforme enunciado por Inês Alves (Alves, 2019, p. 45), apontamento que consideramos importante, o Acórdão do Tribunal da Relação de Lisboa, 26 de outubro de 2010, cit., expede considerações relevantes, sendo que, de acordo com este:

> "… na sociedade de informação em que vivemos, só o banco tem hipótese de controlar os riscos que para ele são mínimos e que poderão ser desastrosos para a A. Por isso, numa ótica de defesa do consumidor, não tendo o banco demonstrado

[80] Disponível para consulta em https://jurisprudencia.pt/acordao/193620/ .
[81] Neste sentido, veja-se, entre outros, o Ac. do TRL, de 15 de março de 2016, onde foi relator Rijo Ferreira, Processo 1063/12.1TVLSB.L1-1, bem como o Ac. do TRG, de 17 de dezembro de 2014, onde foi relator Fernando Fernandes Freitas, Processo 1910/12.8TBVCT.G1, ambos disponíveis para consulta em http://www.dgsi.pt/ .

> culpa da A. na movimentação fraudulenta da conta, o mesmo terá de suportar as consequências da fraude no circuito cuja fiabilidade, de resto, ele próprio se comprometeu contratualmente a garantir".

Conforme já anteriormente abordado, existe uma presunção de culpa desde logo associada ao banco, e, se este não a conseguir ilidir, será sempre o responsabilizador pela prática fraudulenta, recaindo sobre si o reembolso imediato – temática a que dedicaremos mais atenção nos pontos seguintes – do montante da operação não autorizada (Alves, 2019, p. 46).

## 4.5. A Importância da Notificação à Entidade Bancária

Conforme anteriormente mencionado, no título 2.3.1, a notificação por parte do cliente à entidade bancária a dar conhecimento da ocorrência de uma operação fraudulenta opera um papel fundamental no que diz respeito à distribuição dos prejuízos decorridos da operação não autorizada.

Procurando uma exposição clara desta temática, consideramos importante fazer uma ligeira distinção entre as perdas ocorridas antes da comunicação do cliente à entidade bancária e aquelas que ocorrem após a comunicação. Isto porque, as repartições que ocorrem antes da notificação assumem uma complexidade ligeiramente mais elevada, que pressupõe alguns esclarecimentos prévios (Barreira, 2015, p. 42).

Esta notificação de uma operação não autorizada, caracteriza-se pelo momento a partir do qual o utilizador se poderá ilibar da responsabilização decorrente de um ato ilícito de fraude – artigo 110º, n.º 1, al. b), do RJSPME/DSP2. A partir deste momento, o cliente deixa de suportar as consequências financeiras associadas à apropriação abusiva do seu instrumento de pagamento (Barreira, 2015, p. 42).

De notar que a redução dos riscos e consequências destes atos é possível de reduzir, se a comunicação ao banco for feita assim que se tome conhecimento, sem atrasos injustificados, dentro do prazo de treze meses, conforme estipula o artigo 112º, n.º 1, do RJSPME/DSP2 – tornando, desta forma, inválidas quaisquer cláusulas contratuais que estipulem um prazo específico pois, o cliente poderá não ter conhecimento no próprio dia da prática da operação abusiva, tendo a seu favor o prazo supra mencionado.

Apesar da urgência na notificação, a Diretiva (DSP2) não vem estipular nenhuma forma concreta para a sua realização, pelo que, na falta de estabelecimento, o cliente deverá entrar em contacto com a sua entidade bancária pela forma que achar que seja mais célere. Atualmente, a grande maioria dos utilizadores têm já associado à sua conta de *E-Banking*, um gestor virtual, pelo que, na nossa opinião, salvo douto conhecimento, esta será uma das possíveis formas de contacto, uma vez que se encontra disponível a todo o momento.

É, no nosso entender, manifesto afirmar que, no caso da entidade bancária não disponibilizar estes canais para a comunicação do cliente, esta está a ir contra o estipulado por lei, nomeadamente no artigo 111º, n.º 1, al. c) e d), incorrendo numa ação de má-fé, em *venire contra factum proprium*, tentando imputar o risco ao seu cliente, não lhe permitindo o acesso ao contacto e posterior prova de que o realizou.

Após a referida notificação da entidade bancária, cabe a esta proteger a conta do seu cliente, nomeadamente através do bloqueio de conta, proibindo assim qualquer movimentação sobre a mesma – art. 108º, n.º 2, al. a) e b), do RJSPME/DSP2.

## 4.6. Dever de Reembolso

No decorrer deste estudo sobre a responsabilidade, surge, como ponto conclusivo, o reembolso dos valores indevidamente retirados. Ora, após a notificação anteriormente estudada, o banco, nos casos em que não se prove a culpa do cliente, deverá reembolsar de imediato os valores erradamente debitados da conta do cliente.

De acordo com o estabelecido no RJSPME/DSP2, o prestador de serviços fica responsável pelo reembolso logo que tome conhecimento da operação, ou após esta lhe ser comunicada, sendo que o atraso no cumprimento desta obrigação compreenderá o pagamento de juros moratórios, conforme fixado pelo artigo 114º, n.ºs 1 e 10, do RJSPME/DSP2.

O incumprimento desta obrigação – reembolso – é considerado, nos termos do artigo 151º, al. dd), uma infração, punível com uma coima de € 10.000,00 (dez mil euros) a € 5.000.000,00 (cinco milhões de euros).

