Universidade de Brasília – UnB

Faculdade de Direito – FD

Programa de Graduação em Direito

Incidentes de segurança em instituições financeiras:

Um panorama das decisões dos Tribunais de Justiça Estaduais sobre o tema

LARISSA TELES NONATO DA SILVA

Brasília

2023

Incidentes de segurança em instituições financeiras:

Um panorama das decisões dos Tribunais de Justiça Estaduais sobre o tema

LARISSA TELES NONATO DA SILVA

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharela em Direito pelo Programa de Graduação da Faculdade de Direito da Universidade de Brasília (FD-UnB).

Orientadora: Professora Doutora ANA FRAZÃO

Brasília

2023

Citar como: SILVA, Larissa Teles Nonato. Incidentes de segurança em instituições financeiras: um panorama das decisões dos Tribunais de Justiça Estaduais sobre o tema, 2023. 113 f. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2023.

LARISSA TELES NONATO DA SILVA

INCIDENTES DE SEGURANÇA EM INSTITUIÇÕES FINANCEIRAS:

UM PANORAMA DAS DECISÕES DOS TRIBUNAIS DE JUSTIÇA ESTADUAIS SOBRE O TEMA

Monografia apresentada como requisito parcial para a obtenção do grau de Bacharela em Direito pelo Programa de Graduação da Faculdade de Direito da Universidade de Brasília (FD-UnB).

Aprovada em 11 de julho de 2023

BANCA EXAMINADORA

Professora Doutora **ANA FRAZÃO**

Faculdade de Direito da Universidade de Brasília (FD-UnB)

Orientadora – Presidente

_____

Professora **TAINÁ AGUIAR JUNQUILHO**

Faculdade de Direito da Universidade de Brasília (FD - UnB)

Doutora - Examinadora

Professor **ANGELO PRATA DE CARVALHO**

Faculdade de Direito da Universidade de Brasília (FD - UnB)

Doutorando - Examinador

DEDICATÓRIA

À minha mãe, que é um exemplo de força, dedicação, coragem e amor.

\

AGRADECIMENTOS

"And I thought about how, actually, if you wanted to, you could say the same thing about life. That life is terrifying and overwhelming and it can happen at any moment. And when you're confronted with life you can either be cowardly or you can be brave, but either way, you're going to live. So you might as well be brave."

- **BOB-WAKSBERG, Raphael.** Someone Who Will Love You in All Your Damaged Glory

Durante a escrita deste trabalho, li a coletânea de contos de Raphael Bob-Waksberg, "Someone Who Will Love You in All Your Damaged Glory". O livro é uma tragicomédia sobre o amor e a habilidade de amar. Durante a leitura, me peguei refletindo sobre a importância que as pessoas que me acompanharam nessa trajetória tiveram na minha história, como aluna, como pesquisadora e como ser humano.

A escrita deste trabalho foi uma batalha contra o medo do fim, o medo do novo começo e a capacidade de isolar a vida, que não para, da folha do texto para pesquisar e escrever. O único motivo deste trabalho estar sendo escrito foi o constante apoio de quem acreditou que ele podia ser escrito. O trecho que inspira esse texto é sobre coragem, e é coragem que todas essas pessoas me proporcionaram.

É a essas pessoas que gostaria de agradecer neste breve texto que é absolutamente insuficiente para expressar a gratidão que sinto por todas elas que, de alguma forma, possibilitaram esse momento.

Em primeiro lugar, agradeço à Professora **Ana Frazão**, que teve a paciência de me orientar durante um longo período até a delimitação do escopo do presente trabalho. Agradeço ainda à banca examinadora, nas pessoas do Professor **Angelo Prata de Carvalho** e da Professora **Tainá Aguiar Junquilho**, pela leitura atenta do trabalho e pelos apontamentos.

Ao **Thiago Sombra**, com quem tive a oportunidade e a alegria de trabalhar por dois anos, e que foi a primeira pessoa a acreditar no meu potencial para a proteção de dados e a tecnologia como profissional. Estendo os agradecimentos aos colegas que me acompanharam nessa jornada, **Ingrid**, **Giovanna**, **Isabella**, **Luiza** e **Gustavo**, que foram minha companhia e apoio durante esses dois anos e que tanto me ensinaram.

Aos meus amigos e companheiros do coração **Evelly**, **Tainá**, **Wanessa**, **Dito**, **Luís**, **Luisa**, **Vit** e **Camila** que estão comigo desde a Ciência Política e que me deram todo o apoio possível para que pudesse concluir este trabalho.

À minha avó, **Dona Raimunda**, que é um exemplo de força e coragem e que sempre sonhou em também um dia usar o capelo, mas nunca teve a oportunidade. Querida avó, a senhora foi a primeira a me dizer que tinha a certeza de que eu venceria. É uma honra ser a neta de uma mulher tão corajosa e forte.

À minha mãe, **Ildelene**, que é o maior exemplo de amor e coragem e que foi o abraço quentinho que eu procurei quando achei que não ia ter forças para continuar. À minha irmã, **Beatriz**, que é companheira de vida, nos bons e nos maus momentos. E ao meu primo, **Lucas**, que não poupou esforços para me guiar quando precisei.

Por fim, agradeço a todos os colegas e professores que de alguma forma fizeram parte dessa jornada. A caminhada não foi fácil, mas as memórias que ficaram são muito preciosas.

Um dos meus filmes favoritos na infância, Spirit, dizia algo similar ao texto de Bob-Waksberg: “Quem perdido está, se encontra na coragem. Tenha fé em ti, não esqueça quem tu és”. Eu decidi ter coragem. E aqui estamos.

RESUMO

Tendo em vista a crescente utilização de tecnologias informatizadas na sociedade houve um aumento significativo de incidentes de segurança da informação envolvendo dados pessoais com potencial danoso aos titulares de dados. As instituições financeiras parecem ser um alvo particularmente preocupante sob o ponto de vista do titular em razão da importância que esses dados possuem e o potencial do dano que podem causar. Ainda assim, há poucos estudos sobre como esses pleitos estão sendo analisados no judiciário brasileiro. O presente trabalho analisa as decisões proferidas pelos Tribunais de Justiça relacionadas à litígios em que haja indicativos ou alegações de que tenha havido um incidente de segurança envolvendo dados pessoais em instituições financeiras, de pagamento ou autorizadas a funcionar pelo Banco Central do Brasil (BACEN). Os achados demonstram que, apesar de tímidos avanços, os Tribunais ainda estão longe de alcançar o nível de sofisticação necessário para a análise dessas lides.

Palavras-chave: Proteção de dados; dados pessoais; incidentes de segurança; vazamento de dados; segurança da informação; instituições financeiras.

ABSTRACT

Given the increasing use of information technology in society, there has been a significant increase in information security incidents involving personal data with potential harm to data subjects. Financial institutions seem to be a particularly worrisome target from the data subject's point of view because of the importance of this data and the potential damage it can cause. Still, there are few studies on how these claims are being analyzed in the Brazilian judiciary. This paper analyzes the decisions handed down by the Courts of Justice related to litigation in which there are indications or allegations that there has been a security incident involving personal data in financial institutions, payment institutions or those authorized to operate by the Central Bank of Brazil (BACEN). The findings show that, despite timid advances, the Courts are still far from reaching the level of sophistication necessary for the analysis of these disputes.

Key words: data protection; personal data; security incidentes; data breaches; information security; financial institutions.

LISTA DE ABREVIATURAS

ANBIMA: Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais

ANPD: Autoridade Nacional de Proteção de Dados

ARPA: U.S. Department of Advanced Research Projects Agency

ARPANET: Forma de Rede (Internet) criada pelo U.S. Department of Advanced Research Projects Agency

BACEN: Banco Central do Brasil

CDC: Código de Defesa do Consumidor

GDPR: *General Data Protection Regulation* (Regulamento Europeu de Proteção de Dados)

LGPD: Lei Geral de Proteção de Dados

MCI: Marco Civil da Internet

RIPD: Relatório de Impacto à Proteção dos Dados Pessoais

RM: *Risk Management* (Gestão de Risco)

LISTA DE FIGURAS

LISTA DE GRÁFICOS

SUMÁRIO

INTRODUÇÃO

A crescente utilização de tecnologias informatizadas na sociedade resulta da facilidade que essas tecnologias agregam ao dia a dia de cidadãos e organizações. No entanto, afirmam Catteli e Idie[1] que, se por um lado, a utilização dessas tecnologias é bem-vinda, a fragilidade decorrente da insuficiência da educação digital e da falta de cultura em segurança cibernética no Brasil causa extrema preocupação.

Segundo o levantamento da Fortinet[2], empresa de soluções em cibersegurança, houve cerca de 360 bilhões de tentativas de ataques cibernéticos aos sistemas de empresas e organizações na América Latina e Caribe em 2022, com base nos dados do FortiGuard Labs. Segundo o documento, no *ranking* da América Latina e Caribe, o Brasil é o segundo com mais registros de ataques cibernéticos, com 103,1 bilhões de tentativas, um aumento de 16% em relação ao que foi registrado em 2021. No México, país que lidera o ranking, foram 187 bilhões de tentativas em 2022.

Em âmbito nacional, destacam-se as estatísticas divulgadas pelo CERT.br[3], Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, apenas em 2022, foram 481.652 (quatrocentos e oitenta e uma mil seiscentos e cinquenta e duas) notificações de incidentes de segurança da informação recebidas pelo órgão, tendo o parâmetro sido mantido em relação aos anos anteriores: 457.270 em 2021 e 531.039 em 2020.

Se considerados esses dados, vê-se que a afirmação de Solov e Hartzog[4] em "*Breached*!" é verdadeira, os eventos de segurança da informação são uma morte anunciada. Para os autores, incidentes de segurança não estão só mais numerosos, estão cada vez mais danosos. Além disso, os autores destacam que foram identificadas diversas

---

[1] CATTELLI, Maria Augusta Peres; IDIE, Renata Yumi. Prevenir para mitigar: a importância do desenvolvimento de cultura de segurança cibernética nas organizações. In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020

[2] FORTINET. Fortinet relata que a América Latina foi alvo de mais de 360 bilhões de tentativas de ataques cibernéticos em 2022. Disponível em: https://www.fortinet.com/br/corporate/about-us/newsroom/press-releases/2023/fortiguard-labs-reports-destructive-wiper-malware-increases-over-50-percent. Último acesso em 2 de julho de 2023.

[3] O Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de Responsabilidade Nacional de último recurso, mantido pelo NIC.br. O NIC.br é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil e implementa as decisões e os projetos do CGI.br, que é responsável por coordenar e integrar as iniciativas e serviços da Internet no país.

[4] SOLOV, Daniel J; HARTZOG, Woodrow. BREACHED!: Why data security law fails and how to improve it. Nova Iorque: Oxford University Press, 2022.

violações de dados e a moral da maioria dessas histórias resume-se à mesma coisa: as violações podiam ser evitadas, mas as pessoas cometeram erros. O que é notável nesses casos é a timidez da evolução ao longo do tempo. Aparentemente, erros já conhecidos e amplamente divulgados continuam a repetir-se. Sendo assim, os autores questionam que, após tantos anos e tantas leis para regulamentar a segurança dos dados, por que é que essas histórias resistem em mudar?

De acordo com os autores Nakamura e Geus "a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida"[5]

Com a entrada em vigor da Lei Geral de Proteção de Dados ("LGPD") a proteção dos dados pessoais[6] também se tornou normativamente regulada. Ainda que a segurança da informação abarque um espectro ainda mais amplo do que a proteção dos dados pessoais, ambos os conceitos estão intrinsecamente ligados, já que o dado pessoal é também um ativo informacional a ser protegido, *lato sensu*.

A partir da proteção legal dos dados pessoais, foi introduzido no arcabouço normativo brasileiro o conceito de incidente de segurança envolvendo dados pessoais. Trata-se, portanto, de um incidente de segurança, ou seja, uma quebra de algum dos princípios da segurança da informação, quais sejam, confidencialidade, disponibilidade e/ou integridade, quando estiverem envolvidos dados pessoais, nos termos da definição legal e da regulamentação.

Sendo assim, passou a ser legalmente exigível que os dados pessoais, especificamente, fossem protegidos de uma situação que pudesse configurar um incidente de segurança.

Ainda assim, não são raros os casos em que dados pessoais sofrem algum tipo de incidente de segurança. Desses, os incidentes envolvendo instituições financeiras parecem ser os mais notados por titulares de dados, em razão da importância que as informações detidas por essas organizações possuem para o titular de dados a nível individual, inclusive os dados pessoais.

---

[5] NAKAMURA, Emílio; GEUS, Paulo. Segurança de redes em ambientes corporativos. São Paulo: Berkeley Brasil, 2002, p. 9.

[6] "Art. 5º Para os fins desta Lei, considera-se: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável". BRASIL. Lei Federal n.º 13709 de 14 de agosto de 2018 (Lei Geral de Proteção de Dados). 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Nesse sentido, este trabalho pretende analisar o arcabouço normativo que envolve a proteção das informações, inclusive as pessoais sob a ótica da segurança dos dados e da prevenção a incidentes de segurança.

O recorte do trabalho são as decisões do judiciário em sede de segunda instância que tratam de eventos considerados pelos autores das ações como incidentes de segurança que envolveram seus dados pessoais em que a parte ré é uma instituição financeira. Para tanto, serão tecidas considerações sobre a anatomia dos incidentes de segurança, as normas e literatura relacionadas a esses eventos e possíveis correlações dessas definições com os eventos encontrados. No entanto, o objetivo do trabalho não é investigar a ocorrência ou não de um incidente de segurança, mas a evolução das decisões do judiciário sobre esses eventos ao longo da vigência da LGPD.

Portanto, o estudo aqui realizado pretende investigar a evolução do processo decisório envolvendo os litígios em que há a alegação da ocorrência de um incidente de segurança envolvendo dados pessoais que teriam ocorrido em instituições financeiras ou aquelas autorizadas a funcionar pelo Banco Central do Brasil ("BACEN").

Os objetivos do presente trabalho são: (i) entender e reunir os requisitos de segurança esperados das instituições financeiras de acordo com as regulamentações existentes, em especial, no âmbito setorial; (ii) entender os requisitos de segurança esperados de controladores de dados pessoais conforme a LGPD e suas implicações nas medidas esperadas de um Controlador em termos de segurança; (iii) verificar se ocorreu a incorporação e, se sim, de que maneira o judiciário incorporou os princípios e requisitos da LGPD e aplicou os conceitos relacionados à Segurança dos Dados Pessoais como parte da fundamentação para a decisão de lides relacionadas à incidentes de segurança envolvendo instituições financeiras.

O trabalho será subdividido em três capítulos. No primeiro capítulo, será explorada a origem da Segurança da Informação e de seus princípios, de forma a conceituar os três pilares principais da segurança da unformação de acordo com os textos clássicos utilizados no meio da segurança da informação e definições trazidas ou expressadas pela literatura. A partir então, o foco principal será a análise de como esses princípios eram utilizados pela regulamentação de cibersegurança voltada para instituições financeiras e de pagamento reguladas pelo BACEN a fim de fornecer um panorama do cenário de regulamentação de segurança da informação, conforme entendimento do BACEN.

Vale ressaltar que, em que pese os tribunais não tenham a obrigação de observar ou realizar o *enforcement* das normas do BACEN, as orientações sobre cibersegurança do órgão regulador oferecem um panorama institucional do que é esperado em termos de segurança da informação por parte das instituições financeiras e instituições autorizadas a funcionar pelo BACEN.

No segundo capítulo, serão analisadas a disposições pertinentes à segurança dos dados pessoais no âmbito da legislação de proteção de dados (notadamente, a LGPD) Nessa etapa, serão analisados, preliminarmente, os princípios: (i) do livre acesso e da qualidade de dados; (ii) da segurança e (iii) da prevenção. Em um segundo momento, serão analisados os artigos que se referem à segurança dos dados pessoais, para além dos princípios, quando se trata de incidentes de segurança e sua prevenção e gerenciamento. Além disso, serão tecidas breves considerações sobre a responsabilidade dos agentes de tratamento sobre incidentes de segurança ocorridos.

Nesse capítulo, o objetivo é demonstrar que existem, desde a vigência da LGPD, normas robustas, ainda que sem contornos precisos definidos, que exigem um determinado parâmetro de segurança das instituições financeiras e de outros tipos de organizações.

No terceiro capítulo serão analisadas as decisões envolvendo pedidos de titulares relacionados a incidentes de segurança envolvendo instituições financeiras. Aqui serão analisadas tanto incidentes confirmados quanto não confirmados, feitas as devidas considerações sobre a aplicabilidade da LGPD nos casos não confirmados, sendo o critério de inclusão na seleção de decisões apenas a argumentação do titular de dados de infringência da LGPD (acesso ilícito ou não autorizado, fraude e etc.)

Nesse sentido, serão tecidos breves comentários em relação à existência ou não de incidente de segurança, entretanto, o objetivo do capítulo é analisar a consideração, pelos tribunais, dos requisitos de Segurança esperados das instituições e seu impacto (ou ausência de impacto) nas decisões de mérito[7]. Serão comparados os resultados encontrados no período de janeiro de 2021 a setembro de 2022, conforme seleção de julgados e metodologia detalhada no corpo do trabalho. O objetivo desse capítulo é responder ao questionamento do trabalho: se os tribunais têm considerado esses

[7] "Impacto", neste ponto, refere-se à fundamentação de fato contribuir ou não para a decisão de mérito (em geral, os casos analisados pleiteiam danos morais e materiais). O objetivo não é definir, no entanto, se a LGPD deve ensejar resultado de deferimento ou indeferimento do pedido pleiteado.

princípios e requisitos no processo decisório, ainda que decidam por afastar a aplicação deles.

CAPÍTULO 1 | Os conceitos de Segurança da Informação presentes no arcabouço regulatório das instituições Financeiras e das instituições autorizadas a funcionar pelo BACEN

1.1. Origem da Segurança da Informação

A história da segurança da informação como disciplina se inicia com o conceito de segurança computacional ("*computer security*", em inglês). A necessidade por *computer security* começou durante a Segunda Guerra Mundial, quando os primeiros computadores *mainframe*[8] foram desenvolvidos para auxiliar as comunicações e decodificar mensagens dos dispositivos criptografados dos inimigos. Para manter a segurança desses computadores e a vantagem informacional na guerra, novos mecanismos de segurança, mais complexos e sofisticados tecnicamente, foram desenvolvidos[9].

Durante esses primeiros anos, a segurança da informação era composta predominantemente de segurança física e estruturas simples de classificação de documentos, haja vista que as principais ameaças consistiam em roubo dos equipamentos físicos, espionagem e sabotagem. Uma das primeiras instâncias em que um incidente foi documentado e classificado fora dessas hipóteses ocorreu nos anos 1960, quando um administrador externo foi identificado alterando o arquivo de senhas[10].

Em 1968 o Doutor Larry Roberts desenvolveu o Projeto ARPANET, que seria o precursor da Internet. Esse projeto derivava do programa governamental estadunidense do *U.S. Department of Advanced Research Projects Agency* ("ARPA") que iniciou a

[8] Um *mainframe* é um tipo de computador de grande porte, projetado para processar grandes volumes de dados e executar tarefas críticas para organizações complexas, como empresas, instituições financeiras, governos e outras entidades que exigem processamento de dados em grande escala. Os mainframes são conhecidos por sua confiabilidade, escalabilidade e segurança robusta.
Essas máquinas são capazes de executar várias tarefas simultaneamente e oferecem suporte a milhares de usuários simultâneos. Eles são altamente confiáveis devido a redundâncias internas, como fontes de alimentação e unidades de armazenamento duplicadas, além de mecanismos de recuperação de falhas. Os mainframes são projetados para lidar com cargas de trabalho de processamento intensivo, manipulando transações de dados em grande escala e executando aplicativos críticos de missão.
IBM Systems Magazine. Mainframe Edition. Disponível em : https://www.ibmsystemsmag.com/mainframe/

[9] WHITMAN, Michael E ; MATTORD, Herbert J. *Principles of Information Security*. Editora Cengage. 7ª Ed. Boston USA, 2022. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Hwk1EAAAQBAJ&oi=fnd&pg=PP1&dq=the+origin+of+information+security%22&ots=VirNfOfYMk&sig=eP_5xUio9nT1R7rDQImFd4KA1M0&redir_esc=y#v=onepage&q=the%20origin%20of%20information%20security%22&f=false

[10] *Ibidem*

pesquisa sobre a viabilidade de uma comunicação em sistemas de rede para dar suporte a troca de informação no exército estadunidense.

Na próxima década, em 1973, o cientista Robert M. Metcalle identificou um problema fundamental com os sistemas ARPANET, resultado da pesquisa do ARPA, em meio à sua crescente utilização. Como um dos criadores da Ethernet, ele sabia que sites remotos individuais não tinham controles e salvaguardas suficientes para proteger os dados de acessos não autorizados. Outros problemas também poderiam ser identificados como: a vulnerabilidade da estrutura de senhas, a falta de procedimentos de segurança para conexões discadas, a inexistência de identificação de usuários e de autorizações[11].

Na metade dos anos 1980, o governo estadunidense aprovou uma série de legislações que reconheciam a segurança de computadores como um problema crítico para sistemas informacionais federais. Como exemplo, o *Computer Fraud and Abuse Act* de 1986 e o *Computer Security Act* de 1987 definiram a segurança computacional e especificaram as responsabilidade e penalidades associadas as infrações contempladas por esses diplomas legais[12].

No século XX, redes de computadores se tornaram mais comuns, bem como a necessidade de conectá-los uns aos outros. Com isso, surgiu a Internet, a primeira rede global. A Internet se tornou disponível ao público nos anos 90, após décadas de domínio pelo governo, academia e profissionais da indústria de computadores[13].

A Internet trouxe conectividade para virtualmente todos os computadores que possuíam acesso a uma linha telefônica ou a uma *local area network* (LAN) conectada à Internet. Como os computadores em rede se tornaram a norma, a habilidade de promover segurança física desses dispositivos foi perdida e a informação passou a estar exposta a ameaças de segurança[14].

No final dos anos 90 e início dos 2000, muitas empresas de grande porte começaram a integrar segurança nas suas organizações. Produtos denominados "*Antivirus*" se tornaram extremamente populares, e a segurança da informação passou a surgir como uma disciplina independente[15].

Essa história demonstra que o conceito de segurança das informações e, mais tarde, de segurança da informação como disciplina, nasce muito antes dos primeiros

[11] *Ibidem*
[12] *Ibidem*
[13] *Ibidem*
[14] *Ibidem*
[15] *Ibidem*

normativos relacionados a proteção dos dados pessoais, especificamente. Esse conceito já nasce com uma importância significativa, já que desde o princípio visava proteger informações que eram cruciais para a atividade que as utilizava.

Sendo assim, "segurança", segundo Whitman e Mattord[16], é proteção. Essa proteção tem como objetivo impedir que agentes possam causar dano, intencionalmente ou não. O *Commitee on National Security Systems* (CNSS), órgão estadunidense de Segurança, define a segurança da informação como a proteção de informação e seus elementos críticos, incluindo os sistemas e *hardware* que usam, armazenam e transmitem informação[17].

O modelo de segurança da informação do CNSS evoluiu de um conceito desenvolvido pela indústria da segurança da informação chamado *C.I.A triad* ou, em português, "tríade C.I.D" (Figura 1.1). Esse conceito tem sido o padrão para a segurança tanto na indústria quanto no governo estadunidense desde o desenvolvimento do *mainframe.*

Esse padrão está apoiado nas três características da informação que dão a ela seu valor dentro de uma organização: confidencialidade (em inglês, *confidentiality*), integridade (em inglês, *integrity*) e disponibilidade (em inglês, *availability*), portanto, C.I.D.

Figura1.1.

C.I.A Triad (Tríade C.I.D)

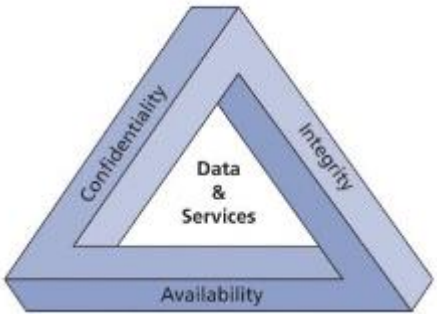


Figura 1.1: Fundamentals of Information Security (WHITMAN; MATTORD, 2022)

[16] WHITMAN, Michael E ; MATTORD, Herbert J. *Principles of Information Security*. Editora Cengage. 7ª Ed. Boston USA, 2022. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Hwk1EAAAQBAJ&oi=fnd&pg=PP1&dq=the+origin+of+information+security%22&ots=VirNfOfYMk&sig=eP_5xUio9nT1R7rDQImFd4KA1M0&redir_esc=y#v=onepage&q=the%20origin%20of%20information%20security%22&f=false. p. 8

[17] *Ibidem*

A Figura 1.2. abaixo demonstra que a segurança da informação inclui outras áreas relacionadas ao gerenciamento da segurança informação (*information security management*), à segurança de dados (*data security*) e à segurança de rede (*network security*).

Figura 1.2

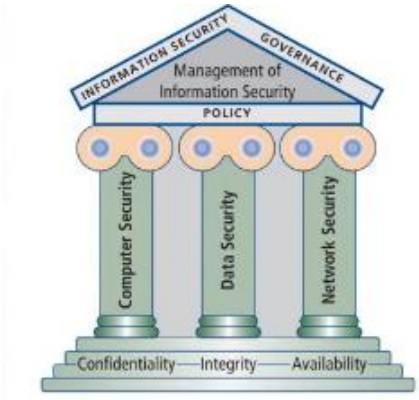


Figura 1.2 : Fundamentals of Information Security (WHITMAN; MATTORD, 2022)

Esses pilares permanecem como princípios da segurança da informação até os dias atuais e orientam a maioria das normas, sejam elas legais, regulatórias ou boas práticas de mercado, relacionadas à segurança da informação para organizações que usam, armazenam ou transmitem esses ativos.

É importante destacar que a segurança da informação abarca a proteção e segurança dos dados pessoais, haja vista que esses são também ativos informacionais. No entanto, os dados pessoais não são as únicas informações protegidas pela disciplina da segurança da informação.

A segurança da informação é uma disciplina mais ampla que abarca os mais diversos níveis de criticidade das informações que não são necessariamente pessoais. Informações sobre modelo de negócio ou abarcadas pelo segredo industrial, informações estratégicas, *know how* e informações referentes às pessoas jurídicas, para citar alguns exemplos, também são abarcadas pela segurança da informação, desde que precisem estar protegidas e garantidas pelos pilares da C.I.D.

1.2. Os princípios da Segurança da Informação

De acordo com Peltier[18], “a segurança da informação compreende o uso de controles de acesso físicos e lógicos, com o intuito de proteger os dados contra modificações acidentais ou não autorizadas, destruição, quebra de sigilo, perda ou dano aos ativos informacionais”.

Para Sêmola, “a segurança da informação é uma área de conhecimento voltada à proteção da informação e dos ativos associados contra indisponibilidade, alterações indevidas e acessos não autorizados”[19]. O autor entende que a segurança da informação deve ser tratada de forma mais ampla, por meio de práticas de gestão de riscos e incidentes que impliquem o comprometimento da confidencialidade, da integridade e da disponibilidade das informações.

Como bem explicado por Whitman e Mattord[20], é a confidencialidade, disponibilidade e integridade das informações que as fazem importantes, por isso, são esses os principais princípios que norteiam os programas de conformidade desde 1970 até os dias atuais.

Mascarenhas Neto e Araújo lecionam que, sob uma perspectiva mais recente, o fator humano passou a ser preponderante para o alcance dos objetivos da segurança da informação[21].

É nesse contexto que Marciano[22] propôs uma definição social em que:

> “a segurança da informação é um fenômeno social no qual os usuários dos recursos informacionais têm razoável conhecimento sobre o uso desses recursos, incluindo os ônus decorrentes, bem como sobre os papéis que devem desempenhar no exercício desse uso”.

[18] PELTIER, T. R. *Information security policies, procedures, and standards: Establishing an Essential Code of Conduct*. USA: Aurebach Publications, 2001, p.8.
[19] SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva.* 2 ed. Rio de Janeiro: Elsevier, 2014.p.41
[20] WHITMAN, Michael E ; MATTORD, Herbert J. *Principles of Information Security*. Editora Cengage. 7ª Ed. Boston USA, 2022. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Hwk1EAAAQBAJ&oi=fnd&pg=PP1&dq=the+origin+of+information+security%22&ots=VirNfOfYMk&sig=eP_5xUio9nT1R7rDQImFd4KA1M0&redir_esc=y#v=onepage&q=the%20origin%20of%20information%20security%22&f=false.
[21] MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. *Segurança da informação: uma visão sistêmica para implantação em organizações.* João Pessoa: Editora da UFPB, 2019.
[22] MARCIANO, João Luiz Pereira. Segurança da informação: uma abordagem social. Tese de Doutorado em Ciência da Informação – Universidade de Brasília, 2006. p.114.

Sobre a origem das falhas em segurança, Mitnick e Simon[23] afirmam que o fator humano é a maior causa de incidentes de segurança da informação. Alexandria[24] partilha da mesma opinião, ao alertar que é um erro comum não considerar os aspectos sociais e humanos envolvidos na construção da segurança da informação.

É na tentativa de prevenir danos causados pelas falhas de segurança que foram elaborados os princípios que norteiam a segurança da informação, disponibilidade, confidencialidade e integridade. Sendo assim, a fim de preservar aquilo que torna a informação um ativo relevante sob o aspecto tanto social como comercial, organizações devem adotar medidas que garantam o cumprimento desses princípios.

Nos próximos itens desse tópico serão abordadas algumas definições para esses princípios.

1.2.1. Princípio da disponibilidade

Segundo Sêmola[25], o princípio da disponibilidade consiste em garantir que toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível para seus usuários, quando eles necessitam delas para qualquer finalidade.

A disponibilidade então, segundo Mascarenhas Neto e Araújo[26], consiste na disponibilidade permanente para os usuários quando essa informação ou dado seja necessária. Como exemplo, os autores descrevem uma organização que deixa de atualizar sua tabela de preços de venda de produtos devido a um erro de sincronização das bases de dados dos sistemas de venda de suas várias filiais. Depois de um longo período, percebe-se que alguns milhares de produtos foram vendidos a um preço inferior, pois os dados não estavam disponíveis quando necessário.

---

[23] MITNICK, Kevin, D.; SIMON, Willian L. Mitnick. *A arte de enganar: ataques de hackers: controlando o fator humano na segurança da informação.* São Paulo: Makron Books, 2003.
[24] ALEXANDRIA, João C. S de. *Gestão de Segurança da Informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica.* São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.
[25] SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva.* 2 ed. Rio de Janeiro: Elsevier, 2014.
[26] MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. *Segurança da informação: uma visão sistêmica para implantação em organizações.* João Pessoa: Editora da UFPB, 2019.

Já segundo Carvalho[27], segundo a análise das informações disponíveis no DAMABOK[28], disponibilidade refere-se ao grau de conhecimento e acessibilidade de dados e metadados, no momento necessário, para quem tem o devido acesso. Portanto, esse pilar envolveria conceitos tanto de governança de dados quanto de segurança da informação.

Por sua vez, Fernandes[29] afirma que um sistema de informação dota de disponibilidade quando os usuários autorizados conseguem acessar livremente os dados desejados. Para obter a disponibilidade, o autor afirma que os gestores de tecnologia precisam garantir um sistema totalmente operacional seja mantido íntegro.

Por fim, ressalta-se a definição trazida pelos autores Jimene e Sicuto[30] que definem a disponibilidade consiste na disponibilidade da informação para a execução dos trabalhos.

Nesse sentido, a disponibilidade pode ser resumida a partir dessas definições como a disponibilidade, no sentido de acesso possível aos dados e metadados, quando esses forem necessários, pelos sujeitos autorizados para a execução das funções e finalidades que esses dados possuem.

1.2.2. Princípio da integridade

Quando se trata do princípio da integridade, Sêmola[31] afirma que a informação deve ter a garantia de que será mantida na condição em que foi disponibilizada por seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.

---

[27] CARVALHO, A. P. (2021). *Proposta de um Framework de Compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): Um estudo de caso para prevenção a fraude no contexto de Big Data*. Dissertação de Mestrado Profissional, Publicação: PPEE.MP.012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 200 p.

[28] BRACKETT, M., AND EARLEY, P. S. The DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Estados Unidos: Technics Publications (2009).

[29] FERNANDES, Rodrigo Moura. *Resiliência e Governança Digital*. In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. *Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética.* 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p.270

[30] JIMENE, Camilla do Vale; SICUTO, Guilherme Hernandes. Segurança da informação sob a perspectiva da legislação brasileira: aspectos convergentes. In MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. *Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética.* 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 43

[31] SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva*. 2 ed. Rio de Janeiro: Elsevier, 2014.

Mascarenhas Neto e Araújo[32] explicam que o objetivo desse pilar é garantir que a informação não seja alterada, de forma que se busque a fidedignidade das informações. Destacam, ainda, que essa garantia perpassa a violação intencional e acidental.

Já Carvalho[33], resumidamente, descreve a integridade como o "grau de conformidade com todas as restrições de integridade definidas no metadado, necessárias para que o dado possa ser confiável. Dessa forma, esse princípio permite a representação das regras de negócio, sem as quais há prejuízo à confiabilidade".

Fernandes[34] afirma que a integridade se refere à consistência conferida às redes, sistemas e dados. Para ele, a integridade de uma rede de computadores ou dos dados ali armazenados é mantida, impede-se que alterações não autorizadas ou não intencionais sejam executadas e assegurando que o sistema se comporte como deveria quando acessados por um usuário autorizado.

Por fim, Jimene e Sicuto[35] definem que a integridade da informação é um princípio que está calcado na ideia de que a informação deve ser confiável, pois possui a garantia de não ter sofrido alterações.

Sendo assim, esse trabalho resume esse princípio como sendo a garantia de que os dados e metadados[36], sejam mantidos da forma que foram disponibilizados, livres de alterações acidentais ou intencionais, quando acessados pelos indivíduos autorizados e de forma que sejam confiáveis.

---

[32] MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. *Segurança da informação: uma visão sistêmica para implantação em organizações.* João Pessoa: Editora da UFPB, 2019. p. 29

[33] CARVALHO, A. P. (2021). *Proposta de um Framework de Compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): Um estudo de caso para prevenção a fraude no contexto de Big Data.* Dissertação de Mestrado Profissional, Publicação: PPEE.MP.012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 200 p.

[34] FERNANDES, Rodrigo Moura. *Resiliência e Governança Digital*. In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. *Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética.* 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 270.

[35] JIMENE, Camilla do Vale; SICUTO, Guilherme Hernandes. Segurança da informação sob a perspectiva da legislação brasileira: aspectos convergentes. In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. *Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética.* 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 43.

[36] "Metadados são dados que fornecem informações sobre outros dados.
Em outras palavras, eles são informações adicionais que descrevem os dados que estão sendo armazenados ou transmitidos. Por exemplo, se você tiver uma foto, os metadados podem incluir informações sobre a câmera utilizada para tirar a foto, a data e a hora em que foi tirada, a localização geográfica e outros detalhes relevantes. Se você tiver um arquivo de música, os metadados podem incluir informações sobre o artista, o álbum e a faixa.
Os metadados são usados em várias áreas, incluindo bibliotecas, arquivos, museus, base (bancos) de dados e sistemas de gerenciamento de informações. Eles são particularmente importantes em áreas como preservação digital e gestão de informações científicas, onde a precisão e a integridade dos dados são essenciais. Os metadados ajudam a garantir que os dados possam ser facilmente localizados, compartilhados e usados de maneira eficiente e precisa" METADADOS. *O que são metadados*?. Disponível em: https://www.metadados.pt/oquesaometadados/. Último acesso em: 10 de julho de 2023.

1.2.3. Princípio da confidencialidade

Sêmola[37] define que o princípio da confidencialidade consiste no fato de que toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando limitar seu acesso e uso às pessoas a quem é destinada.

Mascarenhas Neto e Araújo[38] explicam que a confidencialidade garante que só os destinatários da informação tenham acesso a ela. Isso significa que manter a confidencialidade das informações é ter a segurança de que o que foi dito ou escrito será transmitido ou cedido apenas a quem tem direito. Ressaltam que a violação desse requisito poderá trazer impactos imensuráveis para a organização.

Fernandes[39] afirma que a confidencialidade se refere a manter as informações consideradas confidenciais em sigilo. O autor fornece como exemplo o fato de que informações de crédito, dados bancários ou as informações pessoais dos clientes são, por exemplo alguns dados que precisam ser protegidos de acesso não autorizado. Neste trabalho, entendemos que a confidencialidade não se restringe a informações confidenciais apenas, mas a toda informação que deve ser mantida inacessível a pessoas não autorizadas. Por esse motivo entendemos que essa definição acaba incorrendo em um erro comum, especialmente quando se trata de proteção de dados não sensíveis.

Já Jimene e Sicuto[40] definem esse princípio resumidamente como "a premissa de que a informação precisa ser conhecida somente por quem precise conhecê-la para exercer suas atividades profissionais, baseada no princípio do *need to know*.

Sendo assim, este trabalho define a confidencialidade como a manutenção de dados inacessíveis aos sujeitos que não possuem autorização para acessá-los, mantendo informações restritas a seu nível de acesso.

---

[37]SÊMOLA, Marcos. *Gestão da segurança da informação: uma visão executiva.* 2 ed. Rio de Janeiro: Elsevier, 2014.

[38] MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: Editora da UFPB, 2019. p. 28

[39] FERNANDES, Rodrigo Moura. Resiliência e Governança Digital. In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. *Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética.* 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 269

[40] JIMENE, Camilla do Vale; SICUTO, Guilherme Hernandes. *Segurança da informação sob a perspectiva da legislação brasileira: aspectos convergentes.* In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 43

Sobre o tema nível de acesso, importante mencionar que ainda que informações não sejam sigilosas, quando se trata de dados pessoais, caso essas informações não devam ser acessadas por meio do detentor delas (seja ele controlador[41] ou operador[42]), elas devem ser consideradas confidenciais em relação a terceiros.

Sendo assim, são úteis as considerações trazidas por Mascarenhas Neto e Araújo[43] sobre níveis de classificação de informações. Os autores afirmam que, fundamentalmente, a classificação das informações em uma organização deve ser conduzida sob dois aspectos distintos e cruciais: (i) importância para o negócio e (ii) sua proteção durante seu ciclo de vida.

Para definir os níveis as classes de informação de acordo com a sua importância para a organização os autores adotam a classificação de Amaral (1994)[44]:

> "**A informação crítica** – essencial à sobrevivência da organização;
>
> •**A informação mínima** – essencial para uma boa gestão da organização;
>
> • **A informação potencial** – essencial para a obtenção de vantagens competitivas utilizando-se os sistemas de informação;
>
> • **A informação lixo** – desprovida de qualquer valor."[45] (grifo nosso)

[41] "O controlador é o agente responsável por tomar as principais decisões referentes ao tratamento de dados pessoais e por definir a finalidade deste tratamento. Entre essas decisões, incluem-se as instruções fornecidas a operadores contratados para a realização de um determinado tratamento de dados pessoais" ANPD. Guia orientativo de agentes de tratamento e encarregado. Abril, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Último acesso em: 15 de junho de 2023.

[42] "O operador é o agente responsável por realizar o tratamento de dados em nome do controlador e conforme a finalidade por este delimitada. A definição legal se encontra no art. 5º, inciso VII da LGPD. [...] A previsão acima implica dizer que o operador só poderá tratar os dados para a finalidade previamente estabelecida pelo controlador. Isso demonstra a principal diferença entre o controlador e operador, qual seja, o poder de decisão: o operador só pode agir no limite das finalidades determinadas pelo controlador." ANPD. Guia orientativo de agentes de tratamento e encarregado. Abril, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia_agentes_de_tratamento_e_encarregado___defeso_eleitoral.pdf. Último acesso em: 15 de junho de 2023.

[43] MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. *Segurança da informação: uma visão sistêmica para implantação em organizações.* João Pessoa: Editora UFPB, 2019.

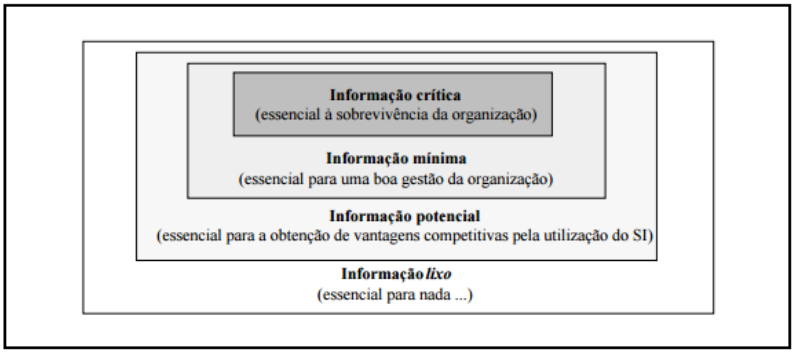
[44] AMARAL, L. A. M. *PRAXIS: um referencial para o planejamento de sistemas de informação.* Tese de Doutorado apresentada na Universidade do Minho, Portugal, 1994.

[45] AMARAL, L. A. M. *PRAXIS: um referencial para o planejamento de sistemas de informação.* Tese de Doutorado apresentada na Universidade do Minho, Portugal, 1994.

Amaral ainda fornece um organograma visual dessas classificações como se pode verificar a seguir:

Figura 1.3.

Classificação de Informações



Fonte: AMARAL, L. A. M. PRAXIS: um referencial para o planejamento de sistemas de informação. Tese de Doutorado apresentada na Universidade do Minho, Portugal, 1994

1.3. Análise dos princípios na regulamentação setorial financeira pré-LGPD: Resolução BACEN 4658/2018 e Circular BACEN n.º 3.909/2018

Tratando-se de instituições financeiras e instituições autorizadas a funcionar pelo Banco Central do Brasil ("BACEN"), existem requisitos específicos de Segurança Cibernética e, por consequência de Segurança da Informação.

Em grande medida, as normas específicas do setor estabelecem requisitos similares aos exigidos por normas internacionais de padrões de segurança como a ISO 27001 e 27002. No entanto, as normas regulatórias são, ou deveriam ser, passíveis de *enforcement* pelo órgão regulador que seria o próprio BACEN.

Nesse sentido, este item explorará os requisitos exigidos das instituições financeiras, instituições de pagamento e instituições autorizadas a funcionar pelo BACEN, conforme as normas emitidas pelo órgão.

Para tanto, em uma primeira análise, serão abordadas as normas vigentes no momento imediatamente anterior à vigência da LGPD e as normas publicadas posteriormente.

A Resolução CMN n.º 4,658 de 26 de abril de 2018[46] e a Circular BACEN n.º 3,909 de 16 de agosto de 2018[47], atualmente revogadas, dispunham sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas (i) instituições financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.; e (ii) instituições de pagamento, respectivamente. Naquilo que compreende o escopo deste trabalho, ambas as resoluções estabelecem os mesmos requisitos, portanto, serão analisadas em conjunto.

A Resolução e a Circular estabelecem diversos requisitos técnicos e organizacionais a serem implementados pelas instituições sujeitas ao escopo de aplicação da norma, em relação a (i) Política de Segurança Cibernética e (ii) Contratação de Serviços de Nuvem, respectivamente nos Capítulos I e II das normas.

Em ambos os capítulos são estabelecidos os requisitos mínimos a serem cumpridos pelas instituições dentro do escopo da norma que são, segundo o entendimento do BACEN, o padrão base de segurança dos dados em posse dessas instituições.

Para o escopo deste trabalho, será analisado o Capítulo I da norma, visto que as decisões analisadas no Capítulo III deste trabalho se referem apenas a instituições financeiras, não sendo abarcadas as prestadoras de serviço de computação em nuvem neste escopo.

No Art. 2º das normas, estabelece-se que as instituições referidas no *caput* do art. 1º devem implementar e manter uma política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Neste artigo percebe-se que o escopo principal da norma é garantir que os pilares da Segurança da Informação sejam cumpridos. Ademais, percebe-se que, nesta norma, foram incorporados os três pilares analisados neste trabalho, sendo excluídos outros possíveis princípios elaborados por outras vertentes da Segurança da Informação.

---

[46] BRASIL. Resolução CMN n.º 4,658 de 26 de abril de 2018. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o&numero=4658

[47] BRASIL. Circular BACEN n.º 3,909 de 16 de agosto de 2018. Disponível em: https://normativos.bcb.gov.br/Lists/Normativos/Attachments/50645/Circ_3909_v3_P.pdf

No §1º desse mesmo artigo, o BACEN estipula o nível de complexidade que a Política de Segurança Cibernética deve obedecer tendo em vista as características particulares de cada uma das instituições, sendo relevantes para tanto: (i) o porte, perfil de risco e modelo de negócios da instituição; (ii) a natureza das operações a complexidade dos produtos, serviços, atividades e processos da instituição; e (iii) a sensibilidade dos dados e das informações sob responsabilidade da instituição.

Sobre o item (iii), destaca-se que o termo "sensibilidade" não se refere à dados sensíveis, nos termos do art. 5º, II[48] da LGPD, propriamente ditos. Aqui, a norma parece adotar o termo leigo para sensibilidade, no sentido de aproximá-lo do termo "importância".

No Art. 3º da norma, o BACEN estipula os requisitos mínimos de Políticas de Segurança Cibernética. Para o órgão uma Política Cibernética deve:

> "I - os objetivos de segurança cibernética da instituição;
>
> II - os procedimentos e os controles adotados para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivo de segurança cibernética;
>
> III - os controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis;
>
> IV - o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição;
>
> V - as diretrizes para:
>
> a) a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios;
>
> b) a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da instituição;
>
> c) a classificação dos dados e das informações quanto à relevância; e

[48] "Art. 5º Para os fins desta Lei, considera-se:
I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural"

d) a definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes;

VI - os mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

a) a implementação de programas de capacitação e de avaliação periódica de pessoal;

b) a prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros; e

c) o comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética; e

VII - as iniciativas para compartilhamento de informações sobre os incidentes relevantes, mencionados no inciso IV, com as demais instituições referidas no art. 1º."

Sobre a divulgação da Política de Segurança Cibernética, em um padrão similar ao princípio da transparência da LGPD (art.6º, VI[49]), o BACEN afirma que ela deve ser divulgada aos funcionários da instituição e às empresas parceiras prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações. Neste caso, aplicam-se os mesmos comentários realizados neste item sobre o termo "sensibilidade". Ademais, ressalta-se que a divulgação é direcionada apenas a funcionários e instituições parceiras, não estando incluso o cliente ou o titular dos dados tratados pela instituição financeira e demais instituições do escopo.

Na parte final do capítulo são mencionadas as ações que as instituições precisam tomar para prevenir e agir em face de um incidente de segurança, incluindo o estabelecimento de rotinas, procedimentos e controles, bem como implementação de tecnologias para responder a incidentes. A norma determina controles específicos, atendo-se, portanto, a uma abordagem generalista para a proteção da Segurança da Informação.

[49] "Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
[...]
VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial"

Ainda assim, percebe-se, pelo texto das normas, que se esperava das instituições financeiras um nível avançado de segurança cibernética e da informação, ainda antes da vigência da LGPD.

1.4. Análise dos princípios na regulamentação setorial financeira pós-LGPD: as Resoluções BCB n.º 85/2021 e CMN n° 4.893/2021

Após a vigência da LGPD, foram publicadas as Resoluções BCB n.º 85/2021 e CMN n° 4.893/2021 que atualizam as normas n.º Resolução BACEN 4658/2018 e Circular BACEN n.º 3.909/2018, respectivamente.

Essas atualizações decorrem do Decreto nº 10.139, de 28 de novembro de 2019, que estabeleceu a obrigatoriedade de os órgãos e entidades da administração pública federal direta, autárquica e fundacional revisarem e consolidarem os atos normativos editados no âmbito de suas respectivas competências. Essa medida tinha como propósito revisar, atualizar, simplificar e consolidar os atos normativos, a fim de racionalizar o estoque regulatório.

Em face do disposto nesse Decreto, foi constituída força-tarefa no âmbito das unidades da área de Regulação do BACEN para planejar e executar a revisão dos atos normativos vigentes.

Nesse processo de revisão, foram analisados mais de 2.600 atos normativos vigentes editados pelo Banco Central e pelo Conselho Monetário Nacional. Entre esses temas, foi identificada a necessidade de consolidar as normas que dispõem sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem aplicadas às instituições financeiras, autorizadas a funcionar pelo BACEN e instituições de pagamento[50].

Como mudanças, o BACEN instituiu que, quanto à comunicação ao Banco Central das ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem situação de crise pela instituição de pagamento, as instituições

[50] BRASIL. Banco Central do Brasil. Exposição de motivos n.º 85/2023. Disponível em: https://normativos.bcb.gov.br/Votos/BCB/202174/Voto_do_BC_74_2021.pdf . Último acesso em: 30 de junho de 2023.

financeiras devem estabelecer e documentar os critérios que configurem esse tipo de situação, mantendo a documentação disponível para o BACEN pelo prazo de cinco anos.

Além dessa modificação, as demais mudanças em relação às normas até aqui vigentes foram poucas. Uma delas é a redução do prazo para comunicação ao BACEN de contratações e alterações a contratações relevantes de processamento, armazenamento de dados e de computação em nuvem, que deverá ocorrer em até 10 dias e não mais 60 dias. Essa mudança não impacta o escopo deste trabalho e não será abordada em detalhes.

Nesse sentido, percebe-se que, ainda que as mudanças tenham sido feitas após a vigência da LGPD, os critérios estabelecidos para instituições financeiras em termos de segurança cibernética e segurança da informação não foram alterados significativamente. Além disso, as normas não tecem comentários específicos em relação à proteção dos dados pessoais de seus clientes, estando as instituições financeiras no escopo da LGPD nesse sentido.

Ainda assim, existe uma expectativa de que instituições financeiras devem ter um nível superior de segurança, haja vista que lidam com os ativos financeiros de seus clientes.

Portanto, é de se esperar que, em razão do porte e recursos econômicos que instituições financeiras costumam possuir, as normas sejam aplicadas com rigor e que o gerenciamento de riscos e processos de identificação e remediação de incidentes sejam robustos.

No próximo capítulo, este trabalho tratará do arcabouço legal aplicável tanto a instituições financeiras quanto a outros agentes de tratamento em relação à proteção de dados especificamente. Nele serão entendidos os critérios esperados por todos os agentes de tratamento em relação à segurança dos dados, que, junto às normas específicas do setor, oferecem o panorama do que é esperado em termos de segurança pelas instituições financeiras.

CAPÍTULO 2 | Os conceitos de segurança da informação no texto da LGPD e o cenário pós-regulamentação

Frazão, Carvalho e Milanez[51] explicam que, enquanto na Europa, desde a década de 1980 já eram elaboradas legislações nacionais de proteção de dados pessoais, no Brasil, se testemunhavam ainda a promulgação das primeiras leis estaduais relacionadas tão somente a direito de acesso e retificação de dados pessoais[52].

Desde a inclusão pela Constituição Federal de 1988 do *habeas data* (art. 5º, LXXII) e da previsão de direitos fundamentais relacionados à inviolabilidade da vida privada, da intimidade, da honra, da imagem, da casa, da correspondência, das comunicações telegráficas, dos dados e das comunicações telefônicas dos indivíduos (art. 5, X, XI, XII), o arcabouço legal brasileiro relacionado à proteção dos dados pessoais tem se tornado cada vez mais robusto.

Em 30 de novembro de 2010 o Ministério da Justiça tornou pública a primeira versão do texto que foi utilizado como base para a elaboração da LGPD. A aprovação e sanção da versão final da Lei Geral de Proteção de Dados na forma da Lei Federal n.º 13,709/2018 ocorreu oito anos após o início do debate público sobre o texto e, a partir desse momento, a proteção específica dos dados pessoais passou a fazer parte do arcabouço legislativo brasileiro, de forma específica[53].

---

[51] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ed. Rio de Janeiro: Forense, 2022.

[52] "No Rio de Janeiro, a Lei Estadual 824, de 28 de dezembro de 1984, que "Assegura o direito de obtenção de informações pessoais contidas em bancos de dados operando no Estado do Rio de Janeiro e dá outras providências" e, em São Paulo, a Lei Estadual 5.702, de 5 de junho de 1987, que "Concede ao cidadão o direito de acesso às informações nominais sobre sua pessoa." FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ed. Rio de Janeiro: Forense, 2022. p. 21.

[53] O escopo deste trabalho concentra-se em normas que se referem especificamente às instituições financeiras ou à proteção dos dados pessoais, no entanto, as normas aqui dispostas não contemplam a

Pouco tempo depois, o direito à proteção de dados pessoais também foi inserido no arcabouço constitucional definitivamente por meio da Emenda Constitucional 115/2022, que inseriu o art. 5º, inciso LXXIX que determina que "É assegurado, nos termos da lei, o direito à proteção de dados pessoais, inclusive nos meios digitais".

A entrada em vigor da legislação e a elevação da proteção dos dados pessoais ao patamar de direito constitucional evidenciou a importância desses ativos informacionais para a garantia de direitos dos cidadãos. Portanto, é natural que a legislação também tenha previsto os contornos das hipóteses que configuram a infringência desses direitos, inclusive a quebra do direito à segurança desses ativos informacionais sendo este o ponto de contato entre as disciplinas da proteção de dados e da segurança da informação.

2.1. Dispositivos da LGPD relacionados à Segurança da Informação

Após sua entrada em vigor, as determinações da LGPD passaram a ser exigíveis a todos os agentes de tratamento, balizando sua atuação e tratamento de dados de maneira a tentar proteger os dados pessoais dos titulares.

Dentre os muitos pilares da LGPD, os princípios dispostos no art. 6º do normativo representam os contornos pelos quais os agentes de tratamento devem se pautar para verificar a regularidade do tratamento de dados realizado por eles.

Muitos desses princípios relacionam-se intrinsecamente com a segurança da informação pelo fato de que dados pessoais são um dos tipos de informação que está abarcada pela segurança da informação, ainda que por muito tempo não fosse relegado a esse tipo de ativo o mesmo nível de proteção que informações comerciais estratégicas ou aquelas consideradas protegidas pelo sigilo industrial, por exemplo.

É por esse motivo que, quando se trata de um cenário pós-LGPD, a segurança da informação passou a ser uma das reflexões mais importantes em termos de programas de

completude de normas que de alguma forma disciplinam a proteção das informações. O ambiente regulatório e legal brasileiro tem se beneficiado do interesse do legislador e dos entes governamentais em regulamentar matérias que são parte do universo da proteção das informações, de uma forma ou de outra, em maior ou menor grau. Sendo assim, é evidente que existem outras evoluções relevantes que não serão tratadas com detalhamento neste trabalho. Um exemplo é a Estratégia Nacional de Segurança Cibernética - E-Ciber que é um conjunto de ações estratégicas do governo federal relacionadas a área de segurança cibernética até 2023. A estratégia corresponde ao primeiro módulo da Estratégia Nacional de Segurança da Informação estabelecendo ações com vistas a modificar, de forma cooperativa e em âmbito nacional, características que refletem o posicionamento de instituições e de indivíduos sobre o assunto. Já a Política Nacional de Segurança da Informação (PNSI) também faz parte da estratégia e foi instituída pelo Decreto n.º 9.637/2018 e abrange segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais. Nesse sentido, é evidente que existe um interesse robusto em proteger a informação por parte do Estado Brasileiro haja vista que existe um reconhecimento de que a proteção da informação é crucial para o funcionamento dos setores público e privado.

conformidade em proteção de dados. Sendo assim, a LGPD dedica um capítulo específico à segurança e sigilo de dados, determinando que agentes de tratamento têm o dever da garantia de segurança das informações sob sua responsabilidade.

Para Frazão, Carvalho e Milanez, é fundamental que se aprofunde a compreensão sobre a noção de segurança da informação adotada pela LGPD para que se verifique de que maneira o princípio legal em questão – disposto no artigo 6º, I – se traduz em medidas concretas aptas a serem inseridas em um programa de conformidade, ou *compliance*, em dados[54].

Destaca-se que a segurança da informação abrange um escopo muito maior e mais amplo que a segurança dos dados pessoais, como já afirmado anteriormente neste trabalho, pois se refere a todo tipo de informação considerada relevante pela organização que a trata, incluindo a definição do nível de segurança que cada informação precisa ser submetida[55].

Nesse sentido, para além do princípio da segurança, este trabalho analisará alguns princípios e requisitos da LGPD que se relacionam com a segurança dos dados pessoais e prevenção de incidentes de segurança para oferecer os subsídios necessários para a análise das decisões acerca de incidentes de segurança envolvendo instituições financeiras e sua sofisticação em termos de proteção de dados.

Os princípios analisados serão os princípios do (i) livre acesso e da qualidade de dados, em conjunto; (ii) segurança; (iii) prevenção. Já os dispositivos específicos analisados serão os que se referem especificamente (i) aos Incidentes de Segurança (arts. 46 a 49); (ii) aos instrumentos de mitigação de risco; (iii) ao Programa de Privacidade (art. 50); e (iv) Gestão de Risco.

Todos esses itens tratados na LGPD são fundamentais para o entendimento do impacto de um incidente de segurança da informação e, consequentemente, para a análise de um evento deste tipo em juízo. Portanto, nos itens a seguir, este trabalho se deterá a esses princípios para utilizá-los como baliza para a análise das decisões, logo em seguida.

2.1.1. Princípio do livre acesso (art. 6º, IV) e Princípio da qualidade dos dados (art. 6º, V)

[54] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD.* 1ed. Rio de Janeiro: Forense, 2022 p. 382.
[55] *Ibidem* p. 383.

Em primeiro lugar, analisa-se os princípios do livre acesso, presente no art. 6º, VI[56], da LGPD e o princípio da qualidade de dados, descrito no art. 6º, V[57] do mesmo diploma legal. A razão da análise conjunta desses dois princípios se dá pelo fato de que, como se verá adiante, eles abarcam as situações de perda, eliminação e alteração de dados, algumas das situações que podem ensejar um incidente de segurança. No entanto, a grande maioria das decisões analisadas no terceiro capítulo deste trabalho não estão relacionadas a essas hipóteses. Portanto, apesar de imprescindíveis para a classificação de incidentes de segurança, esses princípios não serão tratados de forma extensa neste trabalho.

O princípio do livre acesso é pertinente em termos de segurança da informação pois relaciona-se com o princípio da disponibilidade descrito na tríade CID. Isso porque esse princípio exige que os agentes de tratamento garantam aos titulares a consulta facilitada e gratuita sobre a forma de tratamento, bem como sua duração. Além disso, os agentes de tratamento devem possuir a integralidade dos dados pessoais tratados e serem capazes de fornecê-la sempre que solicitados[58].

Esse princípio materializa-se de forma direta no direito de acesso que o titular possui, e implicitamente nos artigos 18, 19 e 20 da LGPD. Esses dispositivos indicam as formas pelas quais os titulares podem acessar as informações que lhes dizem respeito.

Nesse sentido, a disponibilidade relaciona-se com esse princípio pois, se estão ausentes ou indisponíveis, ainda que temporariamente, os dados do titular, resta prejudicado o direito ao acesso a esses dados.

Já o princípio da qualidade de dados relaciona-se com o princípio da integridade. Segundo Frazão, Carvalho e Milanez, esse princípio possui intrínseca relação com outros princípios do livre acesso e da transparência por relacionar-se com a autonomia informacional do titular dos dados[59].

Os autores também ressaltam que esse princípio não se resume apenas à atualidade de dados. Para eles, embora os dados desatualizados também configurem uma situação de não conformidade com a LGPD, o princípio abrange um escopo bem mais amplo,

[56] "Art. 6. [...] IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais"
[57] "Art. 6. [...] V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento"
[58] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD.* 1ed. Rio de Janeiro: Forense, 2022. p. 87
[59] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD*. 1ed. Rio de Janeiro: Forense, 2022, p. 89.

servindo também como um mecanismo de avaliação da aptidão dos dados em questão para o atingimento da finalidade do tratamento[60].

Segundo a definição adotada por este trabalho, a integridade perpassa a noção de que os dados devem ser mantidos da forma que foram disponibilizados, livres de alterações acidentais ou intencionais, quando acessados pelos indivíduos autorizados e de forma que sejam confiáveis. Sendo assim, quando o princípio da qualidade de dados determina que os dados tratados devem dotar de exatidão, clareza, relevância bem como devem estar atualizados, a LGPD aproxima esse conceito do pilar da integridade, pois a intenção do legislador aparenta tentar garantir aos dados pessoais justamente o que o princípio da integridade preconiza: a correspondência entre a realidade e os dados pessoais em tratamento.

2.1.2. Princípio da segurança (art. 6º, VII)

O princípio da segurança está delineado pela LGPD no art. 6º, VII, como a utilização de medidas 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 difusão.

Frazão, Carvalho e Milanez explicam que, em outras palavras, esse princípio pretende proteger não apenas os dados pessoais contra divulgações indevidas, mas também a qualidade dos dados, evitando a adulteração destes[61]. Além disso, conforme visto no tópico anterior, adicionaríamos que a segurança também visa proteger a disponibilidade dos dados e garantir seu acesso, pelo titular, a todo momento.

Os autores explicam que medidas técnicas compreendem a utilização de medidas tecnológicas e procedimentos de segurança, enquanto as medidas de ordem administrativa compreendem a utilização de soluções organizacionais que restrinjam, controlem e protejam os dados contra acessos indevidos, o que é particularmente importante em grandes organizações[62].

Já Menke e Goulart[63] afirmam que:

---

[60] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD.* 1ed. Rio de Janeiro: Forense, 2022 p. 89

[61] *Ibidem*. p. 95.

[62] *Ibidem.* p. 95.

[63] MENKE, Fabiano. GOULART, Guilherme Damasio. *Segurança da informação e vazamento de dados*. In: BIONI, Bruno. Tratado de Proteção de Dados Pessoais. São Paulo: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 15 jun. 2023. p. 356.

> "As medidas administrativas são aquelas que visam não somente a promoção da conformidade das ações com toda a LGPD, mas também aquelas que visam a organização da segurança da informação na instituição. Um possível exemplo poderia ser todas as políticas de segurança, standards e guias de procedimentos para controlar o comportamento dos agentes no sentido de "prover um nível aceitável de proteção para os recursos computacionais e para os dados"34. No âmbito da GDPR, o Considerando 78 indica que entre as medidas estão a minimização no tratamento, a pseudonimização e a transparência no tratamento. Já as medidas técnicas envolvem o uso de recursos, como firewalls, antimalware e antivírus, controles de acesso nos sistemas operacionais, tokens, criptografia etc.35.
>
> As medidas de segurança técnicas e administrativas também estão presentes no art. 46 da LGPD. Elas visam, conforme o artigo, a proteção não somente contra acessos não autorizados, o que compromete a confidencialidade dos dados, mas também situações de perda, alteração ou qualquer tratamento inadequado ou ilícito. Portanto, as medidas de segurança visam não somente evitar vazamentos, mas também evitar qualquer tipo de tratamento ilícito ou inadequado. Um exemplo básico é a criação de medidas internas de controle de acesso para impedir que os empregados que não tenham entre suas atribuições o contato com dados dos clientes acessem essas informações."

O Regulamento Europeu ("GDPR") também determina, em seu artigo 5º que os dados pessoais serão tratados de uma forma que garanta sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra sua perda, destruição ou danificação acidental, adotando as medidas técnicas e organizacionais adequadas (*integridade* e *confidencialidade*)[64].

No Considerando 29, o GDPR também determina que os dados devem ser tratados de forma a garantir sua segurança devida e sua confidencialidade, inclusive para evitar o acesso a dados pessoais e equipamento utilizado para seu tratamento, ou a sua utilização por pessoas não autorizadas[65].

Frazão, Carvalho e Milanez[66] também explicam que a materialização desse princípio está situada nos art. 46, 47 e 48 da LGPD, que serão tratados com maior detalhamento nos próximos tópicos deste trabalho.

---

[64] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). Disponível em: <https://eur lex.europa.eu/legalcontent/PT/TXT/?uri=CELEX%3A32016R0679>. Acesso em: 28 jun. 2023. Art. 5 (F)

[65] *Ibidem*

[66] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD*. 1ed. Rio de Janeiro: Forense, 2022

Tendo em vista o exposto, a segurança esperada não deve ser aplicada exatamente aos dados em si, mas sim aos sistemas que os mantêm (medidas técnicas) e ao ambiente geral da instituição (medidas organizativas). Portanto, explicam Menke e Goulart, isso significa que não bastam as medidas técnicas, como o uso de firewalls, métodos criptográficos e controles de conteúdo, se elas não vierem acompanhadas de outras medidas, como treinamentos de segurança, criação de políticas de segurança da informação, inventários de ativos etc.[67]

A *Commission Nationale de l'Informatique et des Libertés* (CNIL), a Autoridade de proteção de dados francesa, recomendou, como medidas de segurança, a conscientização e autenticação dos utilizadores, limitação de acesso aos dados, adoção de ambiente auditável e medidas de gestão de incidentes, segurança dos postos de trabalho (incluindo dispositivos móveis), meios técnicos de proteção da rede interna, segurança em servidores e sites web, armazenamento seguro dos dados, segurança dos dados em todo seu ciclo de vida, integração da segurança da informação na gestão de projetos etc[68].

Esse princípio é central para qualquer consideração a ser feita sobre incidentes de segurança já que é o princípio que baliza tanto a definição de um incidente quanto o que é minimamente esperado como forma de prevenção.

No próximo item, trataremos do princípio que cristaliza a obrigatoriedade da adoção de medidas preventivas.

2.1.3. Princípio da prevenção (art 6º, VIII)

O princípio da prevenção está disposto no art. 6º, VIII, da LGPD e determina que medidas devem ser adotadas para prevenir a ocorrência de danos aos titulares em virtude do tratamento inadequado dos seus dados pessoais.

[67] MENKE, Fabiano. GOULART, Guilherme Damasio. *Segurança da informação e vazamento de dados.* In: BIONI, Bruno. *Tratado de Proteção de Dados Pessoais.* São Paulo: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 15 jun. 2023. p. 356.

[68] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS. *Guide de la sécurité des données personnelles*. Disponível em: <https://www.cnil.fr/sites/default/files/atoms/files/cnil_guide_securite_des_donnees_personnelles-2023.pdf> . Acesso em: 14 de junho de 2023.

Segundo Frazão *et. al.,* a prioridade dos agentes deve ser evitar o dano, sem prejuízo da sua responsabilidade administrativa e civil pelos danos que porventura possam surgir[69].

Portanto, afirmam os autores que os agentes de tratamento precisam formular regras de boas práticas e de governança que garantam o tratamento adequado dos dados pessoais, facilitando a adequação às disposições determinadas na LGPD, bem como agir para que todas as cautelas e medidas preventivas possíveis para prevenção dos dados sejam adequadamente tomadas[70].

Destaca-se que o princípio da prevenção pode ser tido como uma complementação ao princípio da segurança em termos de prevenção de incidentes de segurança. Ambos os princípios auxiliam um ao outro e são intrinsecamente dependentes um do outro em termos de efetividade, haja vista que sem prevenção não haverá segurança plena e sem segurança a prevenção não será capaz de promover efeitos adequados em termos de proteção dos dados pessoais dos titulares.

Nesse sentido, tratados os princípios necessários para a compreensão de um incidente de segurança, faz-se necessária a análise da natureza dos incidentes de segurança conforme a LGPD, bem como seus contornos e configuração.

2.1.4. Incidentes de Segurança (arts. 46 a 49)

É indiscutível a importância relegada pela LGPD à segurança dos dados pessoais. É por esse motivo que afirmam Ana Frazão e Mariana Pinto[71] que a questão da responsabilidade que os agentes de tratamento têm em face da violação dos deveres de segurança é um dos principais pressupostos da LGPD.

É nesse sentido que o art. 44 do normativo determina que:

> "Art. 44. 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 [...]
>
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

[69] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD*. 1ed. Rio de Janeiro: Forense, 2022. p. 96.
[70] *Ibidem.* p. 97.
[71] FRAZÃO, Ana; PINTO, Mariana. *Compliance de Dados e Incidentes de Segurança*. In: PINHEIRO, Carolina da Rosa. Compliance entre teoria e prática: reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado, 2022. Indaiatuba,SP: Editora Foco, 2022.

Frazão e Pinto[72] então argumentam que os incidentes de segurança podem ser causados tanto por falhas técnicas – tecnologias de segurança inadequadas ou insuficientes – como também falhas humanas, tais como não observância das regras de segurança, perda de equipamentos que contêm dados.

A LGPD dedicou um capítulo inteiro ao tratamento e prevenção de incidentes de segurança, trata-se do Capítulo VII – Da Segurança e das Boas Práticas. O artigo 46 determina que:

> "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."

Esse artigo baliza o entendimento sobre incidentes de segurança na LGPD, sendo dele extraído o cerne do que se entende por incidente de segurança. O artigo 48 completa o entendimento sobre incidentes de segurança ao adicionar que devem ser comunicados à autoridade os incidentes que possam causar "risco ou dano relevante aos titulares".

Por fim, a Autoridade esclarece em seu Guia orientativo que o art. 49 determina que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos na LGPD e nas demais normas regulamentares. O artigo 50 será tratado em separado mais adiante neste trabalho haja vista que introduz as medidas de prevenção que devem ser adotadas pelos agentes de tratamento a fim de proteger os dados pessoais.

A Autoridade Nacional de Proteção de Dados ("ANPD") publicou em outubro de 2021 o Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Nesse guia a Autoridade fez considerações importantes sobre o que é esperado dos agentes de tratamento em termos de segurança da informação. Em que pese a maioria das instituições financeiras, objeto de estudo neste trabalho, sejam agentes de tratamento de médio e grande porte, algumas considerações feitas pela autoridade podem ser aproveitadas para fins de exemplificação.

[72]FRAZÃO, Ana; PINTO, Mariana. *Compliance de Dados e Incidentes de Segurança* In: PINHEIRO, Carolina da Rosa. Compliance entre teoria e prática: reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado, 2022. Indaiatuba,SP: Editora Foco, 2022.

A Autoridade determina no Guia Orientativo que as obrigações impostas pelos artigos 46, 47, 49 e 50 da LGPD, referentes à segurança de informação relacionada a dados pessoais, foram baseadas em boas práticas internacionais e refletem um conjunto de orientações sobre o tema.

O artigo 46, § 1º, concede à ANPD a competência para estabelecer parâmetros mínimos para prevenir incidentes de segurança. Ainda assim, ANPD não publicou, até a data de conclusão deste trabalho, a norma regulamentadora que trata de incidentes de segurança[73].

A Autoridade, entretanto, publicou orientações gerais[74] sobre incidentes de segurança, ainda não vinculantes, enquanto perdurar essa lacuna regulatória. Nesse sentido, a Autoridade determinou que um incidente de segurança:

> "É um evento adverso **confirmado** que comprometa a **confidencialidade, integridade ou disponibilidade de dados pessoais**. Pode decorrer de ações **voluntárias** ou **acidentais** que resultem em divulgação, alteração, perda indevidas ou acessos não autorizados a dados pessoais, independentemente do meio em que estão armazenados." (grifo nosso)[75]

Sendo assim, a ANPD esclareceu que os incidentes de segurança podem ocorrer de forma acidental, como o envio de informações para o destinatário incorreto, ou em decorrência de atos intencionais, como a invasão de um sistema de informação ou o furto de um dispositivo de armazenamento de dados.

Ainda, a Autoridade sedimentou que os incidentes de segurança não se restringem às violações da confidencialidade, abrangem também eventos de perda ou indisponibilidade dados pessoais, como já mencionado anteriormente neste trabalho. São exemplos de incidentes de segurança o sequestro de dados (*ransomware*[76]), o acesso não

---

[73] No momento da publicação deste trabalho, essa norma estava em consulta pública e poderá ser acessada por meio do link: https://www.gov.br/participamaisbrasil/regulamento-de-comunicacao-de-incidente-de-seguranca-com-dados-pessoais. Acesso em: 12 de junho de 2023

[74] Autoridade Nacional de Proteção de Dados (ANPD). Comunicação de incidente de segurança. Publicado em 23 de dezembro de 2022. Disponível em https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis. Último acesso em: 10 de julho de 2023.

[75] Autoridade Nacional de Proteção de Dados (ANPD). *Guia Orientativo: Segurança da Informação para Agentes de Tratamento de Pequeno Porte*, Versão 01. Brasília, DF, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em 12 de junho 2023.

[76] *Um ransomware* é um tipo de malware que criptografa os arquivos de um sistema ou dispositivo, impedindo o acesso do usuário a eles. Os atacantes, então, exigem um resgate (*ransom*) para descriptografar os arquivos e restaurar o acesso. Geralmente, eles solicitam o pagamento em criptomoedas para dificultar o rastreamento.

autorizado a dados armazenados em sistemas de informação e a publicação não intencional de dados dos titulares.

Abaixo, reproduz-se a imagem que representa a matriz divulgada pela ANPD para a identificação de um incidente de segurança da informação envolvendo dados pessoais. Nota-se que, assim como já mencionado neste trabalho, os incidentes de segurança decorrem da violação dos princípios da segurança da informação aqui descritos que possam causar risco ou dano relevante ao titular de dados, quando a violação envolver dados pessoais desse titular.

Figura 2.1.
Matriz de identificação para identificação de incidente

Fonte: ANPD. Acesso em 12 de junho de 2023

A Autoridade foi além ao determinar que a avaliação de risco do incidente, devem ser considerados, dentre outros aspectos: (i) o contexto da atividade de tratamento de dados; (ii) as categorias e quantidades de titulares afetados; (iii) os tipos e quantidade de dados violados; (iv) os potenciais danos materiais, morais, reputacionais causados aos titulares; (v) se os dados violados estavam protegidos de forma a impossibilitar a

Os *ransomwares* são disseminados por meio de diferentes métodos, como e-mails de phishing, downloads de arquivos infectados, sites comprometidos ou exploração de vulnerabilidades em sistemas. Uma vez que o *ransomware* é executado no sistema alvo, ele começa a criptografar os arquivos, exibindo uma mensagem com instruções para o pagamento do resgate. KAPERSKY. What is ransomware? How to prevent and remove ransomware. Disponível em: https://www.kaspersky.com/resource-center/threats/ransomware. Último acesso em: 10 de julho de 2023.

identificação de seus titulares; (iv) as medidas de mitigação adotadas pelo controlador após o incidente.

A Autoridade ressaltou que o mesmo tipo incidente pode ou não ser considerado capaz de causar risco ou dano relevante em função da combinação desses critérios. Isso se deve, segundo a Autoridade, ao fato de que a avaliação dependerá do tipo de dado armazenado, do contexto da atividade de tratamento e do fato de os dados estarem ou não protegidos por criptografia[77].

Para a Autoridade, são considerados capazes de causar risco ou dano relevante os incidentes que possam causar aos titulares danos materiais ou morais, expô-los a situações de discriminação ou de roubo de identidade, especialmente se envolverem dados em larga escala, sensíveis e de grupos vulneráveis como crianças e adolescentes ou idosos.

A Autoridade, por fim, também determinou que a mera existência de uma vulnerabilidade em um sistema de informação não constitui um incidente de segurança. A exploração da referida vulnerabilidade, no entanto, pode resultar em um incidente.

Ademais, nem toda fraude pode ser considerada um incidente de segurança. Essa consideração da Autoridade é particularmente interessante para este trabalho pois a maioria das decisões a serem analisadas no Capítulo 3 decorrem de fraudes realizadas com base nos dados pessoais dos clientes de instituições financeiras.

Recentemente a autoridade disponibilizou para consulta pública a minuta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais. As deveriam ser enviadas pela plataforma do Participa Mais Brasil entre os dias 02 e 31 de maio de 2023. Posteriormente, a autoridade prorrogou a consulta por 15 (quinze) dias, sendo o novo prazo 15 de junho de 2023. Nessa minuta foram disponibilizados os parâmetros para a avaliação do risco e da gravidade dos incidentes bem como há a

[77] A criptografia é o processo de transformar informações legíveis em um formato ilegível chamado de texto cifrado, utilizando um algoritmo específico e uma chave de criptografia "O termo criptografia vem do grego e é uma combinação das palavras "*kryptós*",- que significa "escondido", e "*gráphein*", que significa "escrita". Exemplos de criptografia são tão velhos como a proverbial estrada para Roma. De fato, criptografia foi usada pelos romanos para transmitir mensagens militares. Mesmo que a mensagem caísse nas mãos inimigas, eles não seriam capazes de obter qualquer informação a partir dela, uma vez que a mensagem pareceria sem sentido. A pesquisa de algoritmos criptográficos também é referida como criptoanálise e é usada não só para desenvolver algoritmos, mas também para quebrar algoritmos inimigos. " HINTZBERGEN, Jule. HINTZBERGEN, Kees; SMULDERS, André ; BAARS, Hans. *Fundamentos da Segurança da Informação com base na ISO 27001 e na ISO 27002*. Tradução de Alan de Sá. Bransport: Rio de Janeiro, 2018. Edição Biblioteca Pearson.

tentativa de sedimentação de conceitos da segurança da informação já tratados neste trabalho.

A minuta apresenta as seguintes definições:

> "Art. 3º Para efeitos deste Regulamento são adotadas as seguintes definições:
>
> [...]
>
> V - confidencialidade: propriedade pela qual se assegura que o dado pessoal não esteja disponível ou não seja revelado a pessoas, sistemas, órgãos ou entidades não autorizadas e nem credenciadas;
>
> [...]
>
> VII - dado financeiro: dado pessoal relacionado às transações financeiras do titular, inclusive para contratação de serviços e aquisição de produtos;
>
> [...]
>
> IX - disponibilidade: propriedade pela qual se assegura que o dado pessoal esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;
>
> X - incidente de segurança com dados pessoais: qualquer evento adverso confirmado, relacionado à violação das propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais;
>
> XI - integridade: propriedade pela qual se assegura que o dado pessoal não seja modificado ou destruído de maneira não autorizada ou acidental"

Além disso, a minuta descreve em seu Art. 5º que serão considerados incidentes os eventos que puderem causar risco ou dano relevante aos titulares aqueles que envolverem dados sensíveis, dados financeiros, dados de autenticação de sistemas, dados em larga escala ou de crianças, adolescentes ou idosos. Dados financeiros são inegavelmente um tipo de dado que tem o potencial de causar dano relevante, inclusive monetário, caso estejam envolvidos em um incidente de segurança, portanto, é papel das instituições financeiras tratá-los de forma a protegê-los de incidentes de segurança. A Autoridade parece, em razão do teor da minuta, concordar com essa afirmação já que inclui esse tipo de dado como um dos critérios de avaliação da gravidade de incidentes.

Ainda que a minuta não configure uma definição final sobre o tema, já que ainda se encontra em consulta pública, esses conceitos podem oferecer um parâmetro para o entendimento, ainda que preliminar, da autoridade sobre incidentes de segurança.

Ainda no escopo da consulta pública para a minuta, a Autoridade realizou no dia 23 de maio de 2023, Audiência Pública, transmitida ao vivo pelo canal da ANPD no Youtube. O propósito da audiência foi debater a proposta de Regulamento de Comunicação de Incidente de Segurança com Dados Pessoais, tema previsto na Agenda Regulatória 2023-2024 da Autoridade. A sessão aberta com manifestação de comentários e sugestões contou com 47 (quarenta e sete) contribuições de representantes de diversos setores da sociedade.

2.1.5. Instrumentos de prevenção e mitigação de danos

Consideradas as disposições anteriores, tanto regulatórias, setoriais e da legislação específica, espera-se que os agentes de tratamento adotem medidas preventivas que dificultem a ocorrência de incidentes de segurança. Existem, portanto, diversos instrumentos de segurança que podem auxiliar os agentes de tratamento a manter os dados pessoais dos titulares protegidos de incidentes.

Menke e Goulart[78] explicam que o art. 46 prevê a observância das medidas de segurança tanto na fase de concepção dos produtos quanto na fase de execução. A primeira situação envolve o que se convencionou chamar de *privacy by design*[79]. No entanto, Frazão, Carvalho e Milanez ressaltam que não se pode esquecer que o assunto do art. 46 é fundamentalmente a segurança da informação[80].

Mais adiante, o art. 50 da LGPD, ao enunciar a possibilidade de os controladores e operadores adotarem boas práticas de segurança, prevê a criação de um "programa de governança em privacidade" (art. 50, § 2.º, I). Esses programas de governança deverão levar em consideração as chamadas medidas técnicas e administrativas descritas no princípio da segurança já abordado neste trabalho[81].

---

[78] MENKE, Fabiano. GOULART, Guilherme Damasio. *Segurança da informação e vazamento de dados. In: BIONI, Bruno. Tratado de Proteção de Dados Pessoais.* São Paulo: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 15 jun. 2023

[79] BIONI, Bruno Ricardo. *Proteção de dados pessoais: a função e os limites do consentimento.* Rio de Janeiro: Forense, 2019. p. 176: "É a ideia de que a proteção de dados pessoais deve orientar a concepção de um produto ou serviços, devendo eles ser embarcados com tecnologias que facilitem o controle e a proteção das informações pessoais".

[80] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD*. 1ed. Rio de Janeiro: Forense, 2022. p. 393.

[81] MENKE, Fabiano; GOULART, Guilherme Damasio. *Segurança da Informação e Vazamento de Dados. p. 357. BIONI, Bruno. Tratado de Proteção de Dados Pessoais.* São Paulo: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 14 jun. 2023.

Além desses mecanismos trazidos pela literatura, a própria LGPD recomenda a adoção de alguns mecanismos específicos que possuem o objetivo de contribuir para a proteção dos dados pessoais dos titulares durante o tratamento de dados pelos agentes de tratamento. Nos próximos itens, o programa de governança em privacidade e os mecanismos mencionados pela LGPD serão examinados com maior detalhamento.

2.1.5.1. Programa de Governança em Privacidade (art. 50)

De acordo com o exposto até o momento neste trabalho, fica evidente que um incidente de segurança pode decorrer tanto de uma falha técnica quanto de falhas humanas e que a realidade demonstra que existe uma ameaça real da ocorrência de um incidente de segurança, haja vista a frequência e a extensão dos incidentes já noticiados na mídia.

Frazão e Pinto explicam que, ainda que a LGPD se baseie igualmente no *enforcement*[82] a ser conferido pela ANPD, essa faceta é apenas uma parte de um projeto maior que envolve a cooperação inclusive com os agentes de tratamento para criar instituições fortes que possam lastrear a proteção dos dados pessoais. As autoras citam Colin Bennet e Charles Raab[83] para afirmar que os programas de *compliance* devem ir além da legislação, servindo de complementação a ela.

Por esse motivo, Frazão e Pinto[84] argumentam a questão da segurança e do sigilo de dados não esgota o propósito de um bom programa de compliance, isso porque o art. 50, § 1º da LGPD determina que o controlador e o operador deverão estabelecer regras de boas práticas adequada a sua circunstância fática. Além disso, no § 2º do mesmo artigo, a LGPD determina alguns dos critérios essenciais para a configuração dos programas de *compliance*[85].

Os parágrafos 2º e 3º do art. 50 da LGPD preveem os requisitos do chamado "Programa de Governança em Privacidade", exigindo já no texto da lei, alguns

[82] "*Enforcement*" é um termo em inglês que se refere à aplicação ou execução de leis, regras, regulamentos ou políticas. É o processo de garantir que as diretrizes estabelecidas sejam cumpridas e de impor as consequências adequadas em caso de violação.

[83] BENNETT, Colin; RAAB, Charles D. *The governance of privacy: Policy instruments in global perspective.* Cambridge : The MIT Press, 2006, p. 151-152.

[84] FRAZÃO, Ana; PINTO, Mariana. Compliance de Dados e Incidentes de Segurança, 2022. In: PINHEIRO, Carolina da Rosa. Compliance entre teoria e prática: reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado, 2022. Indaiatuba,SP: Editora Foco, 2022. p. 43-45.

[85] Citam Frazão e Pinto que são eles: (i) estrutura do agente econômico; (ii) escala e volume de suas operações; (iii) sensibilidade dos dados tratados e (iv) gravidade dos danos que possam surgir para os titulares de dados. FRAZÃO, Ana; PINTO, Mariana. *Compliance de Dados e Incidentes de Segurança* In: PINHEIRO, Carolina da Rosa. Compliance: entre Teoria e Prática. Editora Foco, 1ª ed., 2022.

parâmetros, ainda que inespecíficos, para a elaboração de um programa de conformidade interno do agente de tratamento[86].

Ainda que a LGPD tenha mantido os parâmetros descritos inespecíficos, há diversos parâmetros utilizados no mercado que podem oferecer uma ideia mínima do que se espera em termos de conformidade. Catelli e Idie[87] afirmam que o conteúdo das políticas varia de acordo com a área de atuação e necessidades de cada organização. Dentre os exemplos mencionados pelas autoras, verifica-se que a classificação das informações e as consequências da violação das normas estabelecidas na política de segurança da informação são os mais relevantes para o escopo deste trabalho.

> "Na prática, [a política de segurança da informação] é distribuída normalmente como uma versão resumida, delineando os principais pontos. Essa distribuição pode ser feita na forma de um folheto emitido para todos os funcionários e incluído como uma parte do termo de introdução para novos funcionários. A versão completa pode ser publicada na intranet da empresa ou em algum outro local que seja facilmente acessível para todos os funcionários. Entretanto, somente a publicação na intranet não é garantia de que será lida por todos os

[86] "Art. 50 [...] § 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."

[87] CATELLI, Maria Augusta Peres ; IDIE, Renata Yumi. *Prevenir para mitigar: a importância do desenvolvimento de uma cultura de segurança cibernética nas organizações.* In: MONTANARO, Domingo; GIOVA, Giuliano; OPICE BLUM, Renato (coord.). *Cyber Risk: Estratégias Nacionais e Corporativas sobre Riscos e Segurança Cibernética.* 1ª ed. São Paulo: Thomson Reuters Brasil, 2020. p. 30.

> funcionários. Deve haver algum programa de conscientização bem balanceado para alcançar todos os funcionários"[88]

Inge Hanschke descreve que é dever das organizações adotar um sistema de gerenciamento integrado de proteção de dados e segurança da informação que seja capaz de controlar e administrar os procedimentos internos e garantir o cumprimento dos requisitos e normas legais. O autor então propõe uma abordagem integrada que conta com controles internos abrangentes[89].

---

[88] HINTZBERGEN, Jule. HINTZBERGEN, Kees; SMULDERS, André ; BAARS, Hans. *Fundamentos da Segurança da Informação com base na ISO 27001 e na ISO 27002.* Tradução de Alan de Sá. Bransport: Rio de Janeiro, 2018. Edição Biblioteca Pearson, p. 67.

[89] "Uma abordagem integrada entre proteção de dados e segurança da informação exige a criação de um sistema de controles internos abrangente, holístico e padronizado, com diretrizes, regras e processos claramente definidos. Dessa forma, propõe-se que um programa de compliance integrado esteja fundamentado nos passos abaixo:

(1) A definição da estratégia (Strategie) da organização para a condução de suas atividades, estabelecendo com clareza:
    a. Uma política de proteção de dados (que delineará os objetivos da organização com o tratamento de dados se de que maneira os cuidados com a privacidade de titulares de dados serão implementados); e
    b. Uma estratégia de segurança da informação (que servirá para expor as características da estrutura interna de segurança da entidade, os riscos a que está submetida e as razoes pelas quais determinadas medidas de segurança serão tomadas.
(2) As condições (Anforderungen) em que ocorre o tratamento de dados, expondo-se:
    a. Quais os riscos a que a organização se submete;
    b. Quais os critérios eleitos pela organização para definir o grau de aceitação de risco;
    c. Qual procedimento se adota para gerenciar tais riscos; e
    d. Quais os mecanismos de revisão e documentação desses critérios e procedimentos.
(3) As diretrizes, organização, instruções e condições técnicas (Richtlinien, Organisation, Handlungsanweisungen und technische Umsetzung) destinadas a operacionalizar as políticas de proteção de dados e segurança da informação, dentre as quais se destacam, a partir de padrões de gestão como o ISSO 27001 e parâmetros do direito positivo:
    a. A criação de Códigos de Conduta relacionados à proteção de dados e à segurança da informação;
    b. A incorporação de soluções organizacionais, como a indicação de encarregados pela proteção de dados e pela segurança da informação;
    c. A capacitação do pessoal;
    d. O gerenciamento de recursos disponíveis para a implementação das políticas e criação de uma arquitetura de proteção de dados e segurança da informação;
    e. A implementação de mecanismos de controle de acesso;
    f. A utilização de soluções de criptografia
    g. O emprego de ferramentas de segurança para ativos físicos;
    h. Mecanismos de segurança operacional no ambiente de trabalho;
    i. Aquisição, desenvolvimento e manutenção de sistemas;
    j. Diretrizes de relacionamento com fornecedores;
    k. Mecanismos de gestão de incidentes de segurança;
    l. Mecanismos de gestão da continuidade dos serviços;
    m. A redação de uma política de conformidade;
    n. Elaboração de relatório de processamento de dados;
    o. Métodos de arquivamento e exclusão;
    p. Fixação de obrigações para funcionários e parceiros;
    q. Adequação de portais eletrônicos às normas de proteção de dados;

Sendo assim, percebe-se que o programa de conformidade visa, principalmente, garantir a segurança dos dados pessoais, sob uma ótica particularizada da organização e levando em conta as necessidades não só do agente de tratamento como controlador ou operador de dados, mas do titular de dados, especialmente quando esses dados possuem a capacidade de causar risco ou dano relevante. Também é possível concluir que o programa de conformidade vai além da adoção de uma política de conformidade e perpassa diversos aspectos técnicos e organizacionais, conforme ditames da legislação.

2.1.5.2. Gestão de Risco

Segundo Whitman e Mattord, a gerência da organização é a responsável por supervisionar, possibilitar e apoiar a estrutura de segurança da informação e suas funções a fim de defender seus ativos informacionais. Portanto, parte da função dos gerentes, diretores e executivos de uma organização é estabelecer e apoiar um programa de gerenciamento de risco efetivo (em inglês, *risk management program* ou "RM")[90].

Os autores afirmam que o gerenciamento de risco envolve descobrir e entender as perguntas chave sobre o risco. As respostas para essas perguntas consistem na descoberta de (i) onde está e o que é o risco (identificação de risco); (ii) o quão grave é o nível atual do risco (análise de risco); (iii) se o nível de risco atual é aceitável (avaliação de risco); e (iv) o que pode ser feito para trazer o risco para um nível aceitável (tratamento ou controle de risco)[91].

Sendo assim, o gerenciamento de risco como um todo consiste em uma operação complexa que constitui uma estrutura de planejamento e design estratégico para a construção de um programa de gerenciamento de riscos[92].

---

r. Mecanismos de proteção aos direitos dos titulares de dados;
s. Diretrizes a serem tomadas diante de violações;
t. Mecanismos de treinamento e informação"

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ed. Rio de Janeiro: Forense, 2022. pp. 394-395. . HANSCHKE, Inge. