O *PHISHING* BANCÁRIO E A SEMELHANÇA ENTRE OS CENÁRIOS DAS JURISPRUDÊNCIAS BRASILEIRA E PORTUGUESA

THE BANKING PHISHING AND THE SIMILARITY BETWEEN THE SITUATION OF BRAZILIAN AND PORTUGUESE JURISPRUDENCE

Daniel Menah Cury Soares[1]

RESUMO: O presente artigo, decorrente de pesquisa teórica e prática, aborda o *phishing* bancário, uma fraude cada vez mais recorrente no Brasil e em Portugal. Ainda busca-se expor, de forma básica, os dois sistemas judiciários no que diz respeito à responsabilidade civil e direito do consumidor em suas normas. Por fim, há a análise e comparação de como o tema é abordado por ambos os poderes judiciários, que se mostram harmônicos em suas decisões.

PALAVRAS-CHAVE: Instituição bancária. *Phishing* bancário. Fraude. Responsabilidade Civil. Segurança digital.

RESUME: This article, resulting from theorical and pratical research, discourse about the banking phishing, an increasingly recurrent fraud in Brazil and Portugal. It still seeks to expose, in a basic way, the two judicial systems with regard to civil liability and consumer rights in their laws. Finally, there is analisys and comparison of how the topic is approached by both judicial sistems, wich are harmonious in their decisions.

KEYWORDS: Banking institution. Banking phishing. Fraud. Liability. Digital Security.

DATA DE RECEBIMENTO: 17/05/2021
DATA DE APROVAÇÃO: 10/12/2021

INTRODUÇÃO

É fato sabido (e até ultrapassado de se constatar) que o mundo está cada vez mais informatizado. Apesar de boa parte da população mundial não possui acesso à tecnologia, há cada vez mais dependência desta para as tarefas e negócios diários. Profissões consideradas ultrapassadas somem e novas demandas

[1] Advogado Júnior, graduado pela Universidade Brasil em 2017. Pós graduando em direito contratual pela Escola Paulista de Direito. Experiência como consultor contratual/processual em direito securitário e atuação no setor jurídico corporativo bancário cível e massificado. Contato: danielmenahadv@gmail.com.

surgem em seus lugares. Comunicações acontecem em tempo real, informações circulam em segundos. A globalização é a realidade.

Uma das áreas mais influenciadas pela tecnologia é a bancária. O *Internet Banking* certamente traz uma série de facilidades para o consumidor, como, por exemplo, a realização de transações que outrora dependiam do deslocamento até as agências bancárias (que trazia como ônus o tempo elevado de espera, horário limitado de funcionamento), consulta a qualquer tempo do saldo em conta, investimentos em tempo real, entre outros diversos benefícios.

No entanto, essa evolução tecnológica também se aplica à criminosos. Considerando que a segurança cibernética da área bancária é mais avançada e eficiente, estes avançaram na tecnologia para obter dados de consumidores e desviar seus recursos financeiros para si através de diversos ardis.

Apenas no mês de outubro de 2020, foram constatados mais de dois milhões de golpes virtuais no Brasil[2]. Muito da situação foi agravada pelas medidas de restrição de circulação impostas em decorrência da pandemia do COVID 19, de forma que o comercio eletrônico teve um grande crescimento[3] e, consequentemente, o número de fraudes virtuais. De acordo com a FEBRABAN (Federação Brasileira de Bancos), houve um aumento de 80% de tentativas de *phishings* bancários[4] (há ainda o agravante de que o brasileiro é considerado "ingênuo" ao navegar pela internet¸ o que indica muito do crescimento e efetividade dos golpes[5]). Em Portugal, a situação também é incomoda, com crescentes reclamações de golpes ano após ano[6].

No decorrer deste trabalho, será apresentado o *phising*, principal ataque utilizado por criminosos cibernéticos para obter dados de consumidores, driblar a

[2] 2,2 MILHÕES DE BRASILEIROS FORAM VÍTIMAS DE GOLPES VIRTUAIS EM OUTUBRO. Disponível em: https://canaltech.com.br/seguranca/2-2-milhoes-de-brasileiros-foram-vitimas-de-golpes-virtuais-em-outubro-174653/. Acesso em 16 nov. 2020.
[3] COMÉRCIO DIGITAL GANHA 57 MILHÕES DE CONSUMIDORES E VAREJO DIZ QUE ELES VIERAM PARA FICAR. Disponível em: https://www1.folha.uol.com.br/mercado/2020/07/comercio-digital-ganha-57-milhoes-de-consumidores-e-varejo-diz-que-eles-vieram-para-ficar.shtml. Acesso em 16 nov. 2020.
[4] GOLPES BANCÁRIOS PELA INTERNET CRESCEM 80% DURANTE A PANDEMIA, DIZ FEBRABAN. Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/09/18/golpes-bancarios-pela-internet-crescem-80percent-durante-a-pandemia-diz-febraban.ghtml. Acesso em 16 nov. 2020.
[5] ESPECIALISTAS: BRASILEIROS SÃO "INGÊNUOS" NO USO DA INTERNET. Disponível em: https://www.terra.com.br/noticias/tecnologia/internet/especialistas-brasileiros-sao-ingenuos-no-uso-da-internet,09685295fb6ea310VgnCLD200000bbcceb0aRCRD.html. Acesso em 16 nov. 2020.
[6] PORTUGUESES QUEIXAM-SE CADA VEZ MAIS DE FRAUDE BANCÁRIA. Disponível em: https://www.dn.pt/dinheiro/portugueses-queixam-se-cada-vez-mais-de-fraude-bancaria-10702661.html. Acesso em 16 nov. 2020.

segurança cibernética dos bancos e conseguir desviar seus recursos financeiros para si. Também será verificada a principal teoria contrária às pretensões das instituições bancárias em juízo e analisado o cenário jurisprudencial de Brasil e Portugal, demonstrando que haver alguma semelhança entre o atual entendimento das cortes dos dois países.

1 O PHISHING: CONCEITO E OCORRÊNCIA NO ÂMBITO BANCÁRIO

Celso Antonio Pacheco Fiorillo e Christiany Pegorari Conte explicam que o *phishing* (junção das palavras inglesas *password* e *fishing*) é "*um tipo de fraude cujo escopo é a obtenção de dados alheios. São difundidos através de spams ou de janelas publicitárias que surgem ao abrir determinados sites*"[7].

Os criminosos se utilizam de truques e mentiras para manipular terceiros e obter suas informações confidenciais, como se as "pescassem". Para isso, utilizam alguma "isca" para fisgarem vítimas desatentas: e-mails, SMS, aplicativos de troca de mensagens (o *Whatsapp*, por exemplo), sites falsos. O roubo de dados pode ocorrer através de vírus ou ao induzir a própria vítima à fornecer os dados. E um dos dados mais visados são os bancários.

Estes dados, por serem geralmente difíceis de obter (dada a forte segurança cibernética das instituições bancárias), costumam ser pescados diretamente da vítima. A maioria dos golpes (no Brasil) ocorre quando os criminosos replicam de forma muito fiel o site verdadeiro da instituição financeira (por muitas vezes, não tão parecido, mas geralmente o suficiente para ludibriar). Através deste site falso, a vítima acaba sendo direcionada para os golpistas, que, através de aplicativos de mensagens, telefonemas, e-mail ou SMS, acabam por induzir para que o consumidor da instituição financeira forneça os dados desejados e que possibilitem o desvio de valores.

7 FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. ***Crimes no meio ambiente digital e a sociedade da informação***. 2ª ed. Brasil, São Paulo: Saraiva, 2016. p. 198.

2 RESPONSABILIDADE CIVIL E DIREITO DO CONSUMIDOR: BREVE EXPLANAÇÃO E COMPARAÇÕES ENTRE OS SISTEMAS JURÍDICOS BRASILEIRO E PORTUGUÊS

2.1 PREVISÕES CONSTITUCIONAIS

Inicialmente, aponta-se que ambos os países possuem previsão expressa de proteção ao consumidor em suas Cartas Magnas.

Na constituição brasileira, a defesa ao consumidor é um dos princípios da ordem econômica, conforme previsto no artigo 170, inciso V[8], bem como um dever do Estado, nos termos do artigo 5º, inciso XXXII[9]. Já na constituição portuguesa, os direitos dos consumidores são abordados em seu 60º artigo[10].

Importante ressaltar que ambas as constituições fazem valer a proteção ali prevista através de leis infraconstitucionais.

2.2 PREVISÕES INFRACONSTITUCIONAIS E A RESPONSABILIDADE CIVIL

No Brasil, a responsabilidade civil objetiva, é pautada no artigo 186 do Código Civil: "*Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito*.". Aqui, nota-se a necessidade dos quatro requisitos clássicos para que nasça o dever de indenizar: a ação ou omissão, o dano, o dolo ou culpa e o nexo de causalidade entre os dois primeiros itens mencionados.

No mesmo códex privado, no artigo 927 e seu parágrafo único, encontra-se prevista a cláusula geral de responsabilidade subjetiva, sendo, neste caso, desnecessária a comprovação de dolo ou culpa:

---

[8] Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios: (...) V - defesa do consumidor;

[9] Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:[...] XXXII - o Estado promoverá, na forma da lei, a defesa do consumidor;

[10] Artigo 60.º

1. Os consumidores têm direito à qualidade dos bens e serviços consumidos, à formação e à informação, à proteção da saúde, da segurança e dos seus interesses económicos, bem como à reparação de danos.
2. A publicidade é disciplinada por lei, sendo proibidas todas as formas de publicidade oculta, indireta ou dolosa.
3. As associações de consumidores e as cooperativas de consumo têm direito, nos termos da lei, ao apoio do Estado e a ser ouvidas sobre as questões que digam respeito à defesa dos consumidores, sendo-lhes reconhecida legitimidade processual para defesa dos seus associados ou de interesses coletivos ou difusos.

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
> Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem.

Disposições semelhantes são localizadas no Código Civil Português, em seu 483º artigo:

> ARTIGO 483º (Princípio geral)
> 1. Aquele que, com dolo ou mera culpa, violar ilicitamente o direito de outrem ou qualquer disposição legal destinada a proteger interesses alheios fica obrigado a indemnizar o lesado pelos danos resultantes da violação.
> 2. Só existe obrigação de indemnizar independentemente de culpa nos casos especificados na lei.

No sistema jurídico brasileiro, ainda há o Código de Defesa do Consumidor (Lei 8.078 de 11/09/1990), que regula as relações de consumo, trazendo normas de proteção e defesa ao consumidor. Essa Lei conceitua o consumidor, em seu artigo 2º, como a "*pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final*".

A mesma lei conceitua fornecedor, produto e serviço em seu artigo 3º e parágrafos:

> Art. 3° Fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços.
> § 1° Produto é qualquer bem, móvel ou imóvel, material ou imaterial.
> § 2° Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista.

No âmbito consumerista, a responsabilidade civil adotada é a objetiva, de modo que se dispensa o requisito da culpa ou dolo, conforme se aufere dos artigos 12, 13,14, 18, 19 e 20 da lei.

A responsabilidade do fornecedor apenas é excluída nas situações elencadas nos incisos I e II do parágrafo 3º do artigo 14, quais sejam: quando não existir defeito no serviço prestado ou quando o dano for gerado por culpa exclusiva do consumidor ou de terceiros.

Semelhante disposição é encontrada no supramencionado Código Civil de Portugal:

> ARTIGO 570º (Culpa do lesado)
> 1. Quando um facto culposo do lesado tiver concorrido para a produção ou agravamento dos danos, cabe ao tribunal determinar, com base na gravidade das culpas de ambas as partes e nas consequências que delas resultaram, se a indemnização deve ser totalmente concedida, reduzida ou mesmo excluída.
> 2. Se a responsabilidade se basear numa simples presunção de culpa, a culpa do lesado, na falta de disposição em contrário, exclui o dever de indemnizar.

Também se apresenta à defesa do consumidor a "Teoria do Risco do Negócio" (ou Risco-Proveito), onde quem empenha atividade lucrativa deve arcar com os riscos que decorrem de tal atividade. Nas palavras de Flávio Tartuce:

> [...] é adotada nas situações em que o risco decorre de uma atividade lucrativa, ou seja, o agente retira um proveito do risco criado, como nos casos envolvendo os riscos de um produto, relacionados com a responsabilidade objetiva decorrente do Código de Defesa do Consumidor[11].

E, naturalmente, as instituições bancárias acabam por se enquadrarem nesta situação. No âmbito dos tribunais superiores brasileiro, o Superior Tribunal de Justiça estabelece em sua súmula de número 479 que "*As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias*.".

Em Portugal, muito da responsabilidade civil de matéria consumerista se pauta nas disposições do Código Civil, já que não há um código voltado especialmente para o direito consumerista. No entanto, há leis que abordam o tema.

A Lei 24/96 apresenta e estabelece o regime legal à defesa dos consumidores, com a definição do consumidor em artigo 2º:

> 1 - Considera-se consumidor todo aquele a quem sejam fornecidos bens, prestados serviços ou transmitidos quaisquer direitos, destinados a uso não profissional, por pessoa que exerça com carácter profissional uma actividade económica que vise a obtenção de benefícios.

[11] TARTUCE, Flávio. ***Manual de direito civil: volume único***. 8. ed. rev, atual. e ampl. São Paulo: Editora Forense, 2018. p. 600.

Ainda diversos direitos dos consumidores são estabelecidos a partir do artigo 3º da lei. Destaque-se o artigo 12, que impõe a responsabilidade objetiva do produtor[12]. Ainda sobre este tema, o Decreto Lei 383/89, que trata sobre a responsabilidade decorrente de produtos defeituosos, sendo o artigo 1º[13] desta norma quase idêntico ao supracitado artigo 12 da Lei 24/96.

Há também a definição do produtor, que, segundo o artigo 2º:

> 1 - Produtor é o fabricante do produto acabado, de uma parte componente ou de matéria-prima, e ainda quem se apresente como tal pela aposição no produto do seu nome, marca ou outro sinal distintivo.
> 2 - Considera-se também produtor:
> a) Aquele que, na Comunidade Económica Europeia e no exercício da sua actividade comercial, importe do exterior da mesma produtos para venda, aluguer, locação financeira ou outra qualquer forma de distribuição;
> b) Qualquer fornecedor de produto cujo produtor comunitário ou importador não esteja identificado, salvo se, notificado por escrito, comunicar ao lesado no prazo de três meses, igualmente por escrito, a identidade de um ou outro, ou a de algum fornecedor precedente.

No que diz respeito aos processos de fraudes ocorridas por *phishing* bancário no Brasil, o grande desafio das instituições financeiras (o que, logicamente, deve ser analisado em cada caso concreto) é se esquivar da responsabilidade, apontando exclusão de responsabilidade por culpa exclusiva de consumidor/terceiro, quando houver a identificação de tal ocorrência. Considerando todas as fases que são percorridas para que o *phishing* tenha êxito, há a necessidade de se comprovar ao magistrado que o golpe ocorreu (novamente, a depender do caso) por descuido da vítima, que forneceu seus dados aos fraudadores e não tomou medidas básicas de segurança digital, de tal forma que não possa atribuir o ato danoso ao alegado fortuito interno nas normas anteriormente elencadas.

[12] 5 - O produtor é responsável, independentemente de culpa, pelos danos causados por defeitos de produtos que coloque no mercado, nos termos da lei.
[13] O produtor é responsável, independentemente de culpa, pelos danos causados por defeitos dos produtos que põe em circulação.

3 O SEMELHANTE CENÁRIO JURISPRUDENCIAL NO BRASIL E PORTUGAL

Ao se analisar a jurisprudência de ambos os países acerca da responsabilidade sobre o *phishing* bancário, nota-se uma grande semelhança, senão um cenário idêntico.

O cenário português é dominado por decisões contrárias aos bancos. A maioria desses julgados dos Tribunais de instância superior (Coimbra, Évora, Lisboa, Guimarães e Porto) entendem que o ônus de comprovar a fraude é da instituição bancária, que possui superioridade financeira e técnica sobre o negócio[14][15][16][17], inclusive isentando o consumidor de culpa em casos de acesso à sites falsos, idênticos ao dos bancos[18]. Também é recorrente que se traga à baila a teoria do risco do negócio:

> No fundo, o legislador entendeu que o prestador de serviços é quem está em melhores condições, do que qualquer outro (incluindo o consumidor), para trazer a factualidade demonstrativa do modo como as coisas se passaram. E é assim, porque o funcionamento do "sistema informático" homebanking "pertencente à sua esfera de risco", funcionando como critério suplementar de distribuição do ónus da prova, ou, melhor dizendo, ao "círculo de vida" em que o facto se produz: é a consagração da denominada teoria das esferas de risco, que preconiza uma ligação umbilical entre o ónus da prova e a dicotomia obrigações de meios/obrigações de resultado. (Cf. Hugo

[14] PORTUGAL. Tribunal da Relação de Coimbra. **Apelação nº 8592/17.9TBCBR.C1**. Apelante: "C...". Apelados: "J..." e "R...". Relator Isaías Pádua. Coimbra, 11 de Fevereiro de 2020. Disponível em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/79b52c7da901f308802585110039aeef?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

[15] PORTUGAL. Tribunal da Relação de Coimbra. **Apelação nº 902/13.4TBCNT.C1**. Apelante: "Banco B..., SA". Apelados: "A..., LTDA". Relator Arlindo Oliveira. Coimbra, 02 de Fevereiro de 2016. Disponível em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/aba8f7cea02531c180257f4f003e6e54?OpenDocument. Acesso em 29. set. 2020.

[16] PORTUGAL. Tribunal da Relação de Lisboa. **Apelação nº 1952/15.1T8SXL.L1-1**. Apelante: "C..., SA". Apelados: "JP...". Relatora Ana Pessoa. Lisboa, 06 de Novembro de 2018. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6211b222ebc916c6802583bc005a6eb8?OpenDocument&Highlight=0,PHISHING. Acesso em 29. set. 2020.

[17] PORTUGAL. Tribunal da Relação do Porto. **Apelação nº 1482/17.7T8PRD.P2**. Apelante: "C...SA". Apelados: "C..." e "D...". Relatora Alexandra Pelayo. Porto, 06 de Novembro de 2018. Disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/2c4dc02af2630df08025843300487635?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

[18] PORTUGAL. Tribunal da Relação de Coimbra. **Apelação nº 5600/11.0TBLRA.C1**. Apelante: "BANCO...SA". Apelado: "V...". Relator Moreira do Carmo. Coimbra, 15 de Janeiro de 2019. Disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/83b3a02768fbc5428025839a00445513?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

> Luz dos Santos, “Plaidoyer por uma distribuição dinâmica do ónus de prova…”, cit., pág. 21 e segs)[19].

Também há decisão sobre a determinação de supressão de cláusulas contratuais que estipulavam a presunção de que operações bancárias fraudulentas eram autorizadas pelo consumidor/vítima:

> – No caso de terceiros, por meio desconhecido e fraudulento, lograrem obter os dispositivos de segurança e acesso a contas bancárias de cliente utilizador de serviços de pagamento (homebanking), não é adequado concluir, sem mais, ser tal quebra de segurança imputável ao utilizador desse serviço.
>
> – Se o banco réu não demonstrou, como era seu ónus, que o utilizador teve qualquer comportamento susceptível de pôr em causa a segurança do sistema, desconhecendo-se o modo como os terceiros lograram obter as chaves de segurança (número do contrato, código de acesso (password) e combinação de três números das 64 possíveis do cartão matriz), tem o mesmo a obrigação de reembolsar imediatamente o ordenante do montante da operação de pagamento não autorizada (art.º 71.º, n.º 1, do Regime dos Sistemas de Pagamento aprovado pelo Dec.-Lei n.º 317/2009, de 30 de Outubro e alterado pelos Decretos-Leis n.ºs 242/2012, de 7 de Novembro e 157/2014, de 24 de Outubro).
> **– São nulas e devem ser excluídas das Condições Gerais do contrato de utilização do serviço Caixadirecta on-line a que aludem os autos, por alterarem as regras de distribuição do risco e modificarem os critérios de repartição do ónus da prova (cf. artigos 12º, 20º e 21º, alíneas f) e g), do Dec.-Lei n.º 446/85, de 25 de Outubro), as cláusulas 9, 10 e 11 das referidas Condições Gerais, ao estabelecerem a presunção de que as operações bancárias realizadas fraudulentamente por terceiro foram consentidas e autorizadas pelo cliente.** (Sumário elaborado pelo Relator)[20](Grifei).

Segue-se interessante e didático julgado do Tribunal da Relação de Guimarães, onde se leva em conta o grau de negligência do consumidor vítima de *phishing*, concluindo-se que a vítima de negligência caracterizada como não-grave não assume o risco. Confira-se:

---

[19] PORTUGAL. Tribunal da Relação de Lisboa. **Apelação nº 18/18.7T8TVD.L1-6**. Apelante: "....BANCO SA". Apelado: "E F L”. Relator Deodato Brotas. Lisboa, 11 de Abril de 2019. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/49a0fa2be2741959802583e60054824e?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

[20] PORTUGAL. Tribunal da Relação de Lisboa. **Apelação nº 1318/09.2TBTNV.L1-6**. Apelante: “C... S.A.". Apelados: "G..." e “S...”. Relator Manuel Rodrigues. Lisboa, 21 de Dezembro de 2017. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8ef681e602628af1802582280031945b?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

I – É o prestador de serviços de pagamento quem tem a obrigação de assegurar que os dispositivos de segurança personalizados do instrumento de pagamento só sejam acessíveis ao utilizador que tenha direito a utilizar o referido instrumento, pertencendo o funcionamento do sistema informático de homebanking à esfera de risco daquele;
II – Com a publicação do Decreto-Lei nº 317/2009, de 30 de outubro, passou a existir uma regulamentação específica dos casos de operações de pagamento não autorizadas, ali se estabelecendo um regime especial de responsabilidade civil objetiva, segundo o qual o risco deve ser suportado pelos bancos, surgindo como regra o reembolso pelo prestador dos serviços;
III – Com vista ao afastamento da referida responsabilidade objetiva do prestador de serviços e de acordo com o Considerando 33) da Diretiva n.º 2007/64/CE, do Parlamento Europeu e do Conselho, de 13 de Novembro de 2007, transposta pelo diploma em análise, "para avaliar a eventual negligência cometida pelo utilizador dos serviços de pagamento, deverão ser tidas em conta todas as circunstâncias", devendo "as provas e o grau da alegada negligência" "ser avaliados nos termos do direito nacional";
IV – Face à doutrina portuguesa sobre esta matéria, "negligência grave" corresponde a "negligência grosseira, erro imperdoável, desatenção inexplicável, incúria indesculpável – vistos em confronto com o comportamento do comum das pessoas, mesmo daquelas que são pouco diligentes";
V – A circunstância de um utilizador do sistema de homebanking, desde a adesão, nunca ter efetuado nenhuma operação com o cartão-matriz, só utilizando o referido serviço para consultas – circunstância que permite considerar como natural que o mesmo não atentasse nos procedimentos relativos à utilização do cartão-matriz e aos alertas com tal utilização relacionados – associada à circunstância de, no momento do fornecimento dos dados do cartão-matriz, o utilizador não se encontrar no site do prestador de serviço, onde os avisos da entidade prestadora do serviço de homebanking surgem, deverão conduzir a considerar como não-grave a negligência do mesmo ao inconscientemente fornecer a terceiros, que para o efeito atuaram fraudulentamente, os dados do seu cartão-matriz.
[...]
XXXII. De modo a descortinar o significado e a abrangência do conceito de "negligência grave", o Ac. do Tribunal da Relação de Guimarães, de 17/12/2014, Proc. n." 1910/12.8TBVCT.G1, optou por colher e citar alguns autores da doutrina:
. Na opinião do Prof. Inocêncio Galvão Teles, a culpa grave apresenta-se como "uma negligência grosseira", pelo que "só por uma pessoa particularmente negligente se mostra suscetível de ser cometida".
. O Prof. Pinto Monteiro defende que o conceito de "negligência grave" concerne a atuações incompatíveis com os valores atinentes ao princípio da boa-fé, isto é, quando o devedor não observe "as regras elementares de prudência".
- A Prof.ª Ana Prata refere que culpa grave é o mesmo que "negligência grosseira, erro imperdoável. desatenção inexplicável, incúria indesculpável- vistos em confronto com o comportamento do

> comum das pessoas, mesmo daquelas que são pouco diligentes", aproveitando para citar René Savatier, que caracteriza a culpa grave como "uma conduta em que a má-fé é verosímil, mas não se encontra absolutamente demonstrada". . Alude ainda que conceito de "negligência grave" tem um sentido similar ao conceito de "negligência consciente" do Direito Penal, o qual se aproxima do conceito de "dolo eventual", e que é definido na alínea a) do artigo 15.° do Código Penal como o comportamento daquele que "por não proceder com o cuidado a que, segundo as circunstâncias, está obrigado e de que é capaz", representa como possível "a realização de um facto que preenche um tipo de crime" mas que atua "sem se conformar com essa realização".
> [...]
> **XXXVIII**. Em casos de fraude informática como o **phishing** e o pharming, tem-se entendido que, quando o utilizador do serviço de homebanking insere dados que são confidenciais em determinada página web, o faz movido pelo sentimento de confiança que deposita na própria instituição bancária. De facto, os hackers, quando engendram o modo de alcançar os seus objetivos, fazem-no de forma que a pessoa comum - cujos conhecimentos informáticos sejam básicos, tal como é o caso da Recorrente - seja induzida em erro e forneça a informação que pretendem, sem causar mínima desconfiança. Apenas uma pessoa muito experiente e muito conhecedora do meio de navegação em ambiente eletrónico é que poderia desconfiar de tal estratagema. Portanto, uma vez tratando-se de uma situação recorrente, em que várias pessoas são induzidas em erro, independentemente da idade, género e habilitações literárias que apresentam, não é correto afirmar que tal conduta - a inserção de dados bancários confidenciais em página web ou afim - evidencie negligência grave por parte dos clientes das instituições bancárias[21].

Este cenário se reflete e é confirmado pelo Supremo Tribunal de Justiça, depositando todo o ônus da fraude à instituição bancária[22].

No Brasil, são numerosos os julgados contrários aos bancos na matéria em anos anteriores nos vinte e sete Tribunais estaduais. Pouco provocado sobre o tema, o Superior Tribunal de Justiça manifestou-se no sentido de que o ônus da prova quando a discussão se referir à movimentação indevida de valores depositados em instituições financeiras é desta, dada a hipossuficiência do

[21] PORTUGAL. Tribunal da Relação de Guimarães. **Apelação nº 2406/17.7T8BCL.G1**. Apelante: "D.S.". Apelado: "CAIXA". Relatora Margarida Sousa. Guimarães, 21 de Dezembro de 2017. Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/2fb0937982d54b5e8025846c003767dd?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

[22] PORTUGAL. Supremo Tribunal de Justiça. **Recurso de Revista nº 1063/12.1VTVLSB.L1.S1**. Recorrentes/Recorridos: "AA", "LDA", "BB", "BANCO BB, SA". Relator Pinto de Almeida. Lisboa, 14 de Dezembro de 2016. Disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/d5a5e5113c6cb9238025808900501cda?OpenDocument&Highlight=0,PHISHING. Acesso em 30 set. 2020.

consumidor, bem como responderem por falha de segurança nas movimentações por internet[23].

No entanto, chama atenção recente crescimento de decisões em sentido contrário nos tribunais brasileiros, onde tem se verificado que vem sendo trazida à luz a negligência do consumidor (comportamentos contrários à segurança na rede[24]) como excludente de responsabilidade das instituições bancárias.

Seguem-se exemplos de negligência dos consumidores que acabaram por pesar na improcedência de seu pleito:

> E, ainda que o autor afirme haver questionado a financiadora sobre a divergência do sacador do boleto, pois aparecia o nome da segunda ré, nota-se que fez esse questionamento pelo aplicativo de mensagens. Logo, quem respondeu, que estava tudo "correto", foi o possível fraudador, uma vez que, repito, não há nenhum elemento que possa vincular aquele contato como feito com preposto da ré BV. Ora, em nenhum momento o autor afirma que entrou em contato com a ré pelos meios oficiais para esse tipo de negociação.
> Em conduta diferente, atraído pela proposta de quitação do veículo em valor inferior, aceitou o boleto enviado pelo WhatsApp para quitação do contrato, sem se preocupar com a autenticidade do canal de comunicação utilizado. Ademais, nem mesmo há nos autos elementos que evidenciem a possível conversa realizada via WhatsApp, já que não produziu nos autos nenhum print desta. Assim, pelos fatos narrados, restou demonstrado que o autor, na verdade, não adotou as cautelas mínimas necessárias para aferir a legitimidade do contato realizado, bem como do boleto bancário enviado[25].

E também:

> Em uma acurada análise dos autos, é fácil constatar que as mensagens de texto enviadas à autora são oriundas de terceiro fraudador.

[23] BRASIL. Superior Tribunal Regional. Agravo Regimental no Recurso Especial Nº 180.257. Agravante: Dawson Equipamentos Indústrias. Agravado: Itaú Unibanco s/a. Relator: Ministro Antonio Carlos Ferreira. Brasília, 7 de Dezembro de 2012. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/889927928/agravo-em-recurso-especial-aresp-180257-sp-2012-0103039-9/decisao-monocratica-889928005.Acesso em 01 out. 2020.

[24] Neste sentido: "*cumpre observar que, em casos envolvendo fraude, é necessária a apreciação das circunstâncias fáticas do dano-evento, a fim de perquirir a influência do comportamento das partes, sobretudo do consumidor, no que tange ao respeito às normas de segurança*.". BRASIL. Tribunal de Justiça de São Paulo. Apelação nº 1009532-74.2020.8.26.0100. APELANTE: Isac Silva de Melo. APELADO: Banco Safra S/A. Relator Marco Fábio Morsello. Julgado em 18 de Agosto de 2020. Disponível em: https://esaj.tjsp.jus.br/esaj/portal.do?servico=740000. Acesso em 15 out. 2020.

[25] BRASIL. Tribunal de Justiça de São Paulo. Apelação nº 1001273-16.2019.8.26.0233. APELANTE: Antonio Clécio Viana. APELADO: BV Financeira S/A – Crédito, Financiamento e Investimento. Relator Desembargador Hélio Nogueira. Julgado em 14 de outubro de 2020. Disponível em: https://esaj.tjsp.jus.br/esaj/portal.do?servico=740000. Acesso em 15 out. 2020.

> Neste sentido, basta uma breve observação do número emissor da mensagem, para perceber que se trata de número particular (fls. 25/27), cuja diferença, dos números genéricos do banco recorrente (fls. 29 e 33), é gritante.
> Não bastasse isso, o site fornecido na mensagem de texto enviada à autora (fl. 27 - mobylysantanderbr.com), é, no mínimo, incomum.
> Destarte, o "phishing" é fraude eletrônica com o objetivo do fraudador em obter dados pessoais, números de cartões de crédito, senhas das vítimas, etc., caso destes autos.
> Entretanto, tal golpe só é possível quando a vítima, acreditando tratar-se de endereço legítimo, se conecta ao link de acesso à pagina da internet, incontroversamente fraudulenta, fornecida pelo terceiro fraudador, e, após o acesso, preenche os dados requisitados pelo falsário.
> Assim, ainda que conste o nome do banco réu na mensagem de texto enviada à parte, a simples observação ao número emissor de tal notificação, assim como ao link fornecido por este, já são suficientes para levantar suspeitas acerca da informação enviada (fls. 27, 29 e 33).
> Desta forma, o conjunto probatório contido nestes autos não indica qualquer ilicitude no proceder do banco réu. Pelo contrário, evidencia a ocorrência de fortuito externo, rompendo o nexo de causalidade, e afastando a responsabilização do banco recorrente[26].

Por fim:

> Da análise dos autos revela-se evidente a culpa exclusiva da autora, que não adotou as cautelas necessárias ao proceder ao pagamento de valores a golpista que, sobrepujando com ardil a sua consciência crítica, conseguiu induzi-la a fazer um depósito, acreditando estar quitando a sua dívida. Com efeito, a demandante realizou toda a negociação via e-mail, fora dos canais oficiais da Serasa. Como bem constou na sentença, o e-mail no qual foi negociada a dívida não pertence ao Serasa, havendo, ainda, divergência quanto a assinatura, o que afasta a responsabilidade da demandada que não teve nenhuma interferência ou benefício com o ocorrido.
> Além do mais, o depósito foi realizado em favor de um terceiro estelionatário que tinha conta no Banco Agibank, sem qualquer relação com o credor (Banco Bradescard), não podendo ser imputada aos demandados qualquer responsabilidade pela fraude, como insiste a autora[27].

É possível verificar algumas decisões recentes neste sentido em Portugal:

[26] BRASIL. Tribunal de Justiça do Rio Grande do Sul. Apelação nº 0079041-30.2017.8.21.9000. APELANTE: Banco Santander Meridional S/A. APELADA: Paola Santos Bohlke. Relator Desembargador José Ricardo de Bem Sanhudo. Julgado em 20 de Fevereiro de 2018. Disponível em: https://www.tjrs.jus.br/novo/busca/?return=proc&client=wp_index. Acesso em 15 out. 2020.
[27] BRASIL. Tribunal de Justiça do Rio de Janeiro. Apelação nº 0029231-10.2018.8.19.0205. APELANTE: Juliana Carolina de Assis. APELADO: Banco Bradescard S.A. Relator Desembargador André Luiz Cidra. Julgado em 12 de Agosto de 2020. Disponível em: http://www4.tjrj.jus.br/ConsultaUnificada/consulta.do#tabs-numero-indice0. Acesso em 15 out. 2020.

> I) Tendo-se apurado que as transferências "sub judice" foram efectuadas fraudulentamente por terceiros, com recurso à técnica conhecida por phishing, logo se conclui que as mesmas não ocorreram por uma qualquer avaria ou deficiência do sistema informático da Ré/BANCO , como defende a Autora . E,
> II) Resultando provado que a utilização do serviço homebanking por banda da autora, se produziu com total desrespeito pela mesma das condições acordadas, maxime no que concerne às que se reportam à segurança , designadamente em sede de transmissão da totalidade dos dados do seu cartão matriz a terceiros, temos assim que ,
> III) Acaba em última análise a Ré/BANCO por provar a culpa da Autora e o seu incumprimento do contrato de homebanking - por violação das mais elementares regras de segurança impostas pelo mesmo - , logrando ilidir a presunção de culpa prevista no art. 799º nº 1 do Código Civil, que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta[28].

Segue ainda julgado oriundo do Tribunal de Relação de Guimarães:

> [...]
> V- O comportamento da Autora ao abrir um email que lhe pareceu proveniente do Banco réu, com o pedido de activação do cartão matriz, sendo-lhe solicitado, para o efeito, que acedesse a um link e introduzisse todos os dígitos do seu cartão, o que ela fez, tendo fornecido a totalidade das coordenadas que se encontram inscritas no cartão matriz, apesar de se encontrar inscrito no cartão matriz que utilizou para inserir todas as coordenadas o seguinte aviso: "Atenção: Nunca indique mais do que dois dígitos deste cartão matriz", mostra-se adequado a viabilizar a realização por terceiros de operações de pagamento não autorizadas.
> VI- Age com culpa o utente que fornece todo o conteúdo do cartão matriz perante uma solicitação numa página idêntica à do Banco, uma vez que contraria toda a lógica do sistema de segurança que não pode ser desconhecida por parte do utilizador.
> VII- Ao divulgar na internet a totalidade das combinações de algarismos que compõem o seu cartão matriz – apesar dos vários avisos e alertas de segurança que constam do cartão matriz, da carta que a Ré enviou à Autora com o cartão, do site da Ré na internet e da página de login do sistema "Net..." - a Autora actuou ao arrepio do contrato de homebanking a que aderiu e em violação de regras básicas de segurança nele previstas para a utilização do serviço "Net...", regras essas acessíveis à Autora, o que permitiu que

[28] PORTUGAL. Tribunal da Relação de Lisboa. **Apelação nº 19530/17.9T8LSB.L-8**. Apelante: "CAIXA ECONOMICA MONTEPIO GERAL". Apelados: "ERCÍLIA..." e "MANUEL...". Relatora Maria Amélia Ameixoeira. Lisboa, 01 de Outubro de 2020. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7610806de9ae00db802585fb003f2229?OpenDocument&Highlight=0,PHISHING. Acesso em 15 out. 2020

> terceiros se apoderassem dos seus elementos de segurança e assim lograssem aceder às contas bancárias tituladas pelas Autoras e efectuar operações fraudulentas.
> VIII- A actuação da Autora, ao inserir a totalidade das coordenadas inscritas no cartão matriz em página electrónica semelhante à do serviço de homebanking da Ré, fazendo uma utilização imprudente e descuidada daquele serviço, violando as regras de segurança impostas pelo respectivo contrato, tendo sido este comportamento causa directa da movimentação das suas contas bancárias por terceiros, configura negligência grave, preenchendo a previsão do artº. 72º, n.º 3 do RSP, pelo que lhe cabe a responsabilidade pelas operações de pagamento não autorizadas executadas, até ao limite do saldo disponível.
> IX- Por sua vez, a Ré, ao provar a culpa da Autora na transmissão da totalidade das coordenadas inscritas no cartão matriz a terceiros e, consequentemente, o seu incumprimento do contrato de homebanking por violação das mais elementares regras de segurança impostas pelo mesmo, ilidiu a presunção de culpa prevista no artº. 799º, nº. 1 do Código Civil que sobre si impendia, pelo que não é responsável pela movimentação das contas bancárias de forma fraudulenta[29].

Ainda que cada processo carregue uma carga fática própria e seu resultado dependa da análise pormenorizada dela, é inegável que há uma "fissura" em um cenário outrora tão rígido. Muito se deve a um entendimento mais preciso dos fluxos de sistemas bancários em geral, permitindo-se identificar algumas negligências de consumidores que venham à romper o nexo causal exigido para a responsabilização dos bancos.

No mais, ressalte-se que as instituições bancárias devem agir proativamente para auxiliar na diminuição de tais ocorrências, sendo o constante *take and down* contra sites fraudulentos e a educação digital (essencial em uma sociedade tão imersa em tecnologia) um ônus de tais empresas para buscar a diminuição das fraudes, economizando provisões e mantendo boa imagem perante o público.

CONCLUSÃO

Conclui-se que o cenário jurisprudencial entre ambos os países é muito parecido, com os judiciários analisando cada vez mais processos deste tipo, devido

[29] PORTUGAL. Tribunal da Relação de Guimarães. **Apelação nº 51/18.9T8PRG.G1**. Apelante: "Caixa". Apelados: "M.A." e "M.G.". Relatora Desembargadora Maria Cristina Cerdeira. Guimarães, 09 de Junho de 2020. Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/3b5685075cfb0e7280258596003abaa5?0OpenDocument&Highlight=0,PHISHING. Acesso em 15 out. 2020.

à alta dos ataques tecnológicos. Nota-se ainda o crescente número de decisões contrárias aos consumidores, resultante de maior conhecimento técnico da forma que o *phishing* ocorre, resultante de negligência de normas básicas de segurança virtual.

REFERÊNCIAS

2,2 MILHÕES DE BRASILEIROS FORAM VÍTIMAS DE GOLPES VIRTUAIS EM OUTUBRO. Disponível em: https://canaltech.com.br/seguranca/2-2-milhoes-de-brasileiros-foram-vitimas-de-golpes-virtuais-em-outubro-174653/. Acesso em 16 nov. 2020.

BRASIL. Superior Tribunal Regional. **Agravo Regimental no Recurso Especial Nº 180.257.** Agravante**:** Dawson Equipamentos Indústrias. Agravado: Itaú Unibanco s/a. Relator: Ministro Antonio Carlos Ferreira. Brasília, 7 de Dezembro de 2012. Disponível em: https://stj.jusbrasil.com.br/jurisprudencia/889927928/agravo-em-recurso-especial-aresp-180257-sp-2012-0103039-9/decisao-monocratica-889928005. Acesso em 01 out. 2020.

_____. Tribunal de Justiça de São Paulo. **Apelação nº 1001273-16.2019.8.26.0233**. APELANTE: Antonio Clécio Viana. APELADO: BV Financeira S/A – Crédito, Financiamento e Investimento. Relator Desembargador Hélio Nogueira. Julgado em 14 de Outubro 2020. Disponível em: https://esaj.tjsp.jus.br/esaj/portal.do?servico=740000. Acesso em 15 out. 2020.

_____. Tribunal de Justiça de São Paulo. **Apelação nº 1009532-74.2020.8.26.0100**. APELANTE: Isac Silva de Melo. APELADO: Banco Safra S/A. Relator Marco Fábio Morsello. Julgado em 18 de Agosto de 2020. Disponível em: https://esaj.tjsp.jus.br/esaj/portal.do?servico=740000. Acesso em 15 out. 2020.

_____. Tribunal de Justiça do Rio Grande do Sul. **Apelação nº 0079041-30.2017.8.21.9000**. APELANTE: Banco Santander Meridional S/A. APELADA: Paola Santos Bohlke. Relator Desembargador José Ricardo de Bem Sanhudo. Julgado em 20 de Fevereiro de 2018. Disponível em: https://www.tjrs.jus.br/novo/busca/?return=proc&client=wp_index. 15 out. 2020.

COMÉRCIO DIGITAL GANHA 57 MILHÕES DE CONSUMIDORES E VAREJO DIZ QUE ELES VIERAM PARA FICAR. Disponível em: https://www1.folha.uol.com.br/mercado/2020/07/comercio-digital-ganha-57-milhoes-de-consumidores-e-varejo-diz-que-eles-vieram-para-ficar.shtml. Acesso em 16 nov. 2020.

ESPECIALISTAS: brasileiros são “ingênuos” no uso da internet. Disponível em: https://www.terra.com.br/noticias/tecnologia/internet/especialistas-brasileiros-sao-ingenuos-no-uso-da-internet,09685295fb6ea310VgnCLD200000bbcceb0aRCRD.html.Acesso em 16 nov. 2020.

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital e a sociedade da informação**. 2ª ed. Brasil, São Paulo: Saraiva, 2016.

GOLPES BANCÁRIOS PELA INTERNET CRESCEM 80% DURANTE A PANDEMIA, DIZ FEBRABAN. Disponível em: https://valorinveste.globo.com/produtos/servicos-financeiros/noticia/2020/09/18/golpes-bancarios-pela-internet-crescem-80percent-durante-a-pandemia-diz-febraban.ghtml. Acesso em 16 nov. 2020.

GONÇALVES, Carlos Roberto. ***Direito civil brasileiro, volume 4: responsabilidade civil***. 12ª edição. São Paulo: Saraiva, 2017.

O DIREITO DO CONSUMIDOR EM PORTUGAL. Disponível em: https://www.conjur.com.br/2020-set-24/daniel-senna-direito-consumidor-portugal. Acesso em 16 nov. 2020.

O GUIA ESSENCIAL SOBRE PHISHING: como funciona e como se proteger. Disponível em: https://www.avast.com/pt-br/c-phishing. Acesso em 16 nov. 2020.

PORTUGAL É DOS PAÍSES ONDE OS UTILIZADORES SÃO MAIS ATACADOS POR PHISHING. Disponível em: https://www.itchannel.pt/news/seguranca/portugal-e-dos-paises-onde-os-utilizadores-sao-mais-atacados-por-phishing. Acesso em 16 nov. 2020.

PORTUGAL. Supremo Tribunal de Justiça. **Recurso de Revista nº 1063/12.1VTVLSB.L1.S1**. Recorrentes/Recorridos: “AA”, “LDA”, “BB”, “BANCO BB, SA”. Relator Pinto de Almeida. Lisboa, 14 de Dezembro de 2016. Disponível em: http://www.dgsi.pt/jstj.nsf/954f0ce6ad9dd8b980256b5f003fa814/d5a5e5113c6cb9238025808900501cda?OpenDocument&Highlight=0,PHISHING. Acesso em 30 set. 2020.

_____. Tribunal da Relação de Coimbra. **Apelação nº 5600/11.0TBLRA.C1**. Apelante: "BANCO...SA". Apelado: "V...”. Relator Moreira do Carmo. Coimbra, 15 de Janeiro de 2019. Disponível em http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/83b3a02768fbc5428025839a00445513?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

_____. Tribunal da Relação de Coimbra. **Apelação nº 8592/17.9TBCBR.C1**. Apelante: "C...". Apelados: "J..." e "R...". Relator Isaías Pádua. Coimbra, 11 de Fevereiro de 2020. Disponível em: http://www.dgsi.pt/jtrc.nsf/c3fb530030ea1c61802568d9005cd5bb/79b52c7da901f308802585110039aeef?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

_____. Tribunal da Relação de Coimbra. **Apelação nº 902/13.4TBCNT.C1**. Apelante: "Banco B..., SA". Apelados: "A..., LTDA". Relator Arlindo Oliveira. Coimbra, 02 de Fevereiro de 2016. Disponível em: http://www.dgsi.pt/jtrc.nsf/8fe0e606d8f56b22802576c0005637dc/aba8f7cea02531c180257f4f003e6e54?OpenDocument. Acesso em 29. set. 2020.

_____. Tribunal da Relação de Guimarães. **Apelação nº 2406/17.7T8BCL.G1**. Apelante: “D.S.". Apelado: "CAIXA”. Relatora Margarida Sousa. Guimarães, 21 de Dezembro de 2017. Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/2fb0937982d54b5

e8025846c003767dd?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

_____. Tribunal da Relação de Guimarães. **Apelação nº 51/18.9T8PRG.G1**. Apelante: “Caixa". Apelados: "M.A.” e “M.G.”. Relatora Desembargadora Maria Cristina Cerdeira. Guimarães, 09 de Junho de 2020. Disponível em: http://www.dgsi.pt/jtrg.nsf/86c25a698e4e7cb7802579ec004d3832/3b5685075cfb0e7280258596003abaa5?OpenDocument&Highlight=0,PHISHING. Acesso em 15 out. 2020.

_____. Tribunal da Relação de Lisboa. **Apelação nº 1318/09.2TBTNV.L1-6**. Apelante: “C... S.A.". Apelados: "G...” e “S...”. Relator Manuel Rodrigues. Lisboa, 21 de Dezembro de 2017. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/8ef681e602628af1802582280031945b?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

_____. Tribunal da Relação de Lisboa**. Apelação nº 18/18.7T8TVD.L1-6**. Apelante: "....BANCO SA". Apelado: "E F L”. Relator Deodato Brotas. Lisboa, 11 de Abril de 2019. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/49a0fa2be2741959802583e60054824e?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

_____. Tribunal da Relação de Lisboa**. Apelação nº 1952/15.1T8SXL.L1-1**. Apelante: "C..., SA". Apelados: "JP...". Relatora Ana Pessoa. Lisboa, 06 de Novembro de 2018. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/6211b222ebc916c6802583bc005a6eb8?OpenDocument&Highlight=0,PHISHING. Acesso em 29. set. 2020.

_____. Tribunal da Relação de Lisboa. **Apelação nº 19530/17.9T8LSB.L-8**. Apelante: “CAIXA ECONOMICA MONTEPIO GERAL". Apelados: "ERCÍLIA...” e “MANUEL...”. Relatora Maria Amélia Ameixoeira. Lisboa, 01 de Outubro de 2020. Disponível em: http://www.dgsi.pt/jtrl.nsf/33182fc732316039802565fa00497eec/7610806de9ae00db802585fb003f2229?OpenDocument&Highlight=0,PHISHING. Acesso em 15 out. 2020

_____. Tribunal da Relação do Porto. **Apelação nº 1482/17.7T8PRD.P2**. Apelante: "C...SA". Apelados: "C..." e "D...". Relatora Alexandra Pelayo. Porto, 06 de Novembro de 2018. Disponível em: http://www.dgsi.pt/jtrp.nsf/56a6e7121657f91e80257cda00381fdf/2c4dc02af2630df0802584330048763 5?OpenDocument&Highlight=0,PHISHING. Acesso em 29 set. 2020.

PORTUGUESES QUEIXAM-SE CADA VEZ MAIS DE FRAUDE BANCÁRIA. Disponível em: https://www.dn.pt/dinheiro/portugueses-queixam-se-cada-vez-mais-de-fraude-bancaria-10702661.html. Acesso em 16 nov. 2020.

SILVA, Marcelo Mesquita; BARRETO, Alesandro Gonçalves; KUFA, Karina. ***Cibercrimes e seus reflexos no direito brasileiro*.** Salvador: Editora Juspodivm, 2020.

TARTUCE, Flávio. **Manual de direito civil: volume único**. 8. ed. rev, atual. e ampl. São Paulo: Editora Forense, 2018.

_____; NEVES, Daniel Amorim Assumpção. ***Manual de direito do consumidor: direito material e processual*****.** São Paulo: Método, 2014.