# 5. O MBWay

Presentemente, conforme temos já vindo a estudar, e será, *a priori*, de conhecimento geral, vivemos atualmente envoltos num ecossistema digital[82], onde a comercialização de produtos e serviços de *E-banking* se encontra em constante mutação. Estes canais digitais permitem ao cliente aceder a todo o tempo aos seus serviços bancário, independentemente do sítio em que se encontrem.

Para além da facilidade que já nos trouxe o *E-Banking* "tradicional", hoje em dia, existem cada vez mais aplicações[83] e soluções de pagamento *on-line* que permitem, aos titulares de uma conta de pagamento ou de um cartão de pagamento, realizar, tal como através da aplicação do banco, transferências entre utilizadores da *app* de pagamento, fazer pagamentos, emitir cartões virtuais ou até mesmo a emissão de códigos para levantamento de numerário em caixas de multibanco[84].

Estas aplicações de pagamento podem ser disponibilizadas através de dois meios diferentes. Ou pelo próprio prestador de serviços, onde a *app* pode permitir o acesso à conta de depósito à ordem e à realização de operações a partir dessa conta, semelhante ao que acontece no *E-Banking*, ou pode apenas possibilitar determinadas operações – são as vulgarmente chamadas de aplicações do banco.

Por outro lado, a *app* pode ser facultada por uma entidade terceira. Nestes casos, a *app* é operada por uma entidade externa à da prestação de serviços, onde é associada uma conta ou cartão de pagamento, podendo, a partir daqui, serem movimentados fundos – são exemplo disto: o MBWay, a Apple Pay, o Google Pay, entre outros.

Não obstante o exposto, ainda que estas *app's* sejam operadas por uma entidade terceira, o prestador de serviços do cliente da aplicação será o responsável último pela correta

[82] O ecossistema digital é considerado um conjunto de ferramentas, plataformas e aplicativos que são unificados sob a mesma estratégia para alcançar um melhor posicionamento de um produto ou serviço. Disponível para consulta em https://blog.internexa.com/pt/ecossistemas-digitais-o-que-sao-e-como-sao-criados , consultado a 19-09-2023.
[83] Doravante designada por *app*.
[84] Para mais informações consultar https://clientebancario.bportugal.pt/pt-pt/aplicacoes-de-pagamento-o-que-sao , consultado a 19-09-2023.

realização da operação através dessa aplicação (tal como acontece nas *app's* que são disponibilizadas pela própria entidade)[85].

Num estudo realizado em agosto do presente ano, a Sage, empresa de apoio na área dos sistemas integrados de gestão e contabilidade, indica que os pagamentos em numerário estão a cair, sendo substituídos por meios de pagamento eletrónico onde o cartão bancário e o MBWay figuram como novas estrelas. Afirmam ainda que o MBWay é já o meio de pagamentos mais privilegiado junto das camadas mais jovens de consumidores.

É precisamente sobre esta aplicação que faremos um breve estudo no presente capítulo, aprofundaremos como funciona, quais os direitos e deveres dos utilizadores deste meio de pagamento, bem como fazer uma breve análise relativa à responsabilidade pela fraude nesta aplicação.

## 5.1. Noção e Funcionalidade

O MBWay é uma aplicação da SIBS (empresa que gere a rede Multibanco – considerada uma das maiores processadoras de pagamentos internacionalmente), que oferece uma solução interbancária para compras e transferências imediatas através de um telemóvel ou qualquer outro aparelho eletrónico[86].

Para poder usufruir do MBWay, basta ser cliente de um dos bancos aderentes[87] – que, hoje em dia, serão quase todos – e fazer a associação, na aplicação, dos cartões bancários pessoais ao número de telemóvel pessoal – ou profissional, consoante a finalidade pretendida. Esta associação pode ser feita através da própria aplicação do *E-Banking* ou em qualquer caixa automática da rede Multibanco[88]. De notar, que o MBWay não exige quaisquer carregamentos, nem tem quaisquer custos de adesão, permitindo ao cliente utilizar qualquer tipo de cartão de débito.

O cliente, quando entra na aplicação, tem disponíveis várias soluções, nomeadamente, enviar e receber dinheiro, pagar em lojas ou restaurantes com a própria aplicação, gerar um

[85] Informação retirada do *site* do Banco de Portugal, disponível para consulta em: https://clientebancario.bportugal.pt/pt-pt/aplicacoes-de-pagamento-o-que-sao, consultado em 20-09-2023.
[86] Definição retirada do site do Jornal Público, disponível para consulta em https://www.publico.pt/2019/02/06/economia/noticia/guia-mb-way-1860978, consultado em 20-09-2023.
[87] Pode ser consultada a lista dos bancos aderentes ao MBWay através da consulta ao site da aplicação, nomeadamente através do link https://www.mbway.pt/bancos-aderentes/ , consultado em 20-09-2023.
[88] Conforme indicado pelo *site* do Multibanco, disponível para consulta em https://www.multibanco.pt/operacoes/mb-way/ , consultado em 20-09-2023.

Cartão MBNet (permite fazer compras *on-line* que aceitam Visa, Mastercard ou AMEX), ou simplesmente gerar um código para fazer levantamentos no Multibanco[89].

Clarificando aqui alguma das funcionalidades, no caso das transferências e do código de levantamento, o utilizador só precisa de procurar o destinatário na sua lista de contactos, selecioná-lo e dar a ordem para transferir. O montante chegará ao cartão que o destinatário tiver associado à sua própria conta de MBWay. Já nos casos dos levantamentos, o código chega por SMS ao contacto associado à aplicação, e permite utilizar o Multibanco sem o cartão físico. No que toca ao pagamento em lojas físicas, o comerciante deverá estar munido de um *software* específico para aceitar este tipo de pagamento – nestes casos recorre-se ao QR Code. Nas compras *on-line*, o processo é semelhante aos anteriores, mas com recurso ao telemóvel, pois em todas as etapas é requerido o código PIN de seis dígitos[90].

De notar que, a própria aplicação do MBWay confere alguns limites à sua utilização ao nível do envio e recebimento de valores. De acordo com o próprio *site*, quer nos envios quer nos recebimentos, o limite da operação são 750,00 euros. A nível mensal, o valor não pode exceder os 2.500,00 euros, nem as 50 (cinquenta) transferências[91].

Já no que toca aos levantamentos, aqui são aplicados os limites gerais do Multibanco, ou seja, 200,00 euros por cada operação num total de 400,00 euros diários[92].

Aqui chegados, e pela sua importância para o restante do estudo, importa referir que de acordo com o artigo 2º do RJSPME/DSP2, o MBWay é considerado um instrumento de pagamento, pelo que serão de aplicar as mesmas regras do *E-Banking*, facto que muitos dos consumidores não têm ainda devida consciência[93].

Ora, neste sentido, os direitos e deveres do utilizador são praticamente idênticos àqueles que se aplicam à utilização da sua aplicação de *E-Banking*, não devendo, a nosso ver, este esperar menos responsabilização por estar a utilizar uma aplicação externa ao banco.

---

[89] Informação retirada do site do Jornal Público, disponível para consulta em https://www.publico.pt/2019/02/06/economia/noticia/guia-mb-way-1860978, consultado em 20-09-2023.
[90] *Idem*
[91] *Vide*, para o efeito, https://www.mbway.pt/perguntas/enviar-dinheiro-mb-way/limites-mb-way/, consultado em 20-09-2023.
[92] Veja-se https://www.multibanco.pt/operacoes/levantamento/, consultado em 20-09-2023.
[93] Veja-se, neste sentido, o artigo de Maria Raquel Guimarães na Nova Consumer Lab, intitulado "MBWay, Engenharia Social e Operações Fraudulentas", disponível para consulta em: https://novaconsumerlab.novalaw.unl.pt/mb-way-engenharia-social-e-operacoes-fraudulentas/ , consultado em 20-09-2023.

O *site* oficial do MBWay enuncia algumas recomendações de segurança[94] aos seus utilizadores, as quais agora aqui mencionamos. Em primeiro lugar, aconselham a associar sempre um número de telemóvel que seja familiar ao utilizador – preferencialmente o seu pessoal. A não partilha do PIN de acesso à aplicação é, igualmente, um dos principais cuidados que o utilizador deverá ter em atenção, nem como forma de pagamento, nem como forma de garantia – o PIN da aplicação (seis dígitos) é equiparado ao PIN do cartão bancário, sendo, por isso, estritamente pessoal e intransmissível. O mesmo se aplica ao código gerado para um levantamento através do MBWay.

O utilizador deverá ter ainda em consideração que, em caso de dúvida, os responsáveis por tal esclarecimento é sempre a aplicação e nunca um desconhecido.

De referir que o MBWay é um método de pagamento com autenticação forte, já estudada anteriormente neste trabalho, no título 2, facto que eleva os níveis de segurança, pelo que deverá ser utilizada.

## 5.2. A Responsabilidade pela Fraude na Aplicação – Análise Jurisprudencial

A elevada mobilização dos pagamentos implica um aumento considerável dos riscos de fraude, comparativamente aos meios eletrónicos ditos tradicionais. Este risco aumenta devido à utilização de redes públicas de *wireless*, palavras-chave pouco seguras, descarregamentos sem segurança que podem levar à instalação de *malwares* nos aparelhos pessoais, SMS, vídeos e mensagens partilhadas nas redes sociais, tudo isto utilizando o mesmo dispositivo daquele em que se acessa à conta bancária. Para além do exposto, a utilização das aplicações desatualizadas, ação frequente entre os utilizadores, que não permita a realização de atualizações, muitas vezes de segurança, consubstanciam na vulnerabilidade do sistema e possíveis intromissões não autorizadas[95].

A maioria dos casos registados de fraude no MBWay é realizada de forma extremamente simples, a nível de esquema informático – nada comparado aos casos de fraude anteriormente estudados –, o que pressupõe uma total desatenção por parte do utilizador do serviço. Este tipo de fraude não implica um conhecimento informático soberbo por parte

[94] Disponível para consulta em: https://www.mbway.pt/seguranca-mb-way/, consultado em 21-09-2023.
[95] Conforme Maria Raquel Guimarães na Nova Consumer Lab, intitulado "MBWay, Engenharia Social e Operações Fraudulentas", disponível para consulta em: https://novaconsumerlab.novalaw.unl.pt/mb-way-engenharia-social-e-operacoes-fraudulentas/, consultado em 21-09-2023.

do burlão, mas sim uma técnica recorrente nestes cenários que se designa de engenharia social[96].

Estes métodos de engenharia social têm tido uma evolução extremamente notória com o correr dos anos, em especial desde a altura pandémica por que passámos, onde a utilização dos meios digitais se tornou quase que indispensável para a grande maioria da população. Acrescido a esse aumento de vida *on-line* está o facto de que este método poder ser exercido através que qualquer forma de telecomunicação, abrangendo assim a sua área de atuação. Nestes casos, a vítima pode ser aliciada por compras fantasma, falsos investimentos, entre outras, sendo que terminam sempre numa consumação de uma operação fraudulenta que, nestes casos, pode ou não ser autorizada pela vítima.

Conforme indica Maria Raquel Guimarães[97], os esquemas fraudulentos mais frequentes surgem das vendas de bens em segunda mão numa plataforma eletrónica, e podem ser acionados quer pelo vendedor, quer pelo comprador. Numa primeira modalidade a vítima é instruída a instalar a aplicação do MBWay no seu telemóvel, com recurso a uma caixa multibanco ou, sendo já utilizador, a efetuar ou receber o pagamento, conforma a posição em que se encontre o autor da fraude. Após a instalação da aplicação é requerido à vítima que insira o seu cartão e código na caixa multibanco, é-lhe requerido para inserir o número e código indicados pelo falso comprador ou vendedor, sendo que, assim será este quem recebe os códigos no seu telemóvel, tendo total acesso à aplicação da parte contrária. Pode, em alternativa, ser o próprio autor da fraude a inserir os dados do utilizador que ele lhe tenha fornecido aquando do acordo da compra. Em qualquer um dos casos, o utilizador está a permitir o acesso a terceiro à sua conta bancária, ainda que sem consciência do ato.

Ora, nestes casos, e uma vez que esta forma de pagamento se encontra prevista no RJSPME/DSP2, bem como esta ausência do cumprimento dos deveres de segurança – negligência grosseira –, toda e qualquer operação fraudulenta que ocorra após esta cessão de dados correrá por conta do utilizador, de acordo com o artigo 115º, n.º 4, do RJSPME/DSP2.

[96] A engenharia social é considerada pelo IBM como uma manipulação das "… pessoas para que compartilhem informações confidenciais, façam download de software malicioso, visitem sites que não deveriam, enviem dinheiro para criminosos ou cometam outros deslizes que comprometam seus bens e sua segurança, sejam eles pessoais ou corporativos". "Como engenharia social explora as fraquezas humanas em vez das vulnerabilidades técnicas ou de sistemas digitais, às vezes é chamado de 'hackeamento humano'". Para o efeito, vide https://www.ibm.com/br-pt/topics/social-engineering, consultado em 21-09-2023.

[97] Maria Raquel Guimarães na Nova Consumer Lab, intitulado "MBWay, Engenharia Social e Operações Fraudulentas", disponível para consulta em: https://novaconsumerlab.novalaw.unl.pt/mb-way-engenharia-social-e-operacoes-fraudulentas/.

Para além desta, uma segunda categoria de operação fraudulenta, ainda de acordo com o estudo da autora acima mencionada, pode ocorrer da seguinte forma: "no momento de o utilizador receber um pagamento do terceiro via MB Way, (…) é instruído, também telefonicamente, para "enviar dinheiro" ao falso comprador em vez de lhe "pedir dinheiro". Assim sendo, esta operação é autorizada ou realizada pelo utilizador, devidamente autenticado e feitas a partir do seu próprio telemóvel, logo, não ficam abrangidas pelo RJSPME/DSP2 como operações não autorizadas, uma vez que são.

Mais uma vez, expressamos a nossa opinião, salvo douto conhecimento, no sentido de que a grande maioria destes crimes acontece pela iliteracia do utilizador, porquanto o dito homem médio não tem, a nosso ver, a devida destreza tecnológica, e não só, para conseguir evitar este tipo de acontecimento, sendo que, nestes casos, a falta de conhecimento é ainda agravada pela engenharia social.

Distrate o supra mencionado, são também formas de fraude no MBWay aquelas que estudamos anteriormente quanto ao *E-Banking*, aplicando-se as regras respetivas, de que somos já conhecedores.

Aqui chegados, a questão a que urge responder será sobre quem recaem os prejuízos pelas ações fraudulentas decorrentes do MBWay, será do utilizador, do banco ou da própria plataforma SIBS?

Junto da nossa jurisprudência esta é uma temática que tem vindo a ser, pelo seu indubitável crescimento, alvo de alguma discussão. No entanto, não existem, ainda, muitas decisões no âmbito do MBWay, pelo que, só o tempo dirá em que sentido estes se começarão a pronunciar de forma mais consistente.

Neste sentido, e por acharmos relevante para a análise do presente ponto, citamos dois acórdãos em que a decisão é inversa.

- Acórdão do Supremo Tribunal de Justiça, de 09 de junho de 2022, onde foi relator Cid Geraldo, Processo 10/20.1PAENT.S1[98]:

> "V - O que resulta da matéria de facto provada é que o arguido, ao longo de um período de 4 meses, enganou pelo menos uma dúzia de pessoas, convencendo-as a aderir ao serviço MB WAY, e associar a aplicação ao número de telemóvel dele, fixando um código PIN

[98] Disponível para consulta em http://www.dgsi.pt/ .

igualmente por ele definido e, na posse do número de telemóvel da vítima e do PIN, aceder ao cartão bancário e à conta bancária daquela e, por via do serviço MBWAY, poder ordenar movimentos bancários a partir da conta da vítima (transferências para outros cartões ou contas bancárias), ou pagamentos de compras e, ainda, efectuar levantamentos em numerário em caixas Multibanco, tendo as vítimas sido abordadas em momentos completamente distintos, por processos independentes e autónomos, invocando o arguido, em alguns casos, identidades diversas e sempre diferentes da sua, indicando números de telemóvel diferentes (e nunca o número de telemóvel do ofendido) onde recebia mensagem com os códigos de activação da aplicação MBWAY, indicando, ainda, um código de 6 dígitos, para definir o PIN MBWAY.

VI - Embora as situações criminosas que ocorreram se tenham processado genericamente da mesma forma, aquele teve de escolher as suas vítimas em plataformas de venda online, procurando aí identificar pessoas que tenham disponibilizado objectos para venda, contactando-as telefonicamente, manifestando a vontade de comprar esses objectos e dispondo-se a pagar os mesmos de imediato, por via da aplicação MBWAY, de forma independente, em momentos distintos, em abordagens autónomas e com algumas variantes, não havendo qualquer ligação entre aquelas pessoas, tendo o cuidado de se certificar que cada uma das vítimas não era conhecedora deste processo de pagamento, (pois, caso contrário, o agente dos factos desliga logo a chamada, não voltando a estabelecer qualquer contacto), desenvolvendo, então, um processo ardiloso, conforme as circunstâncias, tendo em vista ter acesso à conta bancária da vítima, pelo que, nunca poderia haver uma única resolução que abarcasse todas as acções ilícitas descritas. Diferente seria a conclusão se todas as vítimas estivessem reunidas numa mesma sala e o arguido aproveitasse a oportunidade de estarem todas juntas para, de uma só vez, as enganasse e convencesse ao uso da aplicação informática MBWAY, aproveitando o desconhecimento dos ofendidos sobre o modo de funcionamento dessa aplicação, a fim de efectuarem transferências de dinheiro da conta de terceiros associada à aplicação MBWAY. Neste caso, sim, estaríamos perante uma só resolução criminosa, a que corresponderia um só crime de um crime de falsidade informática e um crime de burla informática"

No acórdão em estudo o arguido foi condenado por doze crimes de falsidade informática e seis de burla informática. A ilicitude presente nesta decisão é um exemplo da primeira forma de fraude no MBWay que mencionámos no presente capítulo. No presente caso é até dado o exemplo de que em que circunstâncias a prática repetida deste crime poderia ser apenas condenável uma vez. No nosso modesto entendimento, este acórdão explica de forma clara e sucinta a maioria das fraudes que ocorrem no MBWay.

- Acórdão Tribunal da Relação do Porto, 10 de janeiro de 2023, onde foi relator Rui Moreira, Processo 1053/20.0T8MAI.P1[99]:

> O caso: "Depois de ter colocado à venda um automóvel numa plataforma eletrónica de anúncios, por um preço 1.400 euros, um homem foi contactado por outro que se mostrou interessado na compra e que se ofereceu para realizar o pagamento de um sinal, no valor de 100 euros. Para o efeito solicitou ao proprietário que se dirigisse a uma Caixa Multibanco para que o montante do sinal fosse imediatamente depositado na sua conta bancária. Ao fazê-lo foi levado associar ao seu MBWay o telemóvel do interessado, permitindo assim que este tivesse acesso à sua conta bancária e fizesse vários movimentos indevidos. Ao todo, o proprietário do veículo ficou sem 10.400 euros, que o banco se recusou a repor, o que o levou a recorrer a tribunal. Este julgou improcedente a ação, absolvendo o banco de qualquer responsabilidade pelo sucedido, decisão da qual foi interposto recurso para o TRP. [100]"
>
> "…Permitiu que o utilizador deste número passasse a poder usar o serviço MBWAY para aceder à sua conta bancária, o que ele fez dali extraindo os valores levantados e o valor transferido. Em concordância com a sentença em crise, só pode entender-se que a actuação do autor marido, ora apelante, assim descrita infringiu as suas obrigações de utilizador do serviço, subsumindo-se a sua conduta ao disposto na al. a) do nº 1 do art. 110º do DL n.º 91/2018, fazendo da aplicação em causa um uso indevido, em violação das respectivas condições de utilização, ao não preservar a segurança do que a norma define como "credenciais de segurança personalizadas". Para além disso, e ainda em concordância com o juízo sobre essa conduta constante da sentença recorrida, a actuação do autor marido só pode qualificar-se como negligência grosseira. … Em suma, nada nos habilita a concluir que a conduta do autor marido não deva ser classificada como um desvio grosseiro ao comportamento exigível a um normal ou medianamente capaz utilizador deste sistema, designadamente por representar uma conduta frequente ou recorrente, comum a um número relevante de idênticos utilizadores, e não um desvio inaceitável em relação á conduta esperada desse modelo médio de utilizador… infringindo os princípios mais básicos de segurança relativos à utilização de meios electrónicos de pagamento e de acesso à sua conta bancária, habilitando por si mesmo, com o uso do seu cartão multibanco e do seu PIN de autenticação… Concluímos, assim, em concordância com o tribunal a quo, que o autor marido, nas circunstâncias do caso, actuou com negligência grosseira, para efeitos do preenchimento dos pressupostos do art. 115º, nº 4 do DL n.º 91/2018.

[99] Disponível para consulta em https://www.direitoemdia.pt/

[100] Resumo retirado da página LexPoint, disponível em https://www.lexpoint.pt/conteudos/987/117419/noticias/fraude-por-mbway, consultado em 22-09-2023.

> É, por isso, incontornável a conclusão de que lhe cabe suportar as perdas verificadas, que não devem ser imputadas ao risco de operação do sistema pelo réu.

Ao contrário do que aconteceu com o primeiro acórdão analisado, aqui a questão encontrava-se entre o utilizador e o prestador de serviços – banco. Ora, conforme tinha já sido mencionado, o prestador de serviços não pode ser responsabilizado por um caso de fraude quando estejam verificadas, por parte do banco, todas as condições de segurança e informações sobre a mesa. No presente caso, estamos perante um caso de negligência absoluta por parte do utilizador que não poderá, no nosso entendimento ter outra decisão que não seja a sua total e completa responsabilização pelos danos sofridos.

Conforme afirmado anteriormente, não existem ainda muitas decisões no âmbito da fraude neste meio de pagamento. No entanto, acreditamos que as mesmas aumentaram, sendo que como em qualquer caso de direito, estas deverão ser analisadas casuisticamente e sempre tendo em atenção o tipo de utilizador em questão.

# Conclusão

Aqui chegados é inquestionável o quão imprescindível é atualmente o serviço de *E-Banking*, e o quão este serviço foi revolucionário para o setor bancário. Este acarreta um sem número de comodidades e benefícios ao utilizador e, ainda, uma economia considerável ao prestador de serviços.

O utilizador está, a nosso ver, no centro da evolução destes serviços, é com base nas necessidades e exigências destes que os serviços vão evoluindo e melhorando, tentando sempre trazer o melhor para o cliente. Com as demais atualizações é possível, atualmente, fazer uma panóplia de operações, todas de forma digital, que criam uma autonomia irreversível, a nosso ver, ao utilizador. Este avanço, como pudemos analisar ao longo do presente estudo, não ocorreu só a nível da própria entidade bancária, mas sim através da diversificação de canais, sendo que, no momento atual, são várias as aplicações de pagamento, criadas por empresas diversas dos bancos, disponíveis para o utilizador.

Não obstante esta revolução tecnológica, que abarcou no seu desenvolvimento inúmeras vantagens, também a ela estão associadas diversas desvantagens, de entre as quais, considerada pelos nossos legisladores como uma das mais relevantes – a fraude associada a este serviço de *E-Banking*, que permite o acesso indevido de um terceiro na conta do utilizador, sendo possível a movimentação de fundos, tudo isto sem a sua autorização. Aquilo que depreendemos desta análise é que, da mesma forma que os sistemas evoluem para positivo, o mesmo acontece para o lado inverso, tornando os sistemas cada vez mais inviáveis.

Conforme explanado supra, uma das principais preocupações dos nossos legisladores, não só nacionais, mas um bocado por toda a Europa, tem sido justamente a questão da cibersegurança. O RJSPME/DSP2, amplamente mencionado no presente estudo, vem exatamente nesse sentido, ou seja, no sentido de melhorar as formas de segurança dos sistemas, elevando assim a proteção do utilizador.

Foi no seio da responsabilidade, mencionada anteriormente, no âmbito das operações não autorizadas, que se focou maioritariamente o nosso trabalho. No entendimento de quem se considera responsável por estes prejuízos que, de acordo com a jurisprudência analisada, é, na maioria das vezes, imputada a culpa à entidade bancária.

Este é realmente um tema de importância a debater, uma vez que, apesar de todas as regras estipuladas no RJSPME/DSP2, limitadoras dos deveres de cada parte, que conduzirão à responsabilidade respetiva, é, ainda assim, questionável, de certo modo, algumas formas de responsabilização por parte do banco. Ora, no nosso entender, é bastante claro, com base no RJSPME/DSP2, quais são os requisitos a cumprir por parte do utilizador do *E-Banking* para que este seja responsabilizado. Contudo, tal não é tão facilmente categorizado para a entidade bancária. Quer isto dizer que, a nosso ver, e salvo melhor entendimento, sobre o banco recai sempre o ónus de prova, conforme observado. No entanto, nem sempre essa comprovação é de fácil acesso, uma vez que, dificilmente, o banco conseguirá comprovar que existiu algum tipo de negligência por parte do utilizador.

Ademais, e paralelamente a esta temática da responsabilização pelas operações fraudulentas no âmbito do *E-Banking*, estudámos ainda a mesma no âmbito da aplicação MBWay. Ora, também aqui, é questionável, no nosso entendimento, a responsabilidade das partes. Quem sai responsável por estas operações fraudulentas, a entidade bancária, o utilizador ou será que, em algum momento, poderá ser responsabilizada a SIBS?

Após o presente estudo, concluímos que, até ao momento não existe possibilidade de responsabilizar a SIBS. No entanto, questionamo-nos se não seria, de alguma forma, uma possibilidade de tal acontecer, isto porque, de certo modo, não é a entidade bancária que elabora os termos e condições daquela aplicação, nem, tão pouco, é chamada a intervir ao longo da efetivação das operações. No entanto, e apesar de tecnicamente o banco não poder ser responsável pelas burlas no MBWay, existem já casos com pedidos de reembolso no âmbito das mesmas, o que não nos parece correto.

Ainda a título de questão interna, surge-nos, desta vez relacionada com a proteção do utilizador, a seguinte: o acesso ao serviço de *E-Banking* está vedado através de um VPN – ligação com recurso a tecnologia de criptografia que permite manter seguros os dados de tráfego –, talvez não pudesse ser uma questão futura de análise enquanto solução à diminuição das fraudes *on-line*? Parece-nos que esta não será uma questão para um jurista mas, sim, para os técnicos de cibersegurança.

Não obstante todas as questões colocadas ao longo da presente dissertação, somos a acreditar que um dos principais fatores das burlas se deve, especialmente no âmbito do MBWay, à falta de literacia tecnológica que, no nosso entender, é fundamental para a boa utilização dos serviços. Esta formação e informação ser ministrada não só aos utilizadores,

mas, e essencialmente, aos colaboradores das entidades bancárias para que, aquando da ativação de um serviço de *E-Banking* por parte de um cliente, estes mesmo pudessem fornecer formação no sentido de melhorar o conhecimento daquele que utilizará o serviço, ou seja, de quem depende a boa prática de utilização.

Com esta exposição final não se pretende desvalorizar a evolução, pelo contrário, pretende-se questionar, pois apenas do questionamento surge a vontade de mudança.

Acreditamos que existem saltos tecnológicos que ainda não foram dados, conhecimentos ainda não descobertos, que estarão a ser estudados por quem de direito e que, através de um complemento de áreas, resultarão em espaços digitais mais seguros e completos, que tudo têm para criar um futuro de esperança.

# Bibliografia

Agostinho, A. (2016). *Banca Digital - Disponibilidade de Clientes e Influência da Inovação na Banca de Retalho.* Obtido em 25 de fevereiro de 2021, de Repositório Comum: https://comum.rcaap.pt/bitstream/10400.26/14549/1/Disserta%C3%A7%C3%A3o%20de%20M-GEE%20-%20Artur%20Agostinho%2050032300.pdf

Almeida, C. F. (2015). *Contrato Bancário Geral e Depósito Bancário.* Obtido em 07 de 07 de 2021, de Centro de Estudos Judiciais: https://elearning.cej.mj.pt/course/view.php?id=144&username=guest

Almeida, S. (2015). O regime jurídico português das comunicações comerciais eletrónicas não solicitadas (*spam*): breves notas. *Juristas do Mundo* – Série Excelência Jurídica, Vol. III, Editora Rede, Granada, pp. 515-526.

Alves, I. C. (2019). *Tese de Mestrado intitulada "Operações Abusivas na Banca Eletrónica"*.

Amaral, L. M. (2007). *Sociedade da Informação - O Percurso Português (Parte I).* Obtido em 8 de março de 2021, de APDSI: https://apdsi.pt/wp-content/uploads/prev/2-2.3_luis%20mira%20amaral_070626.pdf

Antunes, J. A. (2009). *Direito dos Contratos Comerciais.* Coimbra: Almedina.

Barreira, C. F. (2015). *A Repartição dos prejuízos decorrentes de fraude informática. Revista Nº 3.* Obtido em Outubro de 2021, de Centro de Investigação Juridico Económica: https://cije.up.pt//client/files/0000000001/2_683.pdf

Bóia, J. (2003). *Educação e Sociedade: Neoliberalismo e os desafios do futuro.* Lisboa: Edições Sílabo.

Cordeiro, A. M. (2008). *Manual de Direito Bancário, 3ª edição.* Coimbra: Almedina.

Ferrão, F. (2000). *E-Business.* Lisboa: Escolar Editora.

Guimarães, M. R. (1999). *As transferências eletrónicas de fundos e os cartões de débito.* Coimbra: Almedina.

Guimarães, M. R. (2011). *O contrato-quadro no âmbito da utilização de meios de pagamento eletrónicos.* Coimbra: Coimbra Editora.

Guimarães, M. R. (Janeiro de 2013). A repartição dos prejuízos decorrentes de operações fraudulentas de banca eletrónica (home banking) - Ac. do TRG de 23.10.2012, Proc. 305/09. *Cadernos de Direito Privado*.

Guimarães, M. R. (Janeiro de 2013). Cadernos de Direito Privado. *A repartição dos prejuízos decorrentes de operações fraudulentasde banca eletrónica (home banking): anotação ao Acórdão do Tribunal da Relação de Guimarães de 23.10.2012, Proc. 305/09.*

Junqueiro, R. (2002). *A Idade do Conhecimento: A Nova Era Digital (2ª ed.).* Lisboa: Editorial Notícias.

Macedo, L. (2005). *Políticas para a Sociedade da Informação em Portugal: Da Concepção à Implementação.* Obtido em 1 de março de 2021, de Biblioteca On-line de Ciências da Comunicação: http://www.bocc.ubi.pt/pag/macedo-lurdes-politicas-sociedade-informacao-portugal.pdf

Marques, G. &. (2006). *Direito da Informática. 2ª Edição.* Coimbra: Almedina.

Marques, G., & Martins, L. (2006). *Direito da Informática. 2ª edição.* Coimbra : Almedina.

Mattelart, A. (2001). *Histoire de la Societé de L'Information (2ª ed.).* Paris: Ed. La Découverte.

Meirelles, D. S. (Jan-Mar de 2006). *O Conceito de Serviço.* Obtido em 11 de janeiro de 2021, de Centro de Economia Política: https://centrodeeconomiapolitica.org/rep/index.php/journal/article/view/593

Monteiro, A. P. (2004). *Contratos de distribuição comercial.* Almedina.

Pereira, A. D. (2001). *Serviços da Sociedade da Informação: Alguns Problemas Jurídicos do Comércio Eletrónico na Internet.* Obtido em 01 de março de 2021, de Faculdade de Direito da Universidade Nova de Lisboa - Working Papers 2/01.

Santos, R. P. (2017). *As Fintech na Geração Millennials.* Obtido em 11 de março de 2021, de Repositório Comum: https://comum.rcaap.pt/bitstream/10400.26/23184/1/RicardoSantos_ISG.pdf

Santos, V. (2018). *As debilidades do serviço de homebanking, em especial quanto aos crimes de fraude informática de pishing e pharming. Aquestão da responsabilidade no âmbito das operações bancárias não autorizadas.* Universidade Católica Portuguesa de Lisboa.

Schwalbach, J. G. (2021). *Direito Digital.* Coimbra: Almedina.

Sousa, H. (2003). *Informação Internacional: Esboçando linhas de fronteira. In Cadernos do Noroeste, Série História, Nº 3.* Obtido em 27 de fevereiro de 2021, de CECS - Minho: http://repositorium.sdum.uminho.pt/bitstream/1822/1593/1/hsousa_ArtigoInformInternacional_2003.pdf

Varela, A. (2012). *Das Obrigações em Geral* (10ª ed., Vol. I). Coimbra: Almedina.

Vasconcelos, M. P. (2019). *Direito Bancário.* Coimbra: Almedina.

Vives, X. (2017). *The Impact of Fintech on Banking*. Obtido em 25 de fevereiro de 2021, de European Economy: https://european-economy.eu/2017-2/the-impact-of-fintech-on-banking/

Webster, F. (1995). *Theories of Information Society (4ª ed.).* Obtido em 27 de fevereiro de 2021, de https://cryptome.org/2013/01/aaron-swartz/Information-Society-Theories.pdf

Zaninelli, T. B. (2007). *A Utilização dos E-Services como Ferramenta para a Obtenção de Vntagem Competitiva nas Organizações.* Obtido em 11 de março de 2021, de Repositório Aberto da Universidade do Porto: https://repositorio-aberto.up.pt/bitstream/10216/11130/2/Texto%20integral.pdf

## Jurisprudência

Todos os acórdãos analisados encontram-se disponíveis para consulta em DGSI ou Direito em Dia

**Supremo Tribunal de Justiça**

- Acórdão de 18 de dezembro de 2013, Processo nº 6479/09.8TBBRG.G1.S1;
- Acórdão de 05 de abril de 2016, Processo nº 4640/11.4TBRG.G2.S1;
- Acórdão de 09 de junho de 2022, Processo nº 10/20.1PAENT.S1;

**Tribunal da Relação de Coimbra**

- Acórdão de 09 de novembro de 2004, Processo n.º 2278/04;
- Acórdão de 10 de setembro de 2013, Processo n.º 6/07.9TBPNH.C1;
- Acórdão de 17 de dezembro de 2014, Processo n.º 15/09.3TBPNC.C1;
- Acórdão de 17 de fevereiro de 2016, Processo 2119/11.TALRA.C2;
- Acórdão de 11 de fevereiro de 2020, Processo nº 8592/17.9T8CBR.C1;

**Tribunal da Relação de Guimarães**

- Acórdão de 23 de dezembro de 2012, Processo 305/09.5TBCBT.G1;
- Acórdão de 17 de dezembro de 2014, Processo 1910/12.8TBVCT.G1;

**Tribunal da Relação de Lisboa**

- Acórdão de 26 de outubro de 2010, Processo n.º 1943/09.1TJLSB.L1-7;
- Acórdão de 05 de novembro de 2013, Processo 9821/11.8T2SNT.L1-1;
- Acórdão de 12 de dezembro de 2013, Processo n.º 164/11.8TBSRT.L1-6;
- Acórdão de 30 de junho de 2011, Processo 189/09.3JASTB.L1-5;
- Acórdão de 17 de dezembro de 2014, Processo n.º 15/09.3TBPNC.C1;
- Acórdão de 15 de março de 2016, Processo 1063/12.1TVLSB.L1-1;
- Acórdão de 18 de dezembro de 2019, Processo 45/17.1PHSXL-3;

**Tribunal da Relação de Porto**

- Acórdão de 07 de dezembro de 2014, Processo 747/12.9TJPRT.P1;
- Acórdão de 10 de janeiro de 2023, Processo 1053/20.0T8MAI.P1;


## Sites Consultados


- www.direitoemdia.pt
- www.dgsi.pt/
- www.bportugal.pt
- www.internetsegura.pt
- www.mbway.pt
- www.sibsanalytics.com
- https://marketeer.sapo.pt/
- https://jornaleconomico.pt/
- infocursos.medu.pt/
- www.anacom.pt/
- www.acepi.pt/
- www.bancobpi.pt/particulares
- www.cgd.pt
- www.publico.pt
- www.multibanco.pt

## Formação Realizada

- Curso de Formação Avançada 2023: "Jurisprudência MBWay – Uma Análise Crítica", de 24 de maio de 2023. Formadora Dra. Inês Custódio Alves.