RESPONSABILIDADE CIVIL DAS INSTITUIÇÕES FINANCEIRAS NA SOCIEDADE 4.0 E A GESTÃO DE RISCO NA ERA DIGITAL

Civil Liability of Financial Institutions in Society 4.0 and Risk Management in the Digital Age
Revista de Direito Bancário e do Mercado de Capitais | vol. 110/2026 | Jan - Jun / 2026
DTR\2026\932

Alexandre Borges Leite
Mestre em Direito Comercial. Advogado. a.leite@rochaleiteadvogados.com.br

Fretz Sievers Junior
Mestre em Direito Administrativo, Mestre e Doutor em engenharia de computação, Advogado. fretz.sievers@gmail.com

Mario Alexandre Gazziro
Doutor em Física Computacional, professor de engenharia da informação na UFABC. mario.gazziro@ufabc.edu.br

Área do Direito: Civil; Bancário; Digital
Resumo: A Responsabilidade Civil das Instituições Financeiras na Sociedade 4.0 é um tema complexo e cada vez mais relevante no cenário jurídico e tecnológico atual exigindo inovações constantes com as novas tecnologias. A crescente digitalização dos serviços bancários, embora traga inúmeros benefícios em termos de comodidade e eficiência, também acarreta novos riscos e desafios, especialmente no que diz respeito à segurança e à proteção dos dados dos clientes, sendo necessária uma análise sobre sua responsabilidade objetiva, como determina a Súmula 479 do STJ. Na sociedade há pessoas que têm facilidade por tecnologia de informação intituladas com tecnofilia e as que tem medo ou não gostam intituladas com tecnofobia, mas precisam dos serviços oferecidos que se encontram informatizados que muitas vezes não há outra forma de ter acesso, tendo a necessidade de ter um dispositivo móvel, para ter acesso aos serviços das instituições financeiras, e precisam de ajuda para conseguir acessar os recursos ou até mesmo benefícios do governo e podem estar sujeitos a golpes por falta de conhecimento.

Palavras-chave: Direito Comercial – Direito bancário – Inteligência artificial – Sistemas de informação.
Abstract: The Civil Liability of Financial Institutions in Society 4.0 is a complex and increasingly relevant topic in the current legal and technological landscape, bringing constant innovation with new technologies. The increasing digitalization of banking services, while bringing considerable benefits in terms of convenience and efficiency, also poses new risks and challenges, especially regarding the security and protection of customer data. Therefore, an objective analysis of their liability is required, as determined by Superior Court of Justice (STJ) Summary 479. In society, there are people who are comfortable with information technology advertised as technophilia, and those who are afraid or dislike it due to technophobia, but who need the services offered, which are computerized and often have no other way to access them. They require a mobile device to access financial institution services. They also need help accessing resources or even government benefits, and may be subject to scams due to a lack of knowledge.

Keywords: Commercial law – Banking law – Artificial intelligence – Information systems.

Para citar este artigo: LEITE, Alexandre Borges; SIEVERS JUNIOR, Fretz. Responsabilidade Civil das Instituições Financeiras na Sociedade 4.0 e a gestão de risco na era digital. *Revista de Direito Bancário e do Mercado de Capitais.* vol. 110. ano 29. São Paulo: Ed. RT, jan./jun. 2026. Disponível em: [URL]. Acesso em: DD.MM.AAAA. Confira as informações gerais da Revista: [https://www.thomsonreuters.com.br/pt/juridico/webrevistas.html]

Sumário:

1 Introdução

Mudanças sociais estão acontecendo de forma constante e muitas vezes não são percebidas por todos através das inovações tecnológicas, seja cada vez mais pelo uso de telefones inteligentes, que antes na sua versão inicial, tinha somente a função de fazer e receber chamadas a distância, tendo um custo elevado na prestação de seus serviços. Atualmente surgem os telefones inteligentes intitulados *smartphones* que além das suas funções básicas de enviar e receber chamadas por voz, são computadores móveis que podem fazer inúmeras funções, inclusive transações bancárias, tendo terminais de pronto atendimento em qualquer lugar e a qualquer hora, sem a necessidade de ir a uma agência bancária.

Essas inovações tecnológicas trazem modificações na contratação de produtos e serviços como por exemplo os contratos eletrônicos, conforme ensina Rebouças (2016). A Sociedade 4.0, com ampla utilização de sistemas de informação, oferece diversos serviços através da utilização de software desktop e aplicativos móveis com a promessa de que cada vez menos, seja mais necessário o auxílio humano de um analista de suporte ou aquele que faça a sua vez. As aplicações oferecem de forma organizada opções de um catálogo de serviços, utilizando uma arquitetura de informação que permite disponibilizá-las de uma forma mais intuitiva, facilitando o seu acesso. Sendo que os contratos podem ser assinados de forma eletrônica conforme a MP 2200-2/2001, que institui a Infra-Estrutura de Chaves Públicas Brasileira e do Decreto 10.278/2020 (LGL\2020\2456), sendo as assinaturas consideradas válidas, vinculantes e executáveis, desde que firmadas pelos representantes legais das partes.

A StatCounter[1], oferece estatísticas através de dados agregados coletados em uma amostra de mais de 5 bilhões de visualizações de página por mês, com mais de 1,5 milhão de sites que propicia estatísticas atualizadas e disponibilizadas, através do seu algoritmo, consegue informar a quantidade de dispositivos dos usuários no Brasil, afirma que entre os dispositivos utilizados, 64,48% são dispositivos móveis, 34,86% são computadores de mesa e somente 0,66% são *tablets*. A computação móvel já ultrapassou o uso dos computadores de mesa no Brasil permitindo que os sistemas de informação sejam acessados em diferentes lugares, verificando sua localização através dos sistemas de GPS – *Global Positioning System,* presentes nos smartphones, permitindo saber a localização do usuário, para ser um dado utilizado para validar sua segurança, através de um histórico de acessos de localidade costuma utilizar os serviços bancários, para compra ou pagamentos.

Com os avanços tecnológicos surge a tecnofilia que conforme AGUIAR (2025) e DE MENEZES (2025), é uma afinidade com um grande interesse pela tecnologia, em especial as novas tecnologias de informação tendo uma facilidade com sistemas de informação, facilitando suas tarefas no cotidiano, ajudando no acesso a informações, de produtos e serviços, facilitando o acesso aos serviços digitais tais como agências bancárias e acesso aos serviços do Governo Digital[2], que apresenta como dados oferecidos ao cidadão 4752 serviços digitais, 3100 sistemas integrados na conta, 285,6 milhões de assinaturas eletrônicas, 169 milhões de contas ativas, sendo serviços totalmente gratuitos.

Em contrapartida, conforme pesquisa recente realizada pelo INAF – Instituto Nacional de Analfabetismo Funcional[3], realizado uma pesquisa no ano de 2024, utilizando telefones inteligentes. Foi realizado uma pesquisa, visando avaliar as habilidades digitais, sendo proposta três tarefas: a primeira foi a realização de compra em um comércio eletrônico, segunda tarefa proposta foi escolher um filme em uma plataforma digital e a última o preenchimento de um formulário para um festival de música, avaliando os seguintes itens: habilidades operacionais em que consiste como saber utilizar a interação com o sistema de informação, o trato com a informação em entender o que está escrito e por fim a produção de conteúdo quando há necessidade de responder um questionamento realizado pelo sistema, realizando interação, comunicação e colaboração.

Entre os pesquisados 48% das pessoas entre 50 e 64 anos tiveram um baixo desempenho nos testes digitais, acertando entre zero e pelo menos uma das três tarefas propostas na avaliação. Outros 46% ficaram na média, acertaram acima de 1/3 e até 2/3 do teste, e apenas 6% obtiveram alto desempenho, ou seja, acima de 2/3 ou mais dos itens. Isso indica um baixo engajamento no uso de ferramentas digitais o que afeta diretamente aos brasileiros a terem acesso ao governo eletrônico tais como os serviços oferecidos pelo E-Gov[4], que garante a identificação de cada cidadão aos serviços digitais do governo, como um importante recurso a assinatura digital que permite firmar negócios jurídicos, através da assinatura digital.

Para os serviços bancários se faz necessário a segurança digital conhecida como *cibersecurity*, em que consiste em utilizar tecnologias visando garantir os pilares da segurança da informação que confidencialidade, integridade, disponibilidade, autenticidade e não repúdio, garantindo a proteção dos dados que trafegam nos meios digitais em conformidade com a Lei Geral de Proteção de Dados Lei 13.709 de 14 de agosto de 2018 (LGL\2018\7222), alterada pela Lei 13.709, de 14 de agosto de 2018 (LGL\2018\7222), para dispor sobre a proteção de dados pessoais.

Em 2024, teve-se 412.528 ocorrências com celulares subtraídos no Estado de São Paulo, conforme apresentado na Secretaria de Segurança Pública[5]. Em 2025 temos 165.533, ocorrências com celulares, sendo um número bem menor considerando o ano passado, porém é um número considerável e se faz necessário cuidados e

prevenção com os aparelhos, pois há inúmeras funcionalidades nos celulares como aplicações bancárias, acesso a cartões de crédito e débito, acesso a benefícios do INSS – Instituto Nacional de Seguridade Social, realização de empréstimos, pagamento de contas, transferência, gerando inúmeros problemas para os seus proprietários, além do prejuízos com o aparelho subtraído.

Neste cenário tem-se a tecnofobia, que é ao contrário da tecnofilia, em que consiste em dificuldades com este mundo digital, como um medo ou rejeição da tecnologia em especial a tecnologia da informação em que os serviços governamentais estão cada vez mais digitalizados e se faz necessário um conhecimento para ter acesso aos serviços, ficando a margem dos benefícios gerados pela tecnologia. E se faz necessário recursos do mundo digital tais como a cibersegurança que se trata de uma segurança lógica *security* e a segurança física *safety* pensando em possíveis roubos, furtos ou perdas e como proteger o acesso aos seus recursos, tão importantes na convivência no mundo moderno acessando os diferentes serviços oferecidos em uma sociedade cada vez mais conectada aos serviços digitais.

Outra questão são os dados que se encontram nos dispositivos móveis que possibilitam ter acesso aos seus dados, gerando problemas para seus usuários que tem seus aplicativos invadidos ou suas contas sequestradas que comprometem a sua identidade virtual, através de suas redes sociais, acesso a contas bancárias, seus cartões de crédito, passar pela pessoa através de assinaturas digitais ou mesmo ter acesso a informações sensíveis como dados de sua saúde e de sua intimidade. Neste artigo iremos focar nas aplicações bancárias e acesso a benefícios que seus usuários estão sujeitos e que através de golpes pode-se gerar fobia no uso desses dispositivos.

Este artigo trata sobre os serviços encontrados no governo eletrônico e que estão relacionados aos aplicativos bancários como o recebimento de benefícios do INSS ou mesmo para aumentar a confiabilidade de sua conta, tendo níveis de acesso como bronze, ouro ou prata para acessar novos serviços, atendendo o acesso aos diversos serviços oferecidos para a sociedade e o acesso aos seus benefícios através dos bancos.

2 Alguns serviços digitais governamentais relacionados às instituições financeiras oferecidas ao cidadão

O Governo Digital no Brasil tem trabalhado em conjunto com as instituições financeiras para aprimorar o atendimento aos cidadãos, tornando os serviços mais acessíveis, eficientes e seguros. Essa colaboração se manifesta em diversas frentes.

A Plataforma Gov.br[6] é o principal portal do governo brasileiro para acesso a serviços públicos digitais. A integração com as instituições financeiras é um pilar fundamental para o atendimento ao cidadão, oferecendo os níveis de conta com diferentes direitos, protegendo a conta do cidadão. Os cidadãos podem criar ou aumentar o nível de sua conta Gov.br (para Prata ou Ouro) utilizando o login de seus bancos credenciados. Isso facilita o acesso a serviços que exigem maior segurança e validação de identidade, sem a necessidade de validação facial em alguns casos. Bancos como Banco do Brasil, Caixa Econômica Federal, Itaú, Bradesco, Santander, BRB e Sicoob já estão integrados.

Através deste portal, é possível consultar e transferir "valores esquecidos" em bancos, como o Sistema Valores a Receber (SVR) do Banco Central conforme a Resolução BCB 98, de 1º de junho de 2021, que trata sobre a remessa ao Banco Central do Brasil de informações relativas a valores a devolver a pessoas naturais e jurídicas. Esse sistema pode ser utilizado na hipótese de uma pessoa falecida que ainda não foi feito o inventário e tenha herdeiros que querem saber os valores que se encontram na conta. Para isso, o sistema pede o número do CPF e a data de nascimento do falecido, sendo necessário ter uma conta ouro. Para ter acesso a essa informação, o solicitante deve ser herdeiro(a), testamentário(a), inventariante ou representante legal e, portanto, legitimamente autorizado(a) a acessar os dados da pessoa falecida. Em caso de paternidade ou união estável pós-morte, pode ser utilizado o sistema para verificar valores a receber do falecido. A opção de verificar Valores a Receber, referente a contas encerradas e em que ainda há algum valor existente, ou Contas de Empresas encerradas, sendo necessário entrar com o número de Cadastro Nacional de Pessoa Jurídica – CNPJ e a data de abertura da empresa.

O sistema Desenrola Brasil[7] é um programa de renegociação de dívidas criado pela Lei 14.690 de 2023 (LGL\2023\10457); o objetivo é propiciar que pessoas que estão negativadas voltem a ter condições de adquirir novas operações de crédito, sendo uma maneira do cidadão conseguir pagar suas dívidas. O programa destina-se a negociar as dívidas compreendidas no primeiro de janeiro de dois mil e vinte e um a trinta e um do mês de dezembro de dois mil e vinte e dois. O programa é dividido em duas faixas. A faixa I é destinada a pessoas físicas com renda bruta mensal de até dois salários-mínimos ou que estejam inscritos no Cadastro Único (CadÚnico), sendo um Programa Social do Governo Federal visando atender a população de baixa renda com benefícios sociais. A faixa II é destinada a pessoas físicas, com dívidas financeiras negativadas até trinta e um de dezembro de dois mil e vinte e dois, com renda de até vinte mil reais**.**

O programa “CRED+” e regulamentado pela Lei 13.999 de 18 de maio de 2020 (LGL\2020\6242), institui que oferece crédito, para microempreendedores individuais (MEIs) e pequenas empresas, que pode ser acessado no portal Gov.br na seção Portal Empresas & Negócios, oferecendo acesso a serviços e produtos financeiros, conectando empreendedores a instituições financeiras habilitadas para análise de crédito. O empresário, através do seu computador ou *smartphone,* pode realizar solicitações com diversas instituições financeiras simultaneamente, verificando qual a melhor proposta que atenda às suas necessidades financeiras, para o seu negócio. Através do Portal do Empreendedor o Microempresário Individual – MEI ou Micro e Pequena Empresa e o Artesão, permitindo escolher um serviço financeiro para o seu negócio, sendo encaminho o pedido para a instituição financeira, caso seja aceita o empreendedor recebera orientações para assinatura do contrato, sendo um serviço gratuito oferecido pelo Governo Federal.

O Pix, é instituído pela Resolução BCB 1 de 12 de agosto de 2020, que institui o arranjo de pagamentos que aprova seu regulamento sendo o sistema de pagamentos instantâneos transformou a forma como os brasileiros realizam transações financeiras, promovendo agilidade, baixos custos e ampla inclusão, basta ter uma conta bancária para ter acesso a este recurso, muito utilizado no mercado nacional.

O Sistema Financeiro Aberto – *Open Finance*[8], instituído pela Resolução BCB 32, de 29.10.2020, estabelece requisitos técnicos e os procedimentos operacionais para a implementação no País permitindo o compartilhamento de dados financeiros dos clientes entre diferentes instituições (com o consentimento do cliente), possibilitando a oferta de produtos e serviços mais personalizados e vantajosos, além de facilitar a gestão financeira do cidadão em um único ambiente, propiciando taxas mais acessíveis para o seu negócio. As informações de uma instituição financeira poderão ser compartilhas com as demais visando oferecer a melhor proposta para o cliente permitindo a movimentação de suas contas bancárias em diferentes plataformas e não apenas pelo aplicativo ou site do banco que possui a conta.

O cliente poderá compartilhar seus dados com outras instituições financeiras, através de plataformas, e receber novas propostas sobre os produtos financeiros em que tem interesse, analisando a menor taxa de juros e o tempo para quitar sua negociação, respeitando a Lei Geral de Proteção de Dados, podendo ser cancelado a qualquer momento. Referente aos produtos que podem ser negociados, são eles: contas bancárias, operações de crédito, investimentos, operações de câmbio. Há previsão de serem implantados seguros e previdência. O compartilhamento das informações do cliente propicia às instituições financeiras conhecerem o cliente e oferecer produtos de acordo com sua necessidade. Este serviço atende tanto pessoas físicas como pessoas jurídicas. Este recurso está disponível no aplicativo do banco; basta apenas o cliente realizar o seu pedido, após a validação dos dados do cliente. A transmissão dos dados poderá ser feita somente entre duas instituições por vez. O cliente pode fazer transações de Pix através do *Open Finance* para pagar uma loja virtual, preservando a sua conta principal. Este serviço permite a integração entre as instituições financeiras com lojas virtuais, permitindo que o cliente ao pagar uma conta, possa verificar o seu saldo e utilizar no próprio aplicativo do lojista sem a necessidade de alterar entre aplicações do lojista e do banco, trazendo mais comodidade ao cliente.

Alguns exemplos de uso dos dados compartilhados por meio do *Open Finance* são: oferta de produtos mais rentáveis e adequados ao perfil do cliente (crédito e investimento) com taxas melhores e tarifas mais baixas; maior agilidade nas contratações dos produtos e na abertura de contas; visão consolidada dos dados das contas, dos cartões ou dos investimentos; aconselhamento financeiro; simplificação da portabilidade de salário e de crédito; entre outros.

Para permitir o compartilhamento de dados, é necessário que o cliente acesse o ambiente (aplicativo ou internet banking) da instituição que ele deseja que receba seus dados (instituição recebedora dos dados), procure pela área do *Open Finance* ou pela funcionalidade “Trazer meus dados” e selecione a instituição de onde deseja trazer os dados (instituição transmissora dos dados). Cada consentimento é dado pelo cliente de forma direta e vale somente para duas instituições (recebedora e transmissora) por vez.

Os dados não são enviados para uma estrutura centralizada, como em alguns países. No Brasil apenas a instituição recebedora de dados acessa os dados. O consentimento pode ser cancelado a qualquer momento nos ambientes digitais de qualquer uma das duas instituições envolvidas no compartilhamento. É possível realizar pagamentos com Pix, possibilitando pagamento por meio de canais mais convenientes, preservando a segurança do processo, propiciando a utilização em lojas virtuais.

As instituições financeiras fazem muitos investimentos no atendimento digital, investindo em tecnologia para melhorar a experiência do cliente, impulsionados também pelas iniciativas do governo digital. A pandemia do COVID-19 incentivou uma aceleração nos serviços digitais das instituições financeiras, oferecendo maior número de serviços digitais que propiciam realizar as transações e serviços bancários via internet banking e aplicativos móveis, permitindo que os cidadãos realizem operações (transferências, pagamentos, investimentos, contratação de crédito).

A utilização da Inteligência Artificial (IA) e Automação: Bancos e *Fintechs* utilizam IA e automação em seus canais de atendimento (*chatbots*, assistentes virtuais) para oferecer suporte rápido e personalizado, além de otimizar processos internos.

A Segurança e Privacidade com a digitalização crescente exigem um compromisso ainda maior com a segurança da informação. As instituições financeiras e o governo trabalham para garantir a proteção dos dados dos cidadãos, em conformidade com a LGPD e a Lei do Sigilo Bancário (Lei Complementar 105/2001 (LGL\2001\236)), utilizando tecnologias como criptografia e autenticação multifatorial.

A convergência entre o governo digital e o setor financeiro é moldada por diversas leis e regulamentações, como a Lei Geral de Proteção de Dados (LGPD – Lei 13.709/2018 (LGL\2018\7222)), sendo fundamental para a proteção de dados pessoais. A LGPD estabelece princípios, direitos dos titulares e obrigações para controladores e operadores, impactando diretamente como as instituições financeiras e o governo tratam as informações dos cidadãos. Isso é crucial para serviços financeiros digitais e plataformas governamentais que lidam com dados sensíveis.

O Marco Civil da Internet (Lei 12.965/2014 (LGL\2014\3339)) estabelece princípios, garantias, direitos e deveres para o uso da internet no país, incluindo a neutralidade de rede, a privacidade e a liberdade de expressão. Embora não seja exclusiva do setor financeiro, serve como base para o desenvolvimento de serviços digitais seguros, pois a internet é uma rede mundial de computadores interligando pessoas e instituições financeiras em qualquer parte do mundo, utilizados nos aplicativos móveis.

A**s** Leis e Resoluções do Banco Central do Brasil (BCB) e do Conselho Monetário Nacional (CMN) são os principais reguladores do sistema financeiro nacional. Diversas resoluções e circulares foram emitidas para regulamentar as *Fintechs* e o *Open Finance*, visando promover a competitividade, a eficiência e a inclusão financeira.

As Sociedades de Crédito Direto (SCDs) e as Sociedades de Empréstimos entre Pessoas (SEPs), regulamentadas pelo BCB (como na Resolução 4.656/2018 (LGL\2018\3555)), permitem que *Fintechs* ofereçam crédito diretamente aos clientes ou realizem empréstimos entre pessoas, sem a intermediação de bancos tradicionais, democratizando o acesso ao crédito.

A Lei do Arranjo de Pagamentos (Lei 12.865/2013 (LGL\2013\9632)) é essencial para o surgimento de novos modelos financeiros, como as *Fintechs* de pagamento, essa lei estabelece as diretrizes para instituições de pagamento e arranjos de pagamento.

A Legislação de Combate à Lavagem de Dinheiro (Lei 9.613/1998 (LGL\1998\81) e Circulares do BCB): as *Fintechs* e as instituições financeiras estão sujeitas a rigorosas obrigações de identificação de clientes (KYC – *Know Your Customer*), monitoramento de transações e relatórios de atividades suspeitas para prevenir crimes financeiros.

A Estratégia de Governo Digital (Decreto 10.332/2020 (LGL\2020\5269) e Lei 14.129/2021 (LGL\2021\3997)) define diretrizes para a digitalização de serviços públicos federais, buscando simplificar processos, reduzir burocracia e melhorar a experiência do cidadão. Isso inclui a oferta de serviços públicos digitais, identidade digital e a promoção da interoperabilidade entre sistemas governamentais. A digitalização de processos governamentais para abertura de empresas, por exemplo, reduz custos e tempo, facilitando a entrada de novas *Fintechs* no mercado e, com o aumento das transações e serviços digitais, a segurança cibernética se torna uma prioridade. Novas políticas e regulamentações (como a Política Brasileira de Cibersegurança estabelecida em dezembro de 2023) são desenvolvidas para proteger os dados e o sistema financeiro contra ataques e fraudes. Com a digitalização, exige-se um foco maior na proteção dos consumidores, especialmente em relação à privacidade dos dados, à transparência nas ofertas de serviços e ao combate a fraudes online.

O ambiente regulatório no Brasil tem se adaptado para fomentar a inovação no setor financeiro, com o Banco Central atuando como um catalisador para tecnologias como o *Open Finance*, que promovem a competição e a criação de novos produtos e serviços. A interação entre o governo digital e as instituições financeiras no Brasil é dinâmica, com a legislação buscando criar um ambiente que favoreça a inovação, a segurança e a inclusão, ao mesmo tempo em que aborda os desafios inerentes à transformação digital.

Diante do exposto, pode-se verificar que os sistemas bancários trazem uma grande quantidade de serviços que se encontram nos dispositivos móveis, e por isso se faz necessária uma gestão de riscos para uma segurança lógica (*security*) e física (*safety*) dos dispositivos móveis.

3 Gestão de riscos e pilares da segurança digital

A experiência do roubo ou furto é muito desagradável e frustrante, pois a vítima tem um sentimento de vulnerabilidade, agradecendo por sair dessa experiência negativa guardando sua vida, sendo seu bem maior, e a saúde, segundo a definição da OMS em Malta (2013) "situação de perfeito bem-estar físico, mental e social", e não apenas como a ausência de doença ou enfermidade. Na Sociedade 4.0, o roubo, furto ou perda de um *smartphone*, além do custo do aparelho, nos causa vários problemas para se viver na vida cotidiana. Agenda de compromisso, organização da vida diária, pagamento de contas, sair de um determinado lugar com o auxílio de um GPS. Além de termos um terminal bancário com cartões de crédito e muitos serviços de instituições bancárias que podem atrapalhar a nossa vida financeira e nossa saúde mental.

Se faz necessário, pensar em gestão de riscos, pois coisas ruins podem acontecer, e saber quais as atitudes deverão ser tomadas ajuda a resolver os problemas. Conforme Pereira (2025) e Beck (2011), o risco é a probabilidade de um evento indesejável ocorrer devido às suas circunstâncias, no caso de dispositivos móveis há um risco iminente, pois conforme mostram os dados de assaltos apresentados na introdução, há uma probabilidade de ficar sem seu dispositivo móvel e, com isso muitas coisas ruins podem acontecer, além do custo do aparelho, transações bancárias tais como pagamentos, transferências, empréstimos, compras, entre outros. Os dados são considerados o petróleo da sociedade moderna, sendo considerados como recursos valiosos (RAIS, 2020): contatos, contas em redes sociais, fotos, vídeos, sons e outros ativos digitais. Por alguns momentos, a pessoa se sente vulnerável e com medo do que pode acontecer sem estar mais na posse do seu dispositivo móvel.

Como pilares da segurança da informação, conforme ensina Barreto (2018) e Comer (2016), os principais são os quatro: confidencialidade, disponibilidade, autenticidade e não repúdio. A confidencialidade consiste em garantir que somente pessoas autorizadas (físicas ou jurídicas) tenham acesso à informação. No caso de transações bancárias entre cliente e a instituição financeira, os sistemas de criptografia devem garantir, através de protocolos de segurança da informação, que os dados fornecidos entre as duas entidades se comuniquem. Caso haja uma interceptação dos dados através dos meios de comunicação que estão sendo utilizados, como por exemplo cabos de cobre ou sem fio (1G, 2G, 3G, 4G, 5G, 802.11 da IEEE etc.), será muito difícil saber quais são os dados que estão trafegando.

A integridade consiste em garantir que os dados que são enviados do ponto de origem, chegarão íntegros ao seu destino. Em aplicações bancárias, a integridade consiste em garantir que os dados enviados, como uma transferência bancária ou o pagamento de um pix, não sejam alterados da sua origem, que é o aplicativo do usuário, até o seu destino, o servidor da agência bancária.

A disponibilidade consiste em que o sistema esteja disponível quando o cliente deseja utilizar. O acesso da agência e conta bancária em um sistema de informação em qualquer lugar e em qualquer hora deve estar disponível para a transação bancária.

A autenticidade é garantir que o cliente que está acessando o sistema seja o proprietário da conta, validando suas credenciais, como usuário e senha no aplicativo, e pode-se adotar a validação de dois ou mais fatores, que pode ser realizada através de uma verificação biométrica, ou um desafio através de um código enviado ao cliente via SMS – *Short Message Service*, ou validar um reconhecimento de imagem do usuário pedindo para que seja capturado uma foto do seu rosto validando a pessoa que está acessando o sistema.

O não repúdio consiste impedir que a pessoas que está fazendo a transação bancária negue sua ação, em um cenário normal, em que a pessoa não esteja sob uma forte coação irresistível. Com as ferramentas existentes hoje referentes a senha, validação de biometria e algo que o cliente saiba, tal como um apelido de infância ou o nome de um amigo mais próximo, fica muito difícil negar sua autoria em situações da vida cotidiana.

Além da segurança lógica, é necessário considerar a segurança física, quando o dispositivo móvel apresenta alguma falha, como uma quebra de tela, ou mesmo seja subtraído do seu proprietário. Neste caso, faz-se necessário pensar quais as ações que devem ser adotadas, visando a proteção dos dados e reduzir as perdas referentes ao acesso indevido de contas bancárias e empréstimos que podem ser realizados enquanto o dispositivo não se encontra mais no poder de seu proprietário.

Uma configuração e fazer o fechamento para pedir autenticação do celular a cada 10 ou 15 segundos, e ativar a validação por biometria da digital. Mas, caso esteja utilizando um software de navegação, essa tela não será ativada e, neste caso poderá ter acesso a outras aplicações do dispositivo.

A vítima do furto ou roubo de seu aparelho celular, dependendo da marca do seu dispositivo, deve-se cadastrar no site do fabricante, pois os dispositivos possuem um número identificador único, intitulado IMEI – *International Mobile Equipment Identity*, que se encontra na caixa do dispositivo, ou no site do fabricante, quando o usuário cadastra seus dados, fica gravado o IMEI no site do fabricante. Um exemplo é no caso dos sistemas operacionais Android, em que tem o Google, através de uma conta do *gmail*, permite localizar o dispositivo através do GPS e de forma remota propicia bloquear o dispositivo de forma remota e apagar seus dados de forma remota, impedindo que seus dados tenham acesso indevido. Para o proprietário restaurar os dados na compra de um novo aparelho, basta restaurar a cópia de segurança (*backup*), que deve ser realizada diariamente, reduzindo os impactos negativos que este evento pode ocasionar.

Uma das medidas é ter um segundo telefone inteligente, que, nesse caso, utiliza a redundância e, caso o dispositivo seja roubado ou furtado, pegar o segundo dispositivo, ir até a prestadora de serviço do celular e comprar um novo chip e fazer a transferência do número para o novo chip e, desta forma, restaurar as contas do aplicativo de mensagem instantânea WhatsApp ou outros aplicativos de mensagem instantânea.

4 Responsabilidade civil

A Responsabilidade Civil é dividida em objetiva e subjetiva. Na responsabilidade subjetiva, a vítima deverá comprovar o ato, dano, nexo causal, culpa ou dolo da Instituição Financeira, sendo uma tarefa difícil, pois o cliente deverá produzir provas do ocorrido, supondo uma falha de segurança de dados sensíveis protegidos pela LGPD, o cliente deveria produzir provas do ocorrido, sendo que muitas vezes está numa condição de hipossuficiência, sem conhecimentos técnicos de saber como

ocorreu a falha, mas somente sofrendo com o dano ocorrido.

Já a responsabilidade objetiva, não há necessidade de fazer a prova sobre o dano, mas sim ter mera relação causal entre o comportamento e o dano que o cliente sofreu.

A Súmula 479 do STJ, as Segunda Seção, julgada em 27.06.2012, *DJe* 01.08.2012, versa 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”.

O Superior Tribunal de Justiça (STJ) pacificou o entendimento de que as instituições financeiras têm responsabilidade objetiva por danos causados por fraudes e delitos de terceiros, desde que ocorram dentro das operações bancárias.

As instituições financeiras são responsáveis pelos prejuízos que o cliente sofra, mesmo que a fraude tenha sido cometida por outra pessoa, se a falha aconteceu dentro dos seus próprios sistemas ou operações, isso se aplica aos aplicativos móveis. O chamado fortuito interno refere-se a eventos imprevisíveis, mas que estão diretamente ligados à atividade da empresa. Fraudes e golpes, como clonagem de cartão, por exemplo, são considerados riscos inerentes à operação bancária.

As instituições financeiras são responsabilizadas pelos danos, independentemente de terem agido com culpa (negligência, imprudência ou imperícia). Basta que o dano tenha ocorrido. Os danos por terceiros significam que os prejuízos podem ser causados por outras pessoas que não são o banco nem o cliente, como golpistas ou hackers. A responsabilidade do banco é limitada a eventos que ocorrem durante operações como transferências, saques, pagamentos e uso de cartões.

Essa súmula é frequentemente utilizada em ações judiciais para responsabilizar bancos por situações como fraudes no PIX, clonagem de cartões de crédito e movimentações não autorizadas na conta de clientes.

5 Conclusão

As mudanças na sociedade, através do advento dos novos recursos da tecnologia da informação, estão mudando a forma de as instituições financeiras se relacionarem com o cliente, sendo que antes era mais usual ir até as agências bancárias, mas, nos dias atuais, através da evolução da velocidade das redes de computadores com as redes de 5G, que permitem uma maior velocidade nas transferências de dados de forma móvel, sem a necessidade de estar em um escritório. A modernização dos *smartphones,* propiciou que os terminais bancários pudessem ser acessados através dos dispositivos móveis, mudando o comportamento dos clientes ao se relacionar com as instituições financeiras, e também que novos tipos de fraudes surgiram, sendo necessária a criação da Súmula 479 para indicar qual a responsabilidade das Instituições Financeiras perante as fraudes a que os clientes estão sujeitos na utilização de seus sistemas de informação, permitindo uma maior segurança de uso aos seus clientes.

A tecnofilia, consiste em usuários que gostam da tecnologia da informação e têm maior facilidade e, desta forma, serão mais aderentes à utilização dos aplicativos das instituições financeiras, porém há uma parcela da população, conforme apresentado na pesquisa INAF, que são analfabetos digitais, e se faz necessário, oferecer outros meios para que tenham acesso aos serviços bancários, que irão precisar com o passar do tempo, como é o caso do acesso aos benefícios da previdência, que são depositados através de contas bancárias, sendo necessário ter alguma familiaridade com os dispositivos móveis e a utilização de recursos digitais para o pagamento de contas, tais como transferências bancárias, PIX, cartões de créditos, pois cada vez mais as cédulas monetárias estão sendo menos utilizadas. Por esse motivo, faz-se necessário o atendimento humano nas agências bancárias, para oferecer um atendimento humanizado às pessoas que não têm tanta afinidade com tecnologia. Também se faz necessário investir na educação em tecnologia da informação, visando à redução do analfabetismo digital, para melhor convivência na sociedade moderna.

6 Referências bibliográficas

AGUIAR, Carlos Eduardo Souza; SILVA, Dayana K. Melo. Tecnologia e decolonialidade: arranjos insurgentes e a questão das cosmotécnicas. Revista Tecnologia e Sociedade, v. 20, n. 62, p. 111-124, 2025.

BARRETO, Jeanine S.; ZANIN, Aline; MORAIS, Izabelly S.; et al. Fundamentos de segurança da informação. Porto Alegre: SAGAH, 2018. E-book. ISBN 9788595025875. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788595025875/]. Acesso em: 01.08.2025. p. 13.

BECK, Ulrich. Sociedade de risco: rumo a uma outra modernidade. São Paulo: Editora 34, 2011.

COMER, Douglas E. Redes de computadores e internet. 6. ed. Porto Alegre: Bookman, 2016. E-book. ISBN 9788582603734. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788582603734/]. Acesso em: 01.08.2025.

MENEZES, Wladimir Jatobá de; CASTILHO, Goiara Mendonça de; SOUZA, Wânia Cristina de. Tecnologia, multitarefas e tecnoestresse: entre a hiperconectividade e os limites da atenção, memória de trabalho e saúde mental digital. Caderno Pedagógico, v. 22, n. 8, p. e17627-e17627, 2025.

BRASIL. Desenrola Brasil: programa de renegociação de dívidas do Governo Federal. Disponível em: [https://www.gov.br/pt-br/servicos/negociar-dividas-da-faixa-i-com-o-programa-desenrola-brasil]. Acesso em: 31.07.2025.

FOLLARI, Roberto. Por fuera de la tecnofilia y la tecnofobia. Revista Ciencias Sociales, v. 1, n. 44, p. 17-29, 2022.

BRASIL. Governo Digital. Disponível em: [https://www.gov.br/governodigital/pt-br]. Acesso em: 31.07.2025.

INAF. Indicador de Analfabetismo Funcional. Disponível em: [https://alfabetismofuncional.org.br/]. Acesso em: 30.07.2025.

MALTA, Deborah Carvalho; SILVA JR., Jarbas Barbosa da. O Plano de Ações Estratégicas para o Enfrentamento das Doenças Crônicas Não Transmissíveis no Brasil e a definição das metas globais para o enfrentamento dessas doenças até 2025: uma revisão. Epidemiologia e Serviços de Saúde, v. 22, n. 1, p. 151-164, 2013.

PEREIRA, Newton Narciso; et al. Gestão de risco em um terminal portuário brasileiro usando técnicas de avaliação de risco aprimoradas pela gestão do conhecimento distribuído. Revista Brasileira de Transportes, v. 5, n. 1, p. 22-69, 2025.

RAIS, Diogo; PRADO FILHO, Francisco Octavio de Almeida. Direito público digital. São Paulo: Thomson Reuters Brasil, 2020.

REBOUÇAS, Rodrigo F. Contratos eletrônicos. São Paulo: Almedina, 2016. E-book. ISBN 9788584931057. Disponível em: [https://integrada.minhabiblioteca.com.br/reader/books/9788584931057/]. Acesso em: 31.07.2025. p. 1.

SÃO PAULO (Estado). Secretaria de Segurança Pública (SSP). Celulares subtraídos 2024 (base de dados). Disponível em: [https://www.ssp.sp.gov.br/assets/estatistica/transparencia/baseDados/celularesSub/CelularesSubtraidos_2024.xlsx]. Acesso em: 28.07.2025.

STATCOUNTER. Platform market share (Brazil): desktop, mobile, tablet. Disponível em: [https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/brazil]. Acesso em: 28.07.2025.

1 StatCounter, disponível em: [https://gs.statcounter.com/platform-market-share/desktop-mobile-tablet/brazil]. Acesso em: 28.07.2025.

2 Governo Digital, disponível em: [https://www.gov.br/governodigital/pt-br]. Acesso em: 31.07.2025.

3 INAF – Indicador de Analfabetismo Funcional, disponível em: [https://alfabetismofuncional.org.br/]. Acesso em: 30.07.2025.

4 E-Gov, disponível em: [https://sso.acesso.gov.br/login?client_id=portal-logado.estaleiro.serpro.gov.br&authorization_id=1985b455a25]. Acesso em: 30.07.2025.

5 SSP – Secretaria de Segurança Pública, disponível em: [https://www.ssp.sp.gov.br/assets/estatistica/transparencia/baseDados/celularesSub/CelularesSubtraidos_2024.xlsx]. Acesso em: 28.07.2025.

6 Gov.br, Portal do Governo Digital, disponível em: [https://www.gov.br/pt-br]. Acesso em: 30.07.2025.

7 Desenrola Brasil, Programa de renegociação de dívidas do Governo Federal, disponível em: [https://www.gov.br/pt-br/servicos/negociar-dividas-da-faixa-i-com-o-programa-desenrola-brasil]. Acesso em: 31.07.2025.

8 Disponível em: [https://www.bcb.gov.br/estabilidadefinanceira/openfinance].