PHISHING DO COMÉRCIO ELECTRÓNICO À RESPONSABILIDADE CIVIL BANCÁRIA POR FRAUDE.[1]

Willkenny Custódio[2]

"A tragédia não é quando um homem morre.
A tragédia é o que morre dentro de um homem quando ele está vivo"
Mário Sérgio Cortella

Resumo

O presente artigo tem como escopo analisar a responsabilização dos danos oriundos de prejuízos resultantes do *"phishing"* a nível da sociedade angolana, buscando, para tal, bases nas demais doutrinas a nível internacional e nacional. Com o desenvolver dos países conectados entre si e com o advento da globalização veio a surgir o termo *"E-Commerce"*, que se trata do comércio realizado através de meios eletrónicos. Por um lado, no polo positivo, trata-se de uma modalidade bem mais prática e até mesmo económica; entretanto, no polo negativo, os riscos pela insegurança dentro desta modalidade de comércio são inúmeros. Nos dias actuais, lojas virtuais são corriqueiras numa sociedade que com o passar dos dias torna-se cada vez mais depende da internet é possível comercializar produtos e serviços até mesmo por redes sociais, para a facilitação desde processo muitos recorrem à banca eletrónica, surgindo uma relação jurídica entre o banco e o clinte por meio do contrato de *internet banking*, neste, os contraentes procuram estabelecer uma forma do cliente movimentar os fundos da conta bancária recorrendo a meios informáticos. Este trabalho irá discorrer sobre o comércio eletrónico e consequentemente sobre a responsabilidade bancária em sede dos danos advindos de fraudes no sistema da banca eletrónica, culminando com o tratamento de dados pessoais do particular face à Lei de Proteção de Dados e a proteção que o consumidor poderá encontrar na Lei de Defesa do Consumidor, entre outros dispositivos jurídicos. Para o efeito, de modo a procedermos a delimitação do estudo, não trataremos das consequências penais advindas desta fraude eletrónica.

Palavras-chaves: Responsabilidade Bancária. Comércio Eletrónico. *Phishing*. Fraude. *E-Commerce*. Banca Eletrónica. Relação Jurídica. Internet *Banking*. Lei de Protecção de Dados. Lei de Defesa do Consumidor.

Abstract

[1] Artigo para a Revista Digital JuLaw – Direito e Justiça (www.julaw.co.ao).
[2] Licenciando em Direito pela Faculdade de Direito da Universidade Católica de Angola.

The purpose of this article is to analyze the liability of damages arising from losses resulting from "phishing" at the level of Angolan society, seeking for this basis in other doctrines at international and national level. With the development of the countries connected to each other and with the advent of globalization, the term “E-Commerce” emerged, which is the trade carried out through electronic means. On the one hand, on the positive side, it is a much more practical and even economic modality; however, on the negative side, the risks of insecurity within this type of trade are numerous. Nowadays, virtual stores are commonplace, in a society that with the passing of days becomes increasingly dependent on the internet it is possible to sell products and services even through social networks, for the facilitation of this process many resort to electronic banking, appearing a legal relationship between the bank and the customer through the internet banking contract, in this case, the contracting parties seek to establish a way for the customer to move funds from the bank account using computer means. This work will discuss e-commerce and, consequently, about bank liability for damages arising from fraud in the electronic banking system, culminating in the treatment of personal data of the individual in the face of the Data Protection Law and the protection that the consumer may enjoy. found in the Consumer Protection Law, among other legal provisions. For this purpose, in order to proceed with the delimitation of the study, we will not deal with the criminal consequences arising from this electronic fraud.

Keywords: Banking Responsibility. E-commerce. Phishing. Fraud. E-Commerce. Electronic Banking. Legal Relationship. Internet Banking. Data Protection Act. Consumer Protection Law.

1. Proémio

O ambiente virtual é um local fértil para a propagação de fraudes devido ao facto de que as relações comerciais são executadas via internet, tornando-se fácil de acontecer actos fraudulentos, sendo assim, acarretando diversos prejuízos aos consumidores. A banca eletrónica tem apresentado uma crescente popularidade nos últimos anos dada a sua grande utilidade visto que tem facilitado de forma bastante eficaz as relações comerciais na sociedade.

O ambiente comercial da internet possui características únicas que as distinguem das formas tradicionais de comércio, trazendo um novo paradigma, porém, o número de fraudes no *e-commerce* vem crescendo a cada dia com a utilização de técnicas cada vez mais práticas e ardilosas, o que demanda do sector um aprimoramento contínuo das ferramentas de análise de operações, dos sistemas anti-fraude e demais formas de segurança.

O consumidor que compra na internet também reclama na internet e a sua insatisfação pode chegar a muitas pessoas, uma vez que o ambiente virtual proporciona grande alcance e visibilidade, no entanto, essa reclamação pode não surtir efeitos práticos e reais uma vez que hodiernamente muitos sites ou lojas virtuais estão surgindo com uma

legalidade e segurança duvidosa, torna-se difícil colocar um facto em juízo para a resolução de um conflito se tal se mostrar inexistente de política de segurança.

As transações eletrónicas em Angola ainda exigem medidas significativas do poder legislativo no sentido de criar regras claras que regulem este tipo de comércio, facilitando a prática dos fornecedores, pois do outro lado, estão os consumidores, que são, em geral, a parte mais fraca da relação de consumo.

Relativamente às leis do Comércio Eletrónico em Angola, o quadro jurídico queixa-se de muitas deficiências até agora, e são regulamentos sobre determinadas leis que creio já existentes no sector das telecomunicações, no entanto, sem um impulso para a sua regularização e publicitação.

2. Conceitualização

2.1. *Phishing*

A palavra *phishing*, é uma corruptela do verbo inglês *fishing* (pescar, em português) é utilizada para designar alguns tipos de condutas fraudulentas que são comentidas na internet. São muito comuns as mensagens eletrónicas *(e-mails*), onde são feitas propagandas de vantagens financeiras, são ofertadas gratuitamente soluções técnicas para os diversos problemas, entre outras. Não sabe a pessoa que recebe tais tipos de artimanhas são enviadas por alguém disposto a aplicar um golpe.

Geralmente, alguns destinatários são convidados a clicarem sobre um *link* que aparece no corpo da mensagem ou abrir um arquivo anexo e, ao fazê-lo, aciona o *download* de um programa malicioso que vai penetrar no seu dispositivo e capturar informações sensíveis e extremamente pessoais, também são exigidos depósitos ou transferências bancárias (a exemplo do *site* de um banco, páginas ou sites sociais, sites de leilões, sites de comércio eletrónico). Tudo se passa por colocações de informações pessoais (número de cartão de crédito ou de dados bancários) e, uma vez na posse dessas informações, o fraudador as utiliza para fazer saques e movimentações bancárias ou outras operações (em nome da vítima).

A categoria delituosa em questão consiste exactamente nisso: em "pescar" ou "fisgar" qualquer incauto ou pessoa desavisada, não acostumada com esse tipo de fraude, uma forma de atrair a vítima (onde será perpetrado o golpe, de furto de suas informações pessoais). O *phishing*, portanto, é uma modalidade, em que a mensagem além de indesejada é também fraudulenta.

3. Breve Esboço Histórico

Podemos dizer que o *phishing* nasceu logo depois da *internet*, já que a internet foi estabelecida por volta de 1985 e em 1987 foi descrita a técnica de *phishing* pela primeira vez em um artigo do grupo HP Internacional. Porém foi somente em 1995, com o lançamento da AOHell como ferramenta de *phishing*, que a prática se fixou enquanto

tática de cibercrime. Já se vão 21 anos de actividade de uma técnica que evolui graças ao comportamento "inseguro" dos usuários. Em 2003 os ataques começaram a falsificar páginas, registrar domínios similares e até criar caixas de *login* e senha sobrepostas a páginas verdadeiras. Foi neste mesmo ano que as denúncias sobre o aumento nos ataques de *phishing* aumentaram assustadoramente. Desde 2001, os atacantes iniciaram os ataques a bancos. E até hoje as instituições bancárias são o principal alvo dos criminosos – ao mesmo tempo em que servem de isca para ataques de *phishing*.

Embora seja uma estratégia amplamente reproduzida e corriqueira – pois diariamente todos nós recebemos vários ataques de *phishing* por *e-mail* – a prática continua sendo desconhecida pela maior parte dos usuários da internet, o que torna este tipo de golpe ainda mais eficiente. O facto é que os ataques de *phishing* vêm causando sérios problemas, desde os anos 90 e até hoje não há uma forma de evitá-los, se não for através da mudança de comportamento dos usuários. Para evitar ser vítima desse tipo de fraude é importante reconhecer os perigos do *phishing*, compreender como os ataques são feitos e não acessar mensagens suspeitas.

4. Modalidades de Phishing

❖ Falsos e-mails ou mensagens

Essa modalidade é a mais comum e os outros casos do golpe acabam sendo uma espécie sua. Nela os saqueadores enviam *e-mails* aparentando tratar-se de empresas reais, como grandes bancos. Por exemplo: o usuário recebe uma mensagem dizendo que seus dados precisam ser actualizados, pois a conta bancária pode ser desactivada. Estas mensagens podem chegar via *WhatsApp* ou mensagem normal para dar uma maior credibilidade às vítimas.

❖ *Bitcoins*[3]

As criptomoedas[4] estão sendo muito usadas e os criminosos perceberam que seria um meio interessante de aplicar golpes por *phishing*. Nela normalmente os saqueadores utilizam sites disfarçados de serviços cambiais ou e-mails com oportunidade de compra que são aliciantes, no entanto, falsas.

❖ *Vishing*

Nesta modalidade, o telefone é a forma usada para atacar. Os saqueadores personalizam uma mensagem automática e fazem repetidas ligações para vários números diferentes. Mais uma vez, sob o pretexto de serem empresas onde os utentes estão

[3] É uma ***criptomoeda descentralizada*** ou um ***dinheiro eletrónico*** para transações ponto-a-ponto. É considerada a primeira moeda digital mundial descentralizada, constituindo um sistema económico alternativo e responsável pelo ressurgimento do sistema bancário livre.

[4] Uma ***criptomoeda*** é um meio de troca, podendo ser centralizado ou descentralizado que se utiliza da tecnologia de ***blockchain*** e criptografia para assegurar a validade das transações e a criação de novas unidades da moeda.

financeiramente vinculados (principalmente bancos), persuadem as pessoas a digitarem ou informarem dados pessoais.

- ***Spear Phishing***

Com essa modalidade, os saqueadores visam atingir um número menor de pessoas, mas a chance de sucesso termina sendo maior. São enviadas mensagens personalizadas com informações bem convincentes, como nome, sobrenome e outros dados, que levam o usuário a acreditar que está recebendo um *e-mail* legítimo de alguém familiar ou um agente de uma empresa.

Essas são apenas algumas modalidades de como os criminosos podem usar *phishing* para fazer vítimas.

5. Contrato de *Internet Banking* - Caracterização

Conhecido por *internet banking*[5], este serviço posto à disposição pela entidade bancária, possibilita aos seus clientes, mediante a aceitação de determinados requisitos a utilização de uma panóplia de operações bancárias *online*, relativamente às contas de que sejam titulares, utilizando para o efeito canais telemáticos que conjugam os meios informáticos com os meios de comunicação à distância através de uma página segura do banco, consubstanciando uma prestação de serviços, a subscrição ao *internet banking* faz-se mediante um contrato de adesão[6][7]e, com base nele, o cliente solicita à instituição bancária a utilização de um serviço informático de forma a movimentar os fundos depositados, surgindo o direito de utilizar este serviço apenas com a adesão ao contrato de banca eletrónica, mais precisamente a todas as condições de utilização previstas no contrato.

O contrato de *internet banking* é um contrato socialmente típico, mas legalmente atípico, uma vez que, apesar de não estar previsto na lei, é de tal forma solicitado pela prática[8]. Este modelo comum deriva, essencialmente, da utilização pelos bancos de cláusulas contratuais gerais muito semelhantes nos contratos de banca eletrónica. A doutrina portuguesa tem debatido em torno da caracterização ou natureza jurídica deste contrato, alguns caracterizando-o como contrato de adesão outros por contrato-quadro. Por se tratar de um acordo estabelecido entre uma instituição bancária e um cliente, segue o sistema adoptado pelos bancos para a celebração dos seus contratos. O recurso a este tipo de cláusulas contratuais gerais surge através de questões de economia de tempo,

---

[5] **Banco internético** (do inglês ***internet banking***), ***banco on-line***, ***on-line banking***, às vezes também ***banco virtual***, ***banco eletrónico*** ou ***banco doméstico***, são termos utilizados para caracterizar transações, pagamentos etc., pela internet. Esse sistema possibilita ao usuário utilizar os serviços do banco fora do horário de atendimento ou de qualquer lugar onde haja acesso à internet.

[6] "(...) o seu clausulado encontra-se pré-elaborado e é imposto à parte contratualmente mais fraca (cliente) que se limita a aceitar as condições pré-estabelecidas pelo outro contraente (Banco)"

[7] São aplicáveis a este contrato de adesão os mecanismos legais de proteção do consumidor e controlo das cláusulas contratuais gerais, mais precisament, a Lei nº 4/03, de 18 de Fevereiro e a Lei nº 15/03, de 22 de Julho.

[8] CORDEIRO, MENEZES. Tratado de Direito Civil Português. Tomo I. 3ª edição (reimpressão). Coimbra: Almedina, 2007, pp. 472-473.

rapidez e maior racionalização em termos legais e processuais. Segundo Maria Raquel Guimarães, entende-se por contrato-quadro, o contrato de base que visa definir as principais regras às quais irão ser submetidos acordos a celebrar sucessivamente no futuro – contratos de execução do contrato-quadro – destinado a preparar, facilitar e até potenciar a conclusão destes, mas com eles não se confundindo[9]. Este contrato estipula, assim, uma parte substancial do conteúdo de uma pluralidade de contratos contemporâneos ou futuros[1011]. A principal virtualidade desta figura consiste na reunião de diferentes contratos singulares celebrados em virtude da sua execução num único "vínculo jurídico" conseguindo-se desta forma prosseguir objectivos de simplificação e racionalização[12].

O contrato de *internet banking* é um contrato-quadro face às sucessivas operações de transferência eletrónica de fundos ordenadas através do serviço de banca eletrónica, pois, regula, prevê e simplifica as operações de pagamento a realizar no futuro com este instrumento de pagamento. Desde modo, sempre que é realizada uma operação de pagamento eletrónica através do serviço de *internet banking* é celebrado um novo contrato de execução do contrato-quadro de banca eletrónica. A celebração destes contratos de execução apenas se torna possível em virtude da adesão do cliente ao serviço de *internet banking* por via do contrato-quadro. O que sucede com o contrato de *internet banking* é o seguinte: no momento da sua celebração, os contraentes desconhecem quando emitirão ordens de pagamento no âmbito daquele serviço, em benefício de quem e quais os seus montantes. É mister existir uma renovação da vontade por parte do utilizador e do prestador de serviços em cada operação de pagamento, celebrando-se, por conseguinte, um contrato *ex novo*.

5.1. Relação Contratual

A vinculação entre o banco e o cliente gera uma relação obrigacional complexa de onde avultam direitos subjectivos, deveres primários de prestação, deveres secundários e deveres acessórios.

5.1.2. Deveres do Banco

- **Dever de emissão e entrega ao utilizador dos dispositivos segurança associados ao *internet banking***

[9] GUIMARÃES, MARIA RAQUEL., O Contrato-quadro...(2011), cit., p.62
[10] ALMEIDA, CARLOS FERREIRA., O Contrato bancário geral e depósito bancário, in Coleção de Formação Contínua – Direito Bancário, Lisboa: Centro de Estudos Judiciários (2015), cit., p.26.
[11] Podemos verificar que esta figura contratual potencia uma "multiplicadade de outros contratos subsequentes, simplificados, na sua conclusão e execução, através do recurso a meios electrónicos" GUIMARÃES, MARIA RAQUEL., A reparação dos prejuízos decorrentes de operações fraudulentas de banca electrónica *(home banking)*.
[12] GUIMARÃES, MARIA RAQUEL., O Contrato-quadro...(2011), cit., pp. 160-161.

Neste dever, o banco enquanto prestador do serviço obriga-se a emitir e a entregar à contraparte (cliente) os dispositivos de segurança associados, nomeadamente nome ou número de utilizador e códigos de acesso.

- **Dever de correcta execução das ordens de pagamento autorizadas**

No surgimento da vontade para requisição de um serviço de *internet banking*, o banco não conhece de antemão o momento em que serão emitidas ordens de pagamento através daquele, em benefício de quem, e quais os seus montantes. Significando isso que, a celebração do contrato de banca eletrónica não constitui uma autorização genérica para todas as ordens de pagamento que o utilizador deste serviço pretenda realizar[13].

- **Dever de manutenção de um serviço de internet banking**

Nesta e como em qualquer outra prestação de serviços com um pendor contínuo no tempo, o fornecedor deve efectuar manutenções, o mesmo ocorre com a prestação de *internet banking*, o dever de manter operacionais os sistemas informáticos que o sustentam, bem como de assegurar que não se verifiquem falhas técnicas durante as operações de pagamento, logo, estamos perante um dever acessório de conduta por parte da entidade bancária, a prestação de um serviço eficaz e seguro.

- **Dever de tornar intransmissível os códigos de acesso**

O banco deve assegurar que os mecanismos de segurança personalizados associados à conta bancária do cliente sejam intransmissíveis a outras pessoas. Isto é, o banco deve adoptar todas as medidas que estejam ao seu alcance para impedir que os códigos de acesso sejam interceptados por terceiros. Este dever encontra-se entrelaçado com o dever de segredo profissional, na medida em que os membros das instituições bancárias não devem revelar ou utilizar informações sobre factos ou elementos respeitantes à vida da instituição ou às relações desta com os seus clientes cujo conhecimento lhes advenha exclusivamente do exercício das suas funções ou da prestação dos seus serviços, designadamente: nomes dos clientes, as suas contas de depósito, respectivos movimentos e demais operações bancárias.

5.1.3. Deveres do Cliente

- **Dever de utilização correcta do serviço internet banking**

O cliente deve utilizar o serviço de *internet banking* de acordo com as condições que regem a sua emissão e utilização, este deve utilizar o serviço no limite da provisão

[13] GUIMARÃES, MARIA RAQUEL., (Ainda) a responsabilidade pelo uso indevido de instrumentos de pagamento electrónicos em operações presenciais e à distância (2015).

existente na sua conta bancária, no caso de ser uma conta à ordem[14], abstendo-se de efectuar operações a descoberto, salvo se tal tiver sido previamente acordado.

- **Dever de sigilo**

Este é um dever de confidencialidade por parte do cliente relativamente aos dados pessoais, sendo que estes permitem o seu acesso ao sistema de *internet banking.* Uma vez digitados os códigos de acesso, o sistema reconhece o utilizador do serviço de banca como legítimo portador.

6. Responsabilidade Civil Bancária por Fraude

Antes de nos debruçarmos sobre a responsabilidade civil bancária por fraude, é mister para o efeito, partirmos do regime jurídico da simulação constante do Código Civil para encontrarmos uma definição de fraude no âmbito do direito civil **(art. 240º nº 1 e 242º nº 1 do Código Civil)**, bem como o **art. 1245º do Código Civil** relativo à nulidade do jogo e da aposta. Nesta senda, para qualificar uma actuação como fraudulenta, é necessário o preenchimento cumulativo de dois elementos psicológicos – um comportamento deliberado que o torna doloso e a intenção específica de obter uma vantagem em prejuízo de terceiros, ou seja, para haver uma actuação fraudulenta, o sujeito deve visar, como fim imediato, retirar benefícios em prejuízo de terceiros. No âmbito do contrato de *internet banking*, a situação típica de uma actuação fraudulenta é a intromissão de pessoa não autorizada em determinada rede informática através de um meio informático, acompanhada da movimentação do saldo bancário para conta de terceiro[15]. Logo, este comportamento de intromissão e movimentação de valores em conta alheia torna-se fraudulento visto que, determinado sujeito realizou actos sem autorização do titular da conta, algo que faz-nos espécie e descartamos de primeira é a prática de um acto fraudulento pelo titular da conta, tal atitude poderá surgir, no entanto a fraude será contra o banco e não contra si, acarretando para tal sanções penais a si próprio.

O tema da responsabilidade dos bancos no ressarcimento dos prejuízos causados pelos ataques de *phishing* é realmente delicado e de interesse de todo o conjunto da sociedade, em razão da disseminação dos serviços de *Internet Banking* quando exista violação do sistema permitindo que um terceiro, alheio à relação jurídica bancária tenha acesso às quantias monetárias depositadas. Estamos perante um contrato de depósito bancário[16], ou seja, o particular transfere para o banco determinadas quantias monetárias, implicando essa uma transferência de propriedade da coisa transferida. Se na intervenção

[14] **Conta à ordem ou conta corrente** é uma conta de depósito mantida num banco ou outra instituição financeira por uma pessoa física ou jurídica com o propósito de segurança e rapidez de acesso à demanda através de uma variedade de diferentes canais.

[15] GUIMARÃES, MARIA RAQUEL. As transferências eletrônicas...

[16] De acordo ao **art.2º nº7 da Lei n.º 13/05 de 30 de Setembro** (Lei das Instituições Financeiras), **depósito** é contrato pelo qual uma entidade (depositante) confia dinheiro a uma instituição financeira bancária (depositária), a qual fica com o direito de dispor dele para os seus negócios e assume a responsabilidade de restituir outro tanto, com ou sem juro, no prazo convencionado.

ilícita do terceiro não pesa o comportamento do cliente, no sentido de ter facilitado aquela conduta ilícita, a responsabilidade é do banco. Nesta senda, numa situação de fraude informática – *phishing* – de dados de autenticação do cliente, o banco não pode afastar a sua responsabilidade invocando que a situação não ocorreu no seu sistema informático. Note-se que, não existindo comparticipação do particular na operação de fraude, a transferência de verbas para terceiro terá de ser considerada como uma transferência efectivada sem a autorização do titular, logo a responsabilidade da instituição bancária nestes casos implica o dever de indemnizar por danos patrimoniais e morais o cliente, nos termos do Código Civil.

7. Defesa do Consumidor

A proteção ao consumidor é um direito fundamental, portanto, o Estado tem o dever de garantir por meio de políticas públicas o acesso a órgãos específicos que possam resolver os problemas oriundos da relação comercial. A **Lei de Defesa do Consumidor (Lei nº 15/03 de 22 Julho)**, em seu **art.10º nº 2**, relativamente ao direito à reparação dos danos prevê que ***"o fornecedor de serviços responde, independentemente da existência de culpa pela reparação dos danos causados aos consumidores por defeitos relativos à prestação de serviços, bem como por informação insuficiente ou inadequada sobre sua fruição e riscos, excepto quando provar que, tendo prestado o serviço o defeito não existe ou haja culpa exclusiva do consumidor ou de terceiro"*** existindo uma responsabilidade objectiva dos fornecedores de serviços nas relações de consumo, **o art. 12º nº1** da referida lei é bem mais específico colocando a designação ***"por vício do serviço"*** sendo este de consumo duradouro ou não duradouro os fornecedores respondem solidariamente pelos vícios de qualidade ou quantidade[17] que os tornem impróprios ou inadequados ao consumo a que se destinam ou lhes diminuam o valor, salvo melhor opinião, abrimos aqui algumas reservas quanto ao disposto no **art. 10º nº 2**, na medida em que o mesmo abre uma exepção para a provação da inculpabilidade nas circunstâncias de o dano ter como causador um terceiro alheio à relação jurídica preexistente. Há também a atribuição do ônus da prova à entidade bancária. O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em conta as circunstâncias relevantes, tais como o modo de seu fornecimento, o resultado e os riscos que razoavelmente dele se esperam.

Culminando este ponto, todo e qualquer particular encontrará sempre protecção contratual na qualidade de consumidor, pois é seu direito à protecção dos seus interesses económicos, impondo-se nas relações de consumo a lealdade e a boa fé, nos preliminares, na formação e ainda na vigência do contrato de *internet banking*. A boa fé é um dever de conduta das partes com o objectivo de atingir ao máximo o equilíbrio, a segurança e a harmonia nesta relação. O princípio da boa fé nas relações de consumo, assim como todos

[17] Os **vício de qualidade** ocorrem quando o vício for impróprio, ou seja, toda vez que se mostre inadequado para os fins que razoavelmente dele se espera, não atinja sua finalidade, bem como quando não atendam as normas regulamentares de prestabilidade. No **vício de quantidade**, o produto com o conteúdo líquido inferior às indicações constantes do recipiente, da embalagem, rotulagem ou de mensagem publicitária, respeitadas as variações decorrentes de sua natureza.

os princípios aqui relacionados ou não, devem servir como parâmetro de conduta não apenas no tipo de relação ora debatida, mas, em todas as obrigações decorrentes das mais diversas actividades, servindo como um meio de valoração do comportamento tanto dos fornecedores como dos consumidores, a fim de atingir a harmonia e o equilíbrio entre as partes. A responsabilidade pelo serviço é a responsabilidade que tem como facto gerador o defeito, ou seja, a insegurança que tornou o serviço passível de sofrer ataques fraudulentos, logo, a instituição bancária sendo fornecedora deste serviço, imediatamente se imagina que a responsabilidade civil imputada a esta será sempre objectiva – contudo, existem alguns pontos controversos na doutrina.

8. Protecção de Dados Pessoais

Entende-se por protecção de dados pessoais, a possibilidade de cada cidadão determinar de forma autónoma a utilização que é feita de seus próprios dados pessoais, em conjunto com o estabelecimento de uma série de garantias para evitar que estes dados pessoais sejam utilizados de forma a causar discriminação, ou danos de qualquer espécie, ao cidadão ou à coletividade. É importante ressaltar uma diferenciação vital entre três tipos de dados:

1. Dados pessoais são aqueles relacionados a pessoas identificadas ou identificáveis;
2. Dados anónimos são os que perderam a sua capacidade de associação a uma pessoa física;
3. Dados pseudonomizados são aqueles que, com a aplicação de diferentes estratégias de protecção, à primeira vista, podem parecer anónimos, mas na realidade, permitem que o processo de anonimização seja revertido.

Em Angola, a Agência de Protecção de Dados (APD) entrou em funcionamento no dia 8 de Outubro de 2019, com a tomada de posse do Conselho da Administração, um mês depois da criação da instituição pelo Titular do Poder Executivo. A Agência de Protecção de Dados é uma pessoa colectiva de direito público dotada de personalidade jurídica, com autonomia financeira, administrativa e patrimonial, cuja missão é apoiar o Governo, tal é regida pela **Lei nº 22/11 de 17 de Junho (Lei da Protecção de Dados Pessoais)**, a mesma tem o seu âmbito de aplicação subjectiva e territorial previsto no **art. 3º** cuja a aplicabilidade é efectuada por qualquer pessoa e entidade do sector público, privado ou cooperativo pelo que concluímos a aplicação às instituições bancárias tal como rege o **art. 2º nº 11º da Lei das Instituições Financeiras (Lei nº 13/05 de 30 de Setembro)**. Nos termos do **art. 6º nº 1**, o tratamento de dados pessoais deve processar-se de forma transparente e em estrito respeito pelo princípio da reserva da vida privada bem como pelos direitos, liberdades e garantias públicas fundamentais previstos na Constituição da República de Angola e na presente lei. Tal deve ser efectuado de forma lícita e leal, com respeito pelo princípio da boa fé **(art. 7º nº 1).**

As instituições bancárias devem garantir adequados níveis de segurança e de protecção dos dados pessoais dos titulares dos dados. Para o efeito, devem adoptar

diversas medidas de segurança de carácter técnico e organizativo, de forma a proteger os dados pessoais contra a sua perda, difusão, alteração, tratamento ou acesso não autorizados, bem como contra qualquer outra forma de tratamento ilícito, pois é clara a responsabilidade dos bancos assegurar tais medidas, de modo a não perder credibilidade por parte dos seus clientes, estes devem munir-se de materiais bélicos contra-ataques de *phishing*. Os riscos pela utilização da internet são eminentes. Uma das grandes motivações dos criminosos internautas é a procura pelo enriquecimento ilícito, através da manipulação de dados eletrónicos pessoais dos utilizadores da *Web*. Sendo o *internet banking* uma ferramenta que se move com a *internet*, não fica aquém dessa ameaça. Os dados pessoais são tratados para finalidades determinadas, explícitas e legítimas para as quais foram recolhidos, não podendo ser posteriormente tratados de forma incompatível com essas finalidades, ressaltando aqui o **princípio da finalidade** previsto no **art. 9º** da referida lei. É mister pautar pelo impedimento do acesso de pessoa não autorizada aos ficheiros e às instalações utilizadas para o tratamento desses dados.

Os responsáveis pelo tratamento de dados pessoais, bem como as pessoas que, no exercício das suas funções, tenham conhecimento dos dados pessoais tratados, ficam obrigados a sigilo profissional, mesmo após o termo das suas funções. Sobre o mote, cabe ainda ressaltar que qualquer pessoa que tiver sofrido um prejuízo devido ao tratamento ilícito de dados ou a qualquer outro acto que viole disposições legais em matéria de protecção de dados pessoais tem o direito de obter do responsável a reparação pelo prejuízo sofrido.

Luanda, aos 21 de Agosto de 2020

Willkeny Custódio

Referências Bibliográficas

ALMEIDA, Carlos Ferreira. O Contrato Bancário Geral e Depósito Bancário in Coleção de Formação Contínua – Direito Bancário, Lisboa: Centro de Estudos Judiciários (2015).

BOBO, Kikufi Matondo. Comércio Eletrónico em Angola: Impacto e Desafio face à Internacionalização de uma Empresa de Transporte Aéreo – Caso TAAG. Porto, Maio de 2014.

CORDEIRO, António Menezes. Direito Bancário. Almedina, Coimbra (2014).

CORDEIRO, António Menezes. Tratado de Direito Civil Português. Tomo I. 3ª edição (reimpressão). Coimbra: Almedina, 2007

ESTEVES, Jean Soldi. A Responsabilidade Civil nos Contratos Bancários. São Paulo: LTr, 2011.

FREITAS, Lorraine V. G. de. A Responsabilidade Civil dos Intermediadores de Compras na Internet: E-Commerce. Itaperuna-RJ, 2019.

GUEDES, Edmárcio Cerqueira. Fraudes no Internet Banking: Conceituação e Estado Atual dos Mecanismos de Defesa. São Paulo, 2009.

GUIMARÃES, Maria Raquel. O Contrato-quadro no Âmbito da Utilização de Meios de Pagamento Eletrónicos. Coimbra Editora. 2011.
HILÁRIO, Esteves Carlos. Noções Preliminares de Direito do Consumidor. Fac. Simile Editora. Luanda. 2016.
NUNES, Elisa Rangel. Direito Bancário in Revista Direito de Angola. Universidade Agostinho Neto. Faculdade de Direito. Luanda, 2014.

Sites
www.juscertus.blogspot.com/2013/08/contrato-de-homebanking.html?m=1