CLONAGEM DE CARTÃO DE CRÉDITO SOB A PERSPECTIVA DA LEI GERAL DE PROTEÇÃO DE DADOS

CREDIT CARD CLONING FROM THE PERSPECTIVE OF THE GENERAL DATA PROTECTION LAW

Leandro Wünsche Bacellar[1]
Elizeu Luiz Toporoski[2]

RESUMO

O avanço tecnológico transformou os meios de pagamento, substituindo o uso de dinheiro em espécie pelo cartão de crédito, facilitando transações online. No entanto, essa evolução também trouxe desafios, como a vulnerabilidade a fraudes, invasões e clonagem, gerando preocupações com a segurança dos dados pessoais e bancários. Nesse cenário, as instituições financeiras têm sido alvo de ações judiciais de consumidores prejudicados por crimes virtuais. A implementação da Lei Geral de Proteção de Dados (LGPD) é essencial para garantir a privacidade dos titulares, exigindo medidas rigorosas de segurança dos operadores. O presente trabalho busca demonstrar que a aplicação da LGPD pode prevenir vazamentos e fraudes, promovendo um ambiente digital mais seguro para os consumidores.

Palavras-chave: cartão de crédito; clonagem; dados pessoais; instituições financeiras; LGPD.

ABSTRACT

Technological advancement has transformed payment methods, replacing cash with credit cards and facilitating online transactions. However, this evolution has also brought challenges, such as vulnerability to fraud, hacking, and cloning, raising concerns about the security of personal and banking data. In this scenario, financial institutions have become targets of lawsuits from consumers harmed by cybercrimes. The implementation of the General Data Protection Law (GDPL) is essential to ensure the privacy of data subjects, requiring operators to adopt stringent security measures. This work aims to demonstrate that the application of the GDPL can prevent data breaches and fraud, promoting a safer digital environment for consumers.

Key words: credit card; cloning; personal data; financial institutions; GDPL.

[1]Acadêmico do curso de Direito da Universidade do Contestado, Campus Mafra. Santa Catarina. Brasil. E-mail: leandro.bacellar@aluno.unc.br.
[2]Mestre em Direito. Professor do curso de Direito da Universidade do Contestado, Campus Mafra. Santa Catarina. Brasil. E-mail: elizeu.toporoski@gmail.com. ORCID: https://orcid.org/0009-0005-1283-9094

Artigo recebido em: 15/09/2024
Artigo aceito em: 09/10/2024
Artigo publicado em: 18/12/2024
Doi: https://doi.org/10.24302/acaddir.v6.5673

1 INTRODUÇÃO

Com o avanço da tecnologia, as formas de pagamento passaram por transformações significativas. O dinheiro em espécie foi amplamente substituído pelo cartão de crédito, que se tornou um facilitador para pagamentos virtuais, permitindo que os consumidores realizem compras online sem sair de casa. Essa evolução trouxe conveniência, mas também acarretou uma série de desafios, como o aumento no armazenamento de informações pessoais em bancos de dados digitais.

Essa prática, embora ofereça benefícios em termos de agilidade e praticidade, também elevou a suscetibilidade a uma variedade de ameaças, como golpes, vazamentos de dados, invasões por hackers e clonagem de cartões. Assim, enquanto a tecnologia transforma o modo como interagimos financeiramente, ela também exige uma vigilância constante para proteger as informações pessoais e garantir a segurança nas transações.

Diante desse cenário, a responsabilidade das instituições financeiras tem sido cada vez mais questionada pelos consumidores. O tema ganhou destaque em diversos julgamentos nos tribunais brasileiros, onde ações indenizatórias têm sido movidas contra os bancos. Os consumidores buscam responsabilizá-los por crimes como a clonagem de cartões e pela perda irreversível de suas contas bancárias, refletindo a crescente preocupação com a segurança de suas informações.

A partir do momento que é detectada uma fraude no armazenamento de tais dados, questiona-se quais as medidas de segurança deveriam ter sido adotadas pelo operador e como deveriam funcionar de forma preventiva. Tem-se que, a instituição financeira é controladora de dados, uma vez que capta os dados pessoais de seus consumidores para realizar cadastros e, por isto, possui responsabilidades pelo tratamento desses dados pessoais.

Neste norte, em 14 de agosto de 2018 foi promulgada a Lei Geral de Proteção de Dados, que tem como objetivo traçar estratégias e normas de segurança para os

controladores e operadores de dados pessoais, para diminuição e prevenção de golpes nos meios digitais.

A legislação não apenas reforça a responsabilidade dos operadores, mas também busca assegurar que os direitos dos consumidores sejam respeitados em um ambiente digital cada vez mais complexo.

Nesse contexto, a questão central que surge é: em que medida as instituições financeiras são responsáveis pela proteção das informações de seus clientes? Como elas podem, de forma eficaz, prevenir fraudes e garantir a segurança dos dados em conformidade com a legislação vigente, especialmente após a promulgação da Lei Geral de Proteção de Dados (LGPD) em 2018? A problemática envolve não apenas a responsabilidade legal e ética das instituições, mas também a necessidade de mecanismos preventivos robustos para minimizar os impactos de crimes como a clonagem de cartões.

O presente estudo, realizado por meio de pesquisa bibliográfica e documental, e uma abordagem indutiva, tem como objetivo demonstrar que a aplicação da LGPD pode ser uma possibilidade de instrumento preventivo na mitigação da clonagem de cartão de crédito. Além disso, com a adoção de tais práticas de segurança, as instituições financeiras não apenas cumprem a legislação, mas também fortalecem sua credibilidade e confiança perante os consumidores, criando um ambiente digital mais seguro.

2 O SERVIÇO DE CARTÃO DE CRÉDITO

Com o avanço da tecnologia, as formas de pagamento passaram por mudanças significativas, substituindo cada vez mais o dinheiro em espécie por transferência eletrônica.

O uso do dinheiro e do cheque foi substituído pelo cartão de débito e de crédito, como forma de pagamento. Essa substituição pode ser explicada por várias razões, entre elas: a facilidade de porte do *smart card* (cartão inteligente); a expansão das compras pela internet, em que muitos fornecedores disponibilizam apenas as formas eletrônicas de pagamento; impossibilidade de sustação por desacordo comercial; diminuição do risco de inadimplência, como acontece com o cheque sem fundo; segurança quanto ao porte de dinheiro em espécie, entre outras (TEIXEIRA, 2023).

O sistema do cartão de crédito é um contrato complexo, composto por algumas sub modalidades contratuais: entre o titular e o emissor, entre fornecedor e titular e entre emissor e fornecedor. As partes que compõem o sistema são: 1) contrato de emissão, que é celebrado entre a instituição financeira emissora do cartão e o titular do cartão; 2) contrato de aquisição de bens e serviços, celebrado entre o estabelecimento e titular do cartão e 3) contrato de credenciamento, realizado entre estabelecimento e credenciadora (SOUZA, 2013).

Embora o cartão de crédito seja a forma de pagamento mais utilizada para compras online, ele apresenta riscos significativos, especialmente relacionados à segurança no envio de informações pessoais, incluindo dados bancários dos clientes, para os ambientes digitais dos fornecedores.

2.1 VÍCIO NA PRESTAÇÃO DE SERVIÇO

A evolução das formas de pagamento trouxe conveniência, mas também elevou os riscos de segurança.

O aumento das transações digitais e a expansão do comércio eletrônico, também aumentou o número de golpes virtuais, vazamento de dados pessoais, invasão por hackers e principalmente a clonagem de cartões (MOTA, 2021).

Segundo a pesquisa da Confederação Nacional de Dirigentes Lojistas (CNDL), em parceria com o Serviço de Proteção ao Crédito (SPC Brasil), divulgada no final de 2023[3], mais de 7 milhões de brasileiros afirmaram já ter sido vítimas de algum golpe financeiro ou tentativa de um nos últimos 12 meses. E o principal tipo de golpe foi o de cartão clonado.

Nos casos de clonagem de cartão, a instituição financeira é considerada a fornecedora do serviço de administração do cartão de crédito. Se houver um vício na segurança desse serviço que permita a clonagem do cartão, a instituição é responsável pelos danos causados ao consumidor, independentemente de culpa, conforme o dispositivo do art. 14 do CDC:

[3]MENESES, Amanda. Cartão clonado: 5 formas mais comuns de cair no golpe. **Invest News**, 11 jun. 2023. Disponível em: https://investnews.com.br/economia/ cartao-clonado-o-que-fazer/. Acesso em: 03 out. 2024.

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos (BRASIL, 1990).

Diante desse cenário, a responsabilidade das instituições financeiras vem sendo confutada pelos consumidores. Este tema tem sido objeto de diversos julgamentos nos tribunais brasileiros, em ações indenizatórias movidas pelos consumidores contra as instituições financeiras. Os consumidores buscam responsabilizar os bancos pela clonagem de cartão e pela consequente perda irreversível dos fundos de suas contas bancárias.

2.2 RESPONSABILIDADE DAS INSTITUIÇÕES FINANCEIRAS

A responsabilidade civil da instituição financeira refere-se à obrigação que estas instituições têm de reparar danos causados a terceiros devido a atos ou omissões praticados no exercício de suas atividades.

O autor Sergio Cavalieri Filho (2019, p. 534), discorre que o código do consumidor, em seu art. 3º, §º, inclui expressamente a atividade bancária no conceito de serviço. Desde então, não resta a menor dúvida de que a responsabilidade do banco é objetiva em relação aos clientes, nos termos do art. 14 do mesmo Código. Responde, independentemente de culpa, pela reparação dos danos causados aos seus clientes por defeitos decorrentes dos serviços que lhe presta. O que pode discutir quanto às atividades dos bancos é se quem se encontra do outro lado da operação é ou não consumidor, já que os contratos bancários nem sempre são contratos de consumo, nos termos da definição do art. 2º, caput, do CDC.

Neste cenário, o autor aborda a respeito da violação do sistema eletrônico, onde incide a teoria do risco do empreendimento, segundo a qual todo aquele que se disponha a exercer alguma atividade no mercado de consumo tem o dever de responder pelos eventuais vícios ou defeitos dos bens e serviços fornecidos, independentemente de culpa. Esse dever é imanente ao dever de obediência às normas técnicas e de segurança, bem como aos critérios de lealdade, quer perante os bens e serviços ofertados, quer perante os destinatários dessas ofertas (CAVALIERI FILHO, 2019, p. 540).

Se o sistema eletrônico do banco for violado, cabe à instituição financeira assumir os riscos do seu empreendimento. Caso o sistema não ofereça a segurança esperada, o banco deve ser responsabilizado pelo defeito.

O autor Arnaldo Rizzardo (2019, p. 457) aborda sobre a incidência do art. 14 do CDC, pelo qual

> o fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.

Ressalta ainda que, se o titular do cartão dá acesso a terceiro ao número e à senha, não há como responsabilizar a instituição bancária. Mas se o criminoso apõe um leitor de fita magnética (conhecida como 'chupa-cabra' no Brasil, e que nos Estados Unidos são denominados '*skimmer scanners*') na fenda existente no caixa eletrônico, permitindo que o aparelho leia as informações, ocorrendo a cópia da senha, sendo em seguida lidas pelo caixa eletrônico original, existe realmente a responsabilidade por defeito na prestação de serviços. Incide, aí, a responsabilidade (RIZZARDO, 2019, p. 457).

A nossa Corte de Justiça (STJ) editou enunciado acerca da responsabilidade civil das instituições financeiras:

Súmula 479 – "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias" (BRASIL, 2012).

Diante da vulnerabilidade do consumidor, por vezes até hipossuficiente, e do consequente desiquilíbrio que é inerente à relação de consumo, a responsabilidade civil dos fornecedores de produtos ou serviços será sempre objetiva, visto independer da ocorrência de dolo ou culpa, devendo assim e diante da Teoria do Risco Criado, reparar os danos que emergirem desta relação (SILVA; MOREIRA, 2021).

A responsabilidade civil das instituições financeiras é um tema complexo que envolve uma série de fatores jurídicos e práticos. Nesta linha de proteção de dados e segurança, é importante destacar a responsabilidade das instituições em adotar medidas de segurança para o armazenamento desses dados. Atualmente, a

legislação brasileira, possui uma lei específica para esse assunto, a Lei Geral de Proteção de Dados, que será abordada adiante.

3 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados (Lei n. 13.709/2018) foi promulgada em 18 de agosto de 2018, com o objetivo de regulamentar o uso, a proteção e a transferência de dados pessoais no Brasil.

A regulamentação sobre proteção de dados auferiu relevância após o desenvolvimento das tecnologias e o contexto social que facilitava a utilização de informações pessoais sem regras pré-estabelecidas de como coletar e processar essas informações (LIMA; SAMANIEGO; BARONOSVKY, 2021).

O autor Tarcisio Teixeira (2023, p. 52) descreve que, para efeito da lei, conforme o art. 5º, inc. X da LGPD, conceitualmente tratamento de dados consiste em

> Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Enfatiza ainda que, sinteticamente a Lei Geral de Proteção de Dados aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, físico ou digital (TEIXEIRA, 2023, p. 52).

A Lei n. 13.709/18 apresenta em sua íntegra sanções para possíveis violações, em face de uma proposta rebuscada por regras estabelecidas em meio a um conjunto de aspectos disciplinares de autoridade nacional, orientados pela fixação de hipóteses para a coleta dos dados, com categorias que detalham minuciosamente as especiais condições para o tratamento, o armazenamento e os direitos dos titulares de dados sensíveis, além de circunscrever os ditames para o armazenamento dos dados de empresas (com suas obrigações), de indivíduos e de seus segmentos (ALMEIDA; SOARES, 2022).

É necessário frisar que as instituições financeiras funcionam como agentes de tratamento de dados pessoais, pois possuam suas próprias bases de dados dos seus

consumidores, no qual também armazenam suas informações. Assim, também devem zelar pela segurança dessas informações e dados pessoais, evitando que possam ser obtidos de forma indevida e, portanto, facilitar a sua utilização também indevida.

A partir da LGPD, tem-se um marco legal para impor uma correspondência prática às suas disposições. O que antes poderia ocorrer apenas eventual e espontaneamente (sob a forma de autorregulação para governança e gerenciamento de riscos relativos ao uso de dados pessoais), deve agora ser realizado por força de lei e com base na LGPD, por controladores e operadores (GARBACCIO; KISCHELEWSKI, 2024, p. 158)

A LGPD surgiu como uma medida crucial para mitigar tais problemas, impondo diretrizes rigorosas para o tratamento de informações pessoais e fortalecendo a segurança nas transações digitais.

3.1 A EFETIVIDADE DA LGPD NA PROTEÇÃO DE DADOS ARMAZENADOS PELAS INSTITUIÇÕES FINANCEIRAS

É necessário frisar que as instituições financeiras funcionam como agentes de tratamento de dados pessoais, pois possuam suas próprias bases de dados dos seus consumidores, no qual também armazenam suas informações.

Assim, também devem zelar pela segurança dessas informações e dados pessoais, evitando que possam ser obtidos de forma indevida e, portanto, facilitar a sua utilização também indevida (VASCONCELOS, 2023, p. 97).

Visando o sigilo dos dados pessoais, o artigo 46 da LGPD expressa a necessidade de os agentes de tratamento adotarem medidas de segurança, técnicas e administrativas adequadas para proteção de dados pessoais quanto a acessos não autorizados (por exemplo, invasão de servidor) e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (TEIXEIRA, 2023, p. 64).

Vejamos:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda,

> alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução (BRASIL, 2018).

Discriminação, roubo de identidade, fraude, limitação de direitos, perdas financeiras, danos à reputação, perda de controle acerca de suas informações são apenas alguns desses exemplos. É justamente para evitar que esses dados sensíveis caiam em mãos de terceiros mal-intencionados que legislações do mundo todo (e a LGPD) exigem que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas aptas a proteger os dados que tratam (FRAZÃO; TEPEDINO; OLIVA, 2023).

Grande parte das atividades econômicas e da oferta de serviços públicos depende de informações pessoais e, independentemente de haver retorno financeiro ou não, é responsabilidade do controlador e do operador de dados pessoais o uso adequado e a proteção dos dados. Se essa responsabilização já existia anteriormente, com base na legislação civil e consumerista, essa possibilidade foi significativamente reforçada pela promulgação da LGPD (GARBACCIO; KISCHELEWSKI, 2024, p. 162).

Contudo, a sua efetividade depende da implementação prática das normas estabelecidas, do comprometimento das instituições e da capacidade de adaptação às novas exigências e desafios no ambiente de proteção de dados.

A respeito das políticas de governança, o autor Tarcisio Teixeira (2023, p. 66), discorre em sua obra que os operadores devem avaliar os seus riscos conforme as suas operações, o fluxo de dados e as exigências legais para adequar às ferramentas jurídicas, administrativas e informáticas com eficiência e sem burocratizar o negócio; treinar e sensibilizar os colaboradores; indicar o operador e encarregado de dados; minimizar a instituição de riscos, responsabilidades e penalidades desnecessárias e implantar o *compliance* (conformidade) em proteção de dados na instituição, ou seja, adequando-o à LGPD.

É nesse ambiente que a LGPD, em seu artigo 50, impulsiona a adoção de regras de boas práticas e de governança por controladores e operadores de dados como meio de proteção ao titular de dados pessoais:

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.
> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.
> § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá:
> I - implementar programa de governança em privacidade que, no mínimo:
> a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;
> II - demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.
> § 3º As regras de boas práticas e de governança deverão ser publicadas e atualizadas periodicamente e poderão ser reconhecidas e divulgadas pela autoridade nacional.

Reconhece-se que o incremento das atividades de tratamentos de dados é acompanhado respectivamente do aumento dos riscos, podendo ser atingidos os direitos fundamentais dos titulares ou suas liberdades civis, além de prejudicar a

reputação e as operações do agente de tratamento, acarretando perdas financeiras e de mercado (GARBACCIO; KISCHELEWSKI, 2024, p. 164)

A Min. Nancy Andrighi (BRASIL, 2023) aborda sobre a LGPD no que tange ao armazenamento de dados no seguinte trecho do relatório de julgamento do REsp n. 2.077.278/SP:

> CONSUMIDOR. RECURSO ESPECIAL. AÇÃO DECLARATÓRIA DE INEXIGIBILIDADE DE DÉBITO POR VAZAMENTO DE DADOS BANCÁRIOS CUMULADA COM INDENIZAÇÃO POR DANOS MORAIS E REPETIÇÃO DE INDÉBITO. GOLPE DO BOLETO. TRATAMENTO DE DADOS PESSOAIS SIGILOSOS DE MANEIRA INADEQUADA. FACILITAÇÃO DA ATIVIDADE CRIMINOSA. FATO DO SERVIÇO. DEVER DE INDENIZAR PELOS PREJUÍZOS. SÚMULA 479/STJ. RECURSO ESPECIAL PROVIDO.
> 14. Por outro lado, os dados sobre operações financeiras são, em regra, presumivelmente de tratamento exclusivo pelas instituições financeiras. No ponto, a Lei Complementar 105/2001 estabelece que “as instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados” (art. 1º), constituindo dever jurídico dessas entidades “não revelar, salvo justa causa, as informações que venham a obter em virtude de sua atividade profissional.
> 15. Portanto, dados pessoais vinculados a operações e serviços bancários são sigilosos e cujo tratamento com segurança é dever das instituições financeiras. Desse modo, seu armazenamento de maneira inadequada, a possibilitar que terceiros tenham conhecimento dessas informações e causem prejuízos ao consumidor, configura falha na prestação do serviço (art. 14 do CDC e 43 da LGPD).
> 17. Diante do vazamento de dados sigilosos do consumidor, inequívoca é a responsabilidade do fornecedor pelo defeito no serviço prestado. O próprio art. 44 da LGPD, à semelhança do art. 14, § 1º, do CDC, estabelece que o tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar, considerados o modo pelo qual é realizado, o resultado e os riscos que razoavelmente dele se esperam, as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado, entre outras circunstâncias.
> 18. Sobre o art. 44 da LGPD, inclusive, a doutrina leciona que “a regra coloca em destaque, assim como ocorre em relação à responsabilidade do fornecedor no CDC, a questão relativa aos riscos do desenvolvimento, uma vez que delimita a extensão do dever de segurança àquela esperada em razão das 'técnicas de tratamento de dados disponíveis à época em que foi realizado' e, considerando “a previsibilidade de uma atualização e avanço técnico em atividades vinculadas à tecnologia da informação, mais veloz do que em outras atividades econômicas (MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o direito do consumidor. Revista dos Tribunais, São Paulo, v. 1009, nov., 2019).
> 19. Acrescente-se, ainda, que o art. 45 da LGPD esclarece 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, em especial, ao regime da responsabilidade objetiva por fato do serviço (art. 14 do CDC). 20. Em síntese, o tratamento indevido de dados pessoais bancários configura defeito na prestação de serviço, notadamente quando tais informações são utilizadas por estelionatário para facilitar a aplicação de golpe em desfavor do consumidor (BRASIL, 2023).

O acórdão trata de decisão em Recurso Especial, interposto por consumidora que ajuizou ação declaratória de inexigibilidade de débito por vazamento de dados bancários cumulada com indenização por danos morais e repetição de indébito em face de instituição financeira, vítima de fraude bancária.

Analisando a fundamentação do voto da relatora, entende-se que o tratamento inadequado de dados sigilosos configura um defeito na prestação do serviço, levando à responsabilidade objetiva da instituição pelos danos causados ao consumidor. A decisão reforça que, se houver vazamento de dados que possibilite fraudes, a instituição financeira deve indenizar o consumidor, alinhando-se ao entendimento de que as instituições devem garantir a segurança das informações sob sua custódia, conforme os artigos 14 do CDC e 44 da LGPD. Neste caso exposto, a instituição financeira foi condenada a indenizar a consumidora.

A obrigação legal de adequação às normas de proteção dos dados pessoais é uma realidade. Não é mais possível que as organizações públicas e privadas adiem a absorção dos dispositivos da LGPD. Para que a conformidade legal possa se materializar, é preciso que empresas e órgãos da administração pública direta e indireta invistam no desenvolvimento e implementação de programas de governança e boas práticas, em cumprimento às disposições da LGPD (GARBACCIO; KISCHELEWSKI, 2024, p. 188)

Do ponto de vista legal, o uso de técnicas administrativas adequadas se apresenta como uma ferramenta eficaz para proteger o consumidor contra fraudes, acessos não autorizados e incidentes como destruição, perda ou tratamento inadequado de dados.

A clonagem de cartão de crédito é apenas é exemplo frequente de fraudes bancárias, que impactam diretamente a confiança do consumidor nas relações de consumo. Nesse contexto, a adoção de medidas preventivas e de segurança não apenas fortalece a defesa em litígios, mas também consolida uma política institucional de preservação da credibilidade da instituição financeira, garantindo a confiança daqueles que nela depositam seu patrimônio.

4 CONSIDERAÇÕES FINAIS

Através do presente estudo, verificamos que a crescente digitalização dos meios de pagamento trouxe consigo benefícios significativos, como a praticidade e a eficiência das transações online, mas também aumentou a vulnerabilidade a riscos de segurança, como fraudes e vazamentos de dados. A substituição do dinheiro em espécie por cartões de crédito e débito, enquanto promove a conveniência, também expõe os consumidores a novos desafios. A clonagem de cartões e o vazamento de dados se tornaram problemas recorrentes, gerando uma crescente demanda por proteção mais robusta.

Neste cenário, a responsabilidade das instituições financeiras tem sido amplamente debatida e questionada, especialmente em relação à segurança das informações pessoais dos consumidores. De acordo com o Código de Defesa do Consumidor (CDC), as instituições financeiras têm uma responsabilidade objetiva, ou seja, independentemente de culpa, pelos danos causados aos consumidores devido a falhas na prestação dos serviços. Isso inclui situações em que há vícios na segurança que permitem a clonagem de cartões ou outros tipos de fraudes. A jurisprudência brasileira, incluindo a Súmula 479 do Superior Tribunal de Justiça (STJ), reforça a ideia de que as instituições financeiras devem responder pelos danos causados por fraudes e delitos praticados por terceiros, desde que tais fraudes estejam relacionadas a fortuitos internos no contexto das operações bancárias.

A Lei Geral de Proteção de Dados (LGPD), está em vigor desde setembro de 2020 e representa um marco importante na proteção de dados pessoais no Brasil. A legislação impõe diretrizes rigorosas sobre como as informações devem ser coletadas, processadas e armazenadas, exigindo que as instituições financeiras adotem medidas técnicas e administrativas para garantir a segurança desses dados. A LGPD visa não apenas a proteção contra acessos não autorizados e usos indevidos, mas também busca promover uma maior confiança dos consumidores através da transparência e da responsabilidade na gestão dos dados pessoais.

Por fim, a integração de políticas de governança e a adoção de medidas de segurança em conformidade com a LGPD se tornam fundamentais para mitigar riscos e proteger os dados pessoais dos consumidores.

Assim, é possível concluir que, as instituições que adotam essas práticas não só evitam possíveis incidentes de segurança e consequentemente penalidades legais, mas também reforçam sua credibilidade e confiança junto aos seus consumidores. Por tanto, a implementação adequada da LGPD pode ser uma possibilidade de ferramenta para a segurança no ambiente digital e para proteção dos direitos dos consumidores.

REFERÊNCIAS

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados – LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, n. 3, p. 26–45, jul. 2022. DOI: https://doi.org/10.1590/1981-5344/25905.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018**, Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jul. 2024.

BRASIL. **Lei n. 8.078, de 11 de setembro de 1990**. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 10 jul. 2024.

BRASIL. Supremo Tribunal de Justiça. **Informativo n. 791**. Brasília: STJ, Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?b=INFJ&materia=&orgao=&ano=&relator=&operador=e&thesaurus=JURIDICO&p=true&l=25&refinar=S.DISP.&acao=pesquisar&dtdj=&dtde=&livre=791. Acesso em: 14 abr. 2024.

BRASIL. Supremo Tribunal de Justiça. Recurso Especial 2077278/SP. Relatora Min. Ministra Nancy Andrighi, Julgado em 03 out. 2023. **Diário de Justiça do Supremo Tribunal de Justiça**, 09 out. 2023. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202301909798&totalRegistrosPorPagina=40&aplicacao=processos.ea. Acesso em 09 ago. 2024.

BRASIL. Supremo Tribunal de Justiça. Súmula n. 479. **DJe**, Brasília, 01 ago. 2012. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/stj/sumulas/sumula-n-479-do-stj/1289711067. Acesso em: 09 ago. 2024.

CAVALIERI FILHO, Sergio. **Programa de responsabilidade civil.** 13 ed. São Paulo: Atlas, 2019.

FRAZÃO, Ana; TEPEDINO Gustavo; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais**: e suas repercussões no direito brasileiro. São Paulo: Revista dos Tribunais, 2023.

GARBACCIO, Grace Ladeira; KISCHELEWSKI, Flávia Lubieska N. Governança e boas práticas na Lei Geral de Proteção de Dados por meio da conformidade, da gestão de riscos e da accountability. **Revista Brasileira de Estudos Políticos**, v. 128, 15 jul. 2024. DOI: https://doi.org/10.9732/2024.V128.894.

LIMA, Adrianne; SAMANIEGO, Daniela; BARONOSVKY, Thainá. **LGPD para contratos**: adequando contratos e documentos à Lei Geral de Proteção de Dados. Rio de Janeiro: Grupo GEN, 2021. *E-book*.

MENESES, Amanda. Cartão clonado: 5 formas mais comuns de cair no golpe. **Invest News**, 11 jun. 2023. Disponível em: https://investnews.com.br/economia/cartao-clonado-o-que-fazer/. Acesso em: 03 out. 2024.

MOTA, Matheus de Oliveira. **Estudo de caso sobre segurança em e-commerce**. 2021. Trabalho de Conclusão de Curso (Graduação em Ciência da Computação) – Pontifícia Universidade Católica de Goiás. Goiânia, 2021. Disponível em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3206. Acesso em: 13 abr. 2024.

RIZZARDO, Arnaldo. **Responsabilidade civil**. 8. ed. Rio de Janeiro: Grupo GEN, 2019. *E-book*.

SILVA, Samanta da; MOREIRA, Vlademir Vilanova. A responsabilidade civil por vício oculto do produto em relação ao direito de indenização ao consumidor. **Academia de Direito**, v. 3, p. 191–216, 2021. DOI: https:www.doi.org/10.24302/acaddir.v3.3146.

SOUZA, Leonam Machado de. Contrato de cartão de crédito: relação entre “estabelecimento” e credenciadora. **Revista da EMERJ**, Rio de Janeiro, v. 16, n. 62, p. 165-200, 2013. Disponível em: https://ojs.emerj.com.br/index.php/revistadaemerj/issue/view/102/148. Acesso em: 05 ago. 2024.

TEIXEIRA, Tarcisio. **Direito digital e processo eletrônico.** São Paulo: SaraivaJur, 2023. *E-book.*

VASCONCELOS, Marta Barros. **A proteção de dados do consumidor no ambiente digital**: a utilização da LGPD na mitigação de fraudes bancárias. Orientador: Mariana de Siqueira. 2023. 138 f. Dissertação (Mestrado em Direito), Centro de Ciências Sociais Aplicadas, Universidade Federal do Rio Grande do Norte, Natal, 2023. Disponível em: https://repositorio.ufrn.br/handle/123456789/54735. Acesso em 02 out. 2024.