

A APLICAÇÃO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NAS AGÊNCIAS BANCÁRIAS: DESAFIOS E ESTRATÉGIAS PARA A CONCRETIZAÇÃO DA PROTEÇÃO DOS CLIENTES

Laura de Oliveira Souza

Graduanda em Direito, Faculdade Metropolitana São Carlos - FAMESC, Bom Jesus do Itabapoana-RJ; e-mail: lauraolisouzaa@gmail.com

Valdeci Ataíde Cápua

Mestre em direito pela FDCI - Faculdade de Direito de Campos dos Goytacazes e Analista Judiciário do TJ-ES; e-mail: valdeci_adv@hotmail.com

RESUMO

Devido ao crescimento acelerado da inteligência artificial e avanço da tecnologia é possível observar a necessidade de adequação da sociedade para que seja possível extrair o melhor de ambas no que tange ao desenvolvimento da sociedade. Porém, com esses avanços, surgem novos desafios no dia a dia de cada um e no âmbito jurídico, uma vez que essas ferramentas quando utilizadas de forma inadequadas, se tornam “uma terra sem lei”. Com isso, percebe-se que devido a utilização maldosa, muitas pessoas acabam caindo em golpes, sendo enganadas, com sentimento de ter sua privacidade violada. Dentre estes golpes, muito se vê nos noticiários e até mesmo no âmbito familiar, no trabalho etc., os golpes bancários, onde as vítimas são enganadas sejam por mensagens, ligações e até mesmo áudios ou imagens dissimuladas, induzidas a realizarem transações fraudulentas. Dessa forma, fazendo-se necessária a criação de mecanismos e leis para que seja possível se ter um alcance de proteção para os usuários deste mundo tecnológico, surge a LGPD. Os dados pessoais são valores que precisam ser resguardados. Neste sentido, com a proteção da Constituição Federal de 1988 e o estabelecimento de linhas gerais com a Lei Geral de Proteção de Dados, o ponto central, que é o seu resguardo, é delimitado. Com isso, o objetivo do trabalho em questão é apresentar a Lei Geral de Proteção de Dados, bem como os desafios enfrentados por instituições bancárias em relação aos golpes que, rotineiramente, são empregados em operações financeiras. A metodologia empregada foi por meio de revisão bibliográfica, com a seleção de artigos e estudos que dissertam de maneira aprofundada sobre o tema. Por fim, o estudo busca identificar como a LGPD se comporta nos casos de golpes e fraudes bancárias, visto que a lei em questão é aplicada de forma geral.

Palavras-chave: LGPD; Instituições Bancárias; Proteção de dados.

ABSTRACT

Due to the accelerated growth of artificial intelligence and the advancement of technology, it is possible to observe the need for society to adapt so that it is possible to extract the best from both in terms of the development of society. However, with these advances, new challenges arise in each person's daily life and in the legal sphere, since these tools, if used inappropriately, become "a land without law". Therefore, it is clear that due to malicious use, many people end up falling for scams, being deceived, with the feeling of having their privacy violated. Among these scams, we see a lot in the news and even in the family sphere, at work, etc., banking scams, where victims are deceived either through messages, calls and even disguised audios or images, induced to carry out fraudulent transactions. Thus, making it necessary to create mechanisms and laws so that it is possible to have a range of protection for users of this technological world, the LGPD emerges. Personal data are values that need to be protected. In this sense, with the protection of the Federal Constitution of 1988 and the establishment of general guidelines with the General Data Protection Law, the central point, which is its protection, is delimited. In this sense, with the protection of the Federal Constitution of 1988 and the establishment of general guidelines with the General Data Protection Law, the central point, which is its protection, is delimited. Therefore, the objective of the work in question is to present the General Data Protection Law, as well as the challenges that are faced by banking institutions in relation to scams that are routinely used in financial operations. The methodology used was through bibliographical review, with the selection of articles and studies that speak in depth on the topic. Finally, the study seeks to identify how the LGPD behaves in cases of bank scams and fraud, given that the law in question is applied generally.

Keywords: LGPD; Banking Institutions; Data protection.

1. INTRODUÇÃO

Por conta de um mundo globalizado, hoje, a informação pode ser considerada um dos ativos que mais são valorizados. E, por conta disso, a concentração dessas informações sempre são requeridas por grandes empresas, com a finalidade de transformar esses dados em estratégias comerciais para cativar os clientes certos e, assim, transformar este poder em concentração de riquezas. Com isso, se antes o indivíduo já tinha uma certa valoração para o mercado, hoje essa valoração multiplicou, pois, através de seus respectivos dados, são coletadas informações cruciais para as grandes empresas (RIBEIRO, 2023, p. 11).

Mesmo tendo suas vantagens, os dados pessoais podem ser violados e, por consequência, usados de maneira indevida e sem o consentimento do titular, podendo causar sérios danos à moral e, ainda, na maioria das vezes, danos econômicos. Por isso, as relações de consumo precisam ser protegidas e monitoradas de maneira correta, visando o resguardo dos dados pessoais de cada indivíduo, como uma barreira para que atividades ilícitas não sejam feitas com dados pessoais sem o consentimento do titular (VASCONCELOS, 2023, p. 11).

Neste sentido, além da normatização da proteção de dados como um direito fundamental na Constituição Federal de 1988, a Lei Geral de Proteção de Dados, criada em 2018, passou a complementar o que já estava estabelecido em texto constitucional, trazendo conceitos e maneiras de resguardo dos dados pessoais no âmbito digital. A LGPD estabelece diretrizes, princípios e as possíveis formas de responsabilização dos agentes do ato ilícito, bem como a responsabilização objetiva e subjetiva.

Diante disso, o presente estudo visa abordar a aplicação da LGPD no que tange a golpes bancários, objetivando estabelecer a aplicação da lei supracitada nos casos em questão. Por isso, o estudo, primeiramente, visa apresentar, por meio de uma linha do tempo, como os dados pessoais eram tratados antes e depois do surgimento da LGPD, e como a ascensão desta mudou o cenário brasileiro. Ademais, objetiva estabelecer sobre a proteção de dados no cotidiano do povo brasileiro, apresentando, de maneira mais aprofundada, sobre o vazamento de dados e também os golpes bancários, bem como o papel da LGPD nos casos em questão.

LINHA DO TEMPO: O SURGIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NO BRASIL

A proteção de dados pessoais é um direito de qualquer cidadão brasileiro, sendo este garantido pela Constituição Federal de 1988. No entanto, antes mesmo da previsão na CF/88, a proteção dos dados era estabelecida, em um contexto mundial, pela Declaração Universal de Direitos Humanos, no ano de 1948 (QUINTILIANO, 2021). De uma forma genérica e implícita, o artigo 12 da referida Declaração dispunha que:

Art. 12. Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei (UNICEF, s.d.).

A mesma proteção à privacidade também encontra-se disposta no artigo 11 do Pacto San José da Costa Rica, que diz: Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. Enquanto isso, no contexto europeu, tal privacidade se dá, ainda que de forma genérica, na Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais, de 1950, em seu artigo 8º: Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.

Em 1981, com o desenvolvimento da sociedade e compartilhamento de informações através de dados automatizados surge a 1º Convenção Internacional sobre a Proteção Pessoal no que tange ao Tratamento Automatizado de Dados de Caráter Pessoal, admitida em Janeiro de 1981. Entre os assuntos abordados encontra-se o reconhecimento da necessidade de “conciliar os valores fundamentais do respeito à vida privada e da livre circulação de informação entre os povos”.

Enquanto isso, na União Europeia, o direito da proteção de dados foi solidificado através da Diretiva 95/96/CE, estabelecida em 1995, que possui finalidade de justificar a adoção da proteção de dados através dos fundamentos e necessidades da mesma. Se entendia que a proteção de dados traria segurança e confiança no desenvolvimento desta tecnologia e logo, no progresso social.

Com efeito, os sistemas informatizados têm garantido notório progresso e aumento do bem estar na vida dos cidadãos. Se hoje o cidadão consegue efetuar uma transferência de recursos financeiros para uma empresa ou a outro cidadão, em alguns segundos, por meio de um aparelho celular, isso se deve à capacidade de tratamento de dados (QUINTILIANO, 2021).

Assim, as informações pessoais, digitais, em caso de Instituições Financeiras, são armazenadas e utilizadas para que o cliente consiga efetuar suas transações. Porém, não existe confiabilidade de que seus dados e informações pessoais estejam sendo guardados com a devida segurança que a proteção de dados estabelece. Abrindo margem para que a vida privada desses clientes, possam vir a sofrer fraudes, ataques ou publicidade indesejada. E por esse motivo, a União Europeia decide então, criar a diretiva, formada por 72 “considerandos” que consideram todos os princípios que devem ter função de guiar como devem ser tratados os dados em uma sociedade (QUINTILIANO, 2021).

No âmbito da União Europeia, os direitos fundamentais foram reconhecidos apenas em 2000, através da Carta de Direitos Fundamentais. Esse documento, veio a ser considerado como direito primário da UE em 2009, através do Tratado de Lisboa. Seu art. 8º, estabelece como um princípio fundamental a proteção de dados:

Proteção de dados pessoais

1. Todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito.
2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação.
3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

O início da regulamentação no Brasil se deu através da CF/88 que, inicialmente, no artigo 5º, inciso LXXIX, tinha a seguinte redação: “é assegurado, nos termos da lei, o direito à proteção dos dados pessoais” (BRASIL, 1988). Ademais, a proteção vai além do dispositivo citado, tendo a previsão constitucional a “proteção ao direito de personalidade, à liberdade de expressão (art. 5º, IX) e pelo direito à informação. Ainda, é garantida a inviolabilidade da vida privada e intimidade (art. 5º, X), o habeas data (art. 5ºLXXII) e a interceptação das comunicações [...]” (LUGATI; ALMEIDA, 2020, p. 10). O Código o Consumidor, em 1990, também dispôs sobre o direito de proteção de dados, estabelecendo que “o consumidor, [...] terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes” (BRASIL, 1990).

Foi apenas em 2011 que surgiu a Lei de Acesso à Informação, a Lei nº 12.527/11, que visa disciplinar sobre o direito de acesso à informação que é previsto na CF/88, que “todos têm direito a receber dos órgãos públicos tanto informações sobre seu interesse particular, quanto de interesse coletivo ou geral” (BRASIL, 1988). O objetivo da Lei é garantir

o direito fundamental à informação e estabelecer as diretrizes a serem seguidas nos que exigiam esse tipo de recebimento de informações, além de incentivar na divulgação de locais de fácil acesso para que essas informações sejam acessadas por qualquer um. A lei em questão possui a publicidade como o princípio basilar (SOARES; JARDIM; HERMONT, 2013).

Com a globalização e o avanço da internet, em 2012 foi sancionada a Lei nº 12.373/12, mais conhecida como Lei Carolina Dieckmann. Em um breve resumo, a aprovação da referida lei se deu por conta de uma invasão em seu computador, que teve o total de 36 fotos íntimas roubadas, sofrendo uma tentativa de extorsão e, por fim, tendo as fotos divulgadas na internet. Na época, assuntos como esse eram poucos abordados e ainda não possuíam uma tipificação específica, o que acabou sendo uma questão de urgência, tendo a finalidade de legislar sobre a segurança de dados e informações no ambiente virtual (ARAÚJO, 2023).

A partir disso, houve a criminalização da “invasão de celulares, computadores ou sistemas informáticos para obter, adulterar ou destruir dados a fim de obter vantagem ilícita, que também pode ser o objetivo da invasão dos dispositivos informáticos para instalar vulnerabilidades” (ARAÚJO, 2023). A Lei Carolina Dieckmann foi a primeira a tratar sobre os crimes cibernéticos, abrindo portas para outras propostas de criminalização de dados e informações que são disseminadas no ambiente virtual (ARAÚJO, 2023).

Em seguida, tem-se o Marco Civil da Internet, que “busca regular o uso da internet, conferindo direitos e garantias do cidadão nas relações travadas no meio virtual, de uma forma principiológica” (QUINTILIANO, 2021). A partir do marco em questão, foi estabelecido que os registros de conexão de usuários da internet seriam reservados pelo prazo de um ano, com sigilo, para que, caso houvesse algum caso a ser apurado, o registro ainda estaria presente. Vale ressaltar que o acesso aos registros depende de decisão judicial e, ainda, poderão ficar registrados pelo prazo maior que um ano através de solicitação do Ministério Público ou de autoridade policial (AGÊNCIA SENADO, 2024).

Desse modo, pode-se considerar que o sistema brasileiro teve um cuidado com a proteção de dados. No entanto, com o avanço da inteligência artificial, os institutos criados acabaram se tornando escassos com a quantidade de novidades que, hoje, podem ser extraídas da internet. O uso da inteligência artificial pode ser excelente se usado de maneira correta. No entanto, pode fazer grandes estragos, necessitando de uma normatização mais abrangente e específica que dê conta de regular todos os institutos necessários para a tipificação do uso da inteligência artificial de forma duvidosa (AGÊNCIA SENADO, 2024).

A ASCENSÃO DA LGPD

Hoje, pode-se dizer que a tecnologia não está mais ligada a um fator secundário em relação a vida de qualquer pessoa, mas sim um elemento que está ligado ao ser humano a partir do momento que este acorda, até quando ele vai dormir. Os dados e as informações retiradas da internet fazem parte da vida e do cotidiano de cada pessoa, sendo através de *posts* nas redes sociais, além de fotos ou até mesmo algum anúncio de vendas (BOTELHO, 2020, p. 7).

Com isso, os dados são considerados como “fatos que são coletados e armazenados, podendo se apresentar em formato eletrônico, analógico ou digital” (AMARAL, 2013, p. 3 *apud* BOTELHO, 2020, p. 7). A partir dessa perspectiva, os dados podem ser transformados em informação, que é quando os dados são acertadamente processados e analisados e, com isso, passam a ter um significado por conta de um certo contexto. Neste sentido, os dados se tornarão informações a partir do momento em que estes estiverem inseridos em algo que possua utilidade, fazendo com que a tomada de decisões seja feita a partir dos elementos encontrados nessa informação (HINTZBERGEN *et al.*, 2018, p. 53 *apud* BOTELHO, 2020, p. 8).

A segurança e a proteção do indivíduo no âmbito digital, no que afeta aos inúmeros usos dos dados pessoais e, de modo especial, no contexto da internet, ainda carece de maior atenção no Brasil, muito embora já se tenha desde 2014 um marco civil que, dentre outros pilares, expressamente previu como princípio estruturante a privacidade, delegando, no entanto, a proteção de dados pessoais a uma legislação específica que se concretizou por meio da promulgação da Lei Geral de Proteção de Dados, Lei 13.709/2018 (doravante LGPD) (SARLET; RUARO, 2021, p. 83).

O advento da Lei nº 13.709 de 2018, mais conhecida como Lei Geral de Proteção de Dados – LGPD –, fez com que o Brasil fosse colocado no rol dos mais de cem países que, de maneira adequada, protegem a privacidade e o uso de dados. A LGPD “cria uma regulamentação para o uso, para a proteção e, notadamente, para a transparência de dados pessoais no Brasil, nos âmbitos privado e público, e estabelece de modo claro quem são as figuras envolvidas e quais duas atribuições” (SARLET; RUARO, 2021, p. 86). Ademais, visa assegurar a integralidade da proteção à pessoa humana na mesma medida que estabelece a obrigação de uma gestão segura dos dados pessoais (SARLET; RUARO, 2021, p. 86).

Reconhecido como um direito fundamental pelo Supremo Tribunal Federal no ano de 2020 e incluído como uma garantia fundamental na CF/88 no ano de 2022, a proteção de

dados nos meios digitais é essencial para o resguardo dos direitos dos indivíduos. A inclusão dessa proteção como garantia constitucional fez a redação do inciso LXXIX, do art. 5º, mudar por conta da Emenda Constitucional nº 115, estabelecendo que “é assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais” (BRASIL, 1988). Esse reconhecimento constitucional ocorreu por conta da era da tecnologia, em que mudanças são feitas todos os dias, superando normas culturais e legais (BRASIL, 2024).

Diante disso, o papel da LGPD é a proteção aos direitos fundamentais da liberdade e da privacidade, diante do livre desenvolvimento da personalidade da pessoa natural. Isso porque,

[...] numa sociedade de informação, em que os dados pessoais passaram a ter valor financeiro na economia globalizada, percebeu-se a necessidade de proteger tais bens jurídicos e, ao mesmo tempo, regulamentar a utilização desses dados por diversos setores, a fim de permitir o fluxo de dados de forma legítima (BRASIL, 2024).

Em seu artigo 1º, a LGPD estabelece que a lei em questão “dispõe sobre o tratamento de dados, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, como o objetivo de proteger os direitos fundamentais [...]” (BRASIL, 1988). Além disso, os fundamentos da LGPD são essenciais para a sua aplicação, sendo: o respeito à privacidade; à autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 1988).

Não custa lembrar que a LGPD evidenciou a transparência como elemento central e, desta forma, torna cristalina a ideia de que todos os procedimentos envolvendo dados pessoais, sobretudo os dados sensíveis, devam ser compatíveis com a finalidade da coleta e minimizados em uma política de uso racional, sobretudo em razão da sua perenidade. Outro aspecto notável foi o fortalecimento da proteção e a decorrente vedação de uso de dados sensíveis para fins discriminatórios independentemente do consentimento do usuário, especialmente face aos riscos de destruição, de divulgação e de acesso indevido em razão da estrutura aberta da internet (SARLET; RUARO, 2021, p. 99).

Neste sentido, a LGPD surgiu para que fosse fornecido o fundamento legal adequado para o tratamento de dados pessoais, fazendo com que houvesse maior segurança jurídica

no que tange aos controladores e operadores, além de estabelecer regras claras de proteção e garantia do direito fundamental à proteção de dados. Com isso, “o tratamento de dados pessoais somente poderá ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular” (BOTELHO, 2020, p. 13).

A PROTEÇÃO DE DADOS NO COTIDIANO BRASILEIRO E POSSÍVEIS VAZAMENTOS DANDO ENSEJO À RESPONSABILIDADE CIVIL

Nos dias atuais, é possível perceber que, apesar de todo o avanço da tecnologia, o vazamento de dados e suas respectivas consequências são considerados assuntos que estão sempre em evidência, podendo ocasionar não somente prejuízos financeiros, mas também emocionais. Neste sentido, pode-se caracterizar o vazamento de informações “como incidente de segurança no qual dados pessoais, como nome completo, CPF, dentre outros, ou informações sensíveis [...] são expostos publicamente ou transferidos para terceiros sem o consentimento do titular” (GALVÃO *et al.*, 2024, p. 180). Essas exposições indevidas ocorrem por conta da popularização dos meios e das plataformas digitais que, por meio de normatização, precisam ser contidas e punidas (GALVÃO *et al.*, 2024, p. 180).

Pode-se dizer que os dados pessoais de cada indivíduo passaram de uma mera expressão da identidade do ser humano para um produto que é instruído na construção e no molde de opinião daqueles que consomem os produtos que estão em redes sociais, “como marketing e propagandas contidas nos canais de comunicação, de modo a invadir e rechaçar o direito fundamental à privacidade” (SIQUEIRA, 2023, p. 8). A partir disso, o fornecimento dessas informações a sites e aplicativos fazem com que estes tenham acesso a informações elementares sobre cada usuário, passando a ter hábitos de consumo, informações de identificação do usuário, preferência política, situação financeira e econômica, dentre outros (FERNANDES; PEREIRA; PEDROSA, 2024, p. 5).

No ano de 1995, Aguiar (1995) *apud* Siqueira (2023, p. 12) estabelecia a necessidade da proteção de dados pessoais que, de forma perfeita, pode se encaixar ainda em dias atuais:

A inserção de dados pessoais do cidadão em bancos de informações tem se constituído em uma das preocupações do Estado moderno, onde o uso da informática e a possibilidade de controle unificado das diversas atividades da pessoa, nas múltiplas situações de vida, permitem o conhecimento de sua conduta pública e privada, até nos mínimos detalhes, podendo chegar à devassa de atos pessoais, invadindo área que deveria ficar restrita à sua intimidade; ao mesmo tempo, o cidadão objeto desta indiscriminada colheita de informações, muitas vezes, sequer sabe da

existência de tal atividade, ou não dispõem de eficazes meios para conhecer o seu resultado, retificá-lo ou cancelá-lo. E assim como o conjunto dessas informações pode ser usado para fins lícitos, públicos e privados, na prevenção ou repressão de delitos, ou habilitando o particular a celebrar contratos com pleno conhecimento de causa, também pode servir, ao Estado ou ao particular, para alcançar fins contrários à moral ou ao Direito, como instrumento de perseguição política ou opressão econômica. A importância do tema cresce de ponto quando se observa o número imenso de atos da vida humana praticados através da mídia eletrônica ou registrados nos disquetes de computador (BRASIL, 1995 *apud* SIQUEIRA, 2023, p. 12).

Neste sentido, a questão central dos bancos de dados é tida como maior do que parece, pois, além de, muitas vezes, serem construídos de forma oculta e sem o consentimento do titular, são usados como mercadorias no mundo digital, “com a finalidade de moldar e influenciar o comportamento das pessoas, que têm seus dados tratados de forma ilícita, causando graves danos à privacidade e à autodeterminação informativa dos indivíduos” (SIQUEIRA, 2023, p. 13).

Por isso, a LGPD foi criada para que houvesse mais controle e transparência nas ações citadas, a fim de buscar a efetividade e aplicabilidade da proteção dos dados, protegendo-os e garantindo que os direitos fundamentais previstos na Constituição Federal sejam respeitados (GALVÃO *et al.*, 2024, p. 183). Entretanto, mesmo com a LGPD em vigor, é possível identificar grande falta de adesão ao que a lei estabelece, pois, para que sejam implementados, as organizações precisam arcar com modificações de alto custo. “A escassez de capital para investimentos em inovação tecnológica dificulta e retarda a adoção de novos programas que visam prevenir incidentes de segurança de dados” (GALVÃO *et al.*, 2024, p. 184).

A responsabilidade civil na LGPD pode ser de forma objetiva ou subjetiva. Naquela, a necessidade de comprovação de dolo ou culpa do agente é desnecessária, visto que o Código Civil estabelece que, nesses casos, “a obrigação de reparar o dano existe independente de culpa, nos casos previstos em lei ou quando a atividade normalmente desenvolvida pelo autor do dano, por sua natureza, implica risco para os direitos de terceiro” (BRASIL, 2002 *apud* ROCHA; HORITA, 2024, p. 32), tendo como elemento primordial o nexo causal entre a conduta e o agente dessa conduta. Já neste está relacionado a “ações ou omissões voluntárias, negligência ou imprudência que viole os direitos de outrem e causem dano, mesmo que seja exclusivamente moral” (FIGUEIREDO, 2020 *apud* ROCHA; HORITA, 2024, p. 31). Neste caso, o nexo de causalidade não precisa ser comprovado, basta evidenciar a voluntariedade do ato ou omissão (FIGUEIREDO, 2020 *apud* ROCHA; HORITA, 2024, p. 31).

A LGPD estabelece parâmetros específicos em relação a responsabilização pelo vazamento de dados, sendo:

Em casos de vazamento de dados decorrentes de não conformidade com as regulamentações legais, os agentes de tratamento de dados são responsáveis e podem ser sancionados administrativamente. A LGPD, nos artigos 42 a 45, estabelece a responsabilidade civil dos agentes de tratamento, exigindo que o responsável pelo controle ou operação de dados pessoais indenize qualquer pessoa que sofra danos patrimoniais, morais, individuais ou coletivos devido ao tratamento de dados, não especificando a necessidade de culpa. Em resumo, a LGPS regulamenta a transparência nos vazamentos de dados, e os agentes de tratamento de dados são responsáveis por indenizar terceiros afetados por violações, independentemente da questão da culpa (BRASIL, 2018; ARAÚJO; FIGUEIREDO, 2020 *apud* ROCHA; HORITA, 2024, p. 33).

Neste sentido, além das responsabilidades expostas, a ausência de consentimento do titular dos dados em caso de vazamento ou até mesmo no tratamento inadequado destes resta, ainda mais, comprovada a responsabilidade no vazamento de dados. O consentimento, na LGPD, é essencial para o seu compartilhamento e arquivamento e, caso não haja, é possível demonstrar que o vazamento foi devidamente contra o que é estabelecido em lei (SIQUEIRA, 2023, p. 19).

GOLPES BANCÁRIOS E A LGPD – FALTA DE LEGISLAÇÃO POSITIVA

Com a globalização, os mecanismos digitais passaram a ser cada vez mais presentes e, não obstante, essenciais na vida do ser humano. A cultura digital passou a influenciar praticamente todos os campos da vida de qualquer indivíduo, como nos meios de comunicação, nos jogos, nos cinemas, na educação e, principalmente, em relação aos acessos a economias em instituições bancárias. A partir da implementação dessa cultura digital, as distâncias passaram a ser reduzidas e um exemplo disso é o cinema, que hoje, filmes e séries podem ser acessados através de plataformas de *streaming* (LAIO; OLIVEIRA; THEES, 2022, p. 2).

Em instituições bancárias, essa redução de distância não é diferente. Houveram grandes impactos que foram causados por essa revolução digital, sendo que “a utilização do comércio eletrônico pelo setor bancário mostrou-se uma evolução inevitável, diante do processo de digitalização de todos os demais serviços fornecidos ao consumidor” (VASCONCELOS, 2023, p. 87). Acontece que, o setor financeiro e também o de oferta de serviços bancários, para além de relações de consumo, também são regulamentados por

normas direcionadas ao adequado funcionamento do sistema financeiro, que é estabelecido pelo Banco Central do Brasil (VASCONCELOS, 2023, p. 87).

O PIX consiste em uma dessas inovações, que é “uma ferramenta instantânea de pagamento, em que transferem recursos em segundos, a qualquer hora ou dia. Essa ferramenta ainda aumenta a velocidade de pagamentos ou transferências que são realizados e recebidos” (BANCO CENTRAL DO BRASIL, 2021 *apud* SILVA; CERKEWUTA, 2022, p. 73). Para que o pagamento via PIX seja realizado, é necessário que as chaves sejam cadastradas, podendo ser o CPF ou o CNPJ, o número de telefone celular, o e-mail ou até mesmo um código aleatório que é gerado pelo próprio banco. Com isso, a chave PIX passa a estar vinculada àquela pessoa natural, que passa a ser considerada como um dado pessoal (SILVA; CERKEWUTA, 2022, p. 73). A partir disso, as instituições bancárias precisam acompanhar as movimentações para questões de segurança, providenciando medidas que ajudem a proteger os dados pessoais de possíveis fraudes bancárias (CAVALCANTE; TAVARES, 2023, p. 314).

Além do conhecido golpe do PIX, Vasconcelos (2023, p. 111) cita os chamados *phishing* e *phaming*, que possuem a “capacidade de utilização de forma fraudulenta de dados de terceiros, sem consentimento, conhecimento, e muitas vezes de forma difícil de ser rastreada e evitada”. Com as fragilidades trazidas pelo *internet banking*, as fraudes estão cada vez mais frequentes, usando indevidamente os dados do consumidor, podendo ocorrer através da introdução de seus dados em sites falsos, por exemplo, o que, de acordo com a jurisprudência do STJ, na Súmula n. 479, “imputar ao consumidor a responsabilidade pela governança de seus dados pessoais mostra-se uma tarefa praticamente impossível de se realizar como visto, tamanha é a quantidade de base de dados espalhadas” (VASCONCELOS, 2023, p. 112).

Diante disso, a LGPD, na defesa dos dados pessoais, precisa buscar a integral proteção destes, frente às diversas vulnerabilidades do consumidor dentre desse movimento contemporâneo do meio digital.

A Lei é aplicável a uma variedade de situações em que há tratamento de dados pessoais, inclusive no setor público, e, assim, não se restringe às hipóteses em que se configura uma relação de consumo. Não obstante, a LGPD é um mecanismo importante para proteger a liberdade e a privacidade dos consumidores, de modo que o próprio Legislador promoveu o diálogo entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor, ao prever expressamente como fundamento da proteção de dados a defesa do consumidor, no seu art. 2º, VI; ao estabelecer a possibilidade de que os direitos dos titulares de dados, quando também consumidores, possam ser exercidos igualmente perante organismos de defesa do consumidor, em seu art. 18, § 8º; e ao determinar, no art. 45, que as hipóteses de violação do direito do titular no âmbito das

relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente. Finalmente, a complementaridade entre ambas as leis é consolidada no art. 64, que estabelece que os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que o Brasil seja parte. Como se nota, tal dispositivo visa consolidar na disciplina da proteção de dados a aplicação harmônica e coordenada de normas de um sistema jurídico, expressa no conceito de diálogo das fontes, formulado por Cláudia Lima Marques (DONEDA e MENDES, 2018, p. 23).

A LGPD, como o próprio nome diz, apresenta um parâmetro geral do resguardo dos dados pessoais, e, por isso, deve agir em conjunto a outras leis e normas para que possa surtir efeitos jurídicos relevantes. Junto ao Código de Defesa do Consumidor, a LGPD tem a capacidade de se adequar para a promoção de uma proteção integral do indivíduo, seja de forma direta ou indireta, fornecendo aos consumidores uma maior possibilidade de controle dos dados, consagrando “no ordenamento jurídico as bases fundamentais para punição dos responsáveis por qualquer dano causado pelo mal-uso das informações (MALDONADO; SOTERO, 2021, p. 225 *apud* VASCONCELOS, 2023, p. 118).

CONSIDERAÇÕES FINAIS

Diante do estudo, foi possível identificar que o meio digital teve uma ascensão muito repentina e que as normas brasileiras, de acordo com o tempo, estava ficando em desvantagem em relação a normatização dessas novidades. Neste sentido, a LGPD foi essencial para o estabelecimento de parâmetros dos dados pessoais nos meios digitais, pois necessitava de um esclarecimento e de uma visão mais aprofundada, já que, junto com as vantagens, também vieram desvantagens, que incluem fraudes e golpes com dados pessoais.

Por isso, o estabelecimento no texto constitucional de título de direito fundamental, junto com a LGPD e também outras leis que revelam o tema abordado, é primordial para se estabelecer a importância da abordagem e também do aprofundamento desse tema em relação a novas normatizações específicas para o resguardo desses dados. Hoje, é necessária a junção de vários dispositivos para haja a devida punição ou efetivação da norma em relação ao uso dos dados pessoais sem o consentimento do titular. Visto isso, é necessário que haja leis específicas abordando sobre o assunto, para que não haja brechas para a sua efetivação.

Por fim, é de suma importância a necessidade das Instituições Financeiras em investir em plataformas que visem mitigar o risco de fraudes e golpes, a fim de proteger os consumidores e estarem de acordo com as normas vigentes.

REFERÊNCIAS

AGENCIA SENADO. **Marco Civil da Internet completa dez anos ante desafios sobre redes sociais e IA.** 2024. Disponível em: <<https://www12.senado.leg.br/noticias/materias/2024/04/26/marco-civil-da-internet-completa-dez-anos-ante-desafios-sobre-redes-sociais-e-ia>>. Acesso em: 16 set. 2024.

ARAÚJO, Janaína. **Dez anos da vigência da Lei Carolina Dieckmann: a primeira a punir crimes cibernéticos.** 2023. Disponível em: <<https://www12.senado.leg.br/radio/1/noticia/2023/03/29/dez-anos-de-vigencia-da-lei-carolina-dieckmann-a-primeira-a-punir-crimes-ciberneticos>>. Acesso em: 13 set. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 13 set. 2024.

BRASIL. Governo Federal – Ministério da Justiça e Segurança Pública. **4 anos da Lei Geral de Proteção de Dados.** 2024. Disponível em: <[https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/4-anos-da-lei-geral-de-protecao-de-dados-pessoais#:~:text=As%20primeiras%20iniciativas%20de%20legislar,prote%C3%A7%C3%A3o%20dos%20titulares%20de%20dados](https://www.gov.br/anpd/pt-br/assuntos/noticias-periodo-eleitoral/4-anos-da-lei-geral-de-protecao-de-dados-pessoais#:~:text=As%20primeiras%20iniciativas%20de%20legislar,prote%C3%A7%C3%A3o%20dos%20titulares%20de%20dados.)>. Acesso em: 16 set. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990.** 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm>. Acesso em: 13 set. 2024.

CAVALCANTE, Jairo Nascimento; TAVARES, Ismael Andrade. **A responsabilidade civil das instituições bancárias por danos sofridos no golpe do PIX.** 2023. Disponível em: <<https://revistas.faculdefacit.edu.br/index.php/JNT/article/view/2536/1709>>. Acesso em: 21 set. 2024.

FERNANDES, Ana Lívia Silva; PEREIRA, Letícia Fernandes; PEDROSA, Jussara de Melo. **Responsabilidade civil por vazamento de dados pessoais: uma análise sob a luz da LGPD.** 2024. Disponível em: <<https://dspace.uniube.br:8443/bitstream/123456789/2711/1/TCC%20Ana%20L%20c%20advia%20e%20Let%20c%20adcia%20Fernandes.pdf>>. Acesso em: 20 set. 2024.

GALVÃO, Heiderivirlandia Leite *et al.* **Incidentes de segurança: regulação e prática de vazamento de dados pessoais frente à LGPD.** 2024. Disponível em: <<https://idonline.emnuvens.com.br/id/article/view/4042/6035>>. Acesso em: 20 set. 2024.

LAIO, Tarliz; OLIVEIRA, Josy Teixeira Silva de; THEES, Andrea. **Reflexos da responsabilidade social em um curso de extensão de tecnologias digitais para idosos.** 2022. Disponível em: <<https://anais.eneds.org.br/index.php/eneds/article/view/680/568>>. Acesso em: 21 set. 2024.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de Almeida. **Da evolução das legislações sobre a proteção de dados: a necessidade de reavaliação do papel do**

consentimento como garantidor da autodeterminação informativa. Revista de Direito, Viçosa, v. 12, n. 02. 2020. Disponível em: <<https://periodicos.ufv.br/revistadir/article/download/10597/5880/48773>>. Acesso em: 13 set. 2024.

QUINTILIANO, Leonardo. **Contexto histórico e finalidade da Lei Geral de Proteção de Dados (LGPD)**. 2021. Disponível em: <<https://www.jusbrasil.com.br/artigos/contexto-historico-e-finalidade-da-lei-geral-de-protecao-de-dados-lgpd/1203647706>>. Acesso em: 13 set. 2024.

RIBEIRO, Rafaela Macedo. **Fraudes bancárias como afronta ao direito da personalidade**: a importância da combinação da LGPD e do BACEN no sistema financeiro. 2023. Disponível em: <<https://repositorio.ufpb.br/jspui/handle/123456789/27656>>. Acesso em: 22 set. 2024.

ROCHA, José Vinicius Pires; HORITA, Fernando Henrique da Silva. **Vazamento de dados à luz da Lei Geral de Proteção de Dados Pessoais**: responsabilidade civil dos fornecedores de serviços digitais. Revista Científica REMAD, vol. 1, 2024. Disponível em: <<http://revistas.fasipe.com.br:3000/index.php/REMAD/article/view/333/303>>. Acesso em: 20 set. 2024.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da Lei Geral de Proteção de Dados (LGPD) – L. 13.709/2018. Rev. Direitos fundam. democ., v. 26, n. 2, p. 81-106, mai./ago. 2021. Disponível em: <<https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172/694>>. Acesso em: 16 set. 2024.

SILVA, Ana Jasmim Barbosa da; CEREWUTA, Pollyanna Marinho Medeiros. **A responsabilidade civil das instituições bancárias por danos sofridos no golpe do PIX**. 2022. Disponível em: <<https://revistas.faculdefacit.edu.br/index.php/JNT/article/view/1942/1314>>. Acesso em: 21 set. 2024.

SIQUEIRA, Klara Nina Vieira de. **A aplicação da responsabilidade civil à luz da LGPD**: um estudo sobre o vazamento de dados pelo INSS. 2023. Disponível em: <<http://www.repositorio.fdv.br:8080/handle/fdv/1646>>. Acesso em: 20 set. 2023.

SOARES, Fabiana de Menezes; JARDIM, Tarciso Dal Maso; HERMONT, Thiago Brasileiro Vilar. Lei de **Acesso à Informação no Brasil**: o que você precisa saber. 2013. Disponível em: <<https://www12.senado.leg.br/transparencia/indice-de-transparencia-dos-portais-legislativos/arquivos/sobre/cartilha-lai>>. Acesso em: 13 set. 2024.

UNICEF. **Declaração Universal dos Direitos Humanos** – Adotada e proclamada pela Assembleia Geral das Nações Unidas (resolução 217 A III) em 10 de dezembro de 1948. Disponível em: <<https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos>>. Acesso em: 13 set. 2024.

VASCONCELOS, Marta Barros. **A proteção de dados do consumidor no ambiente digital**: a utilização da LGPD na mitigação de fraudes bancárias. 2023. Disponível em: <<https://repositorio.ufrn.br/handle/123456789/54735>>. Acesso em: 21 set. 2024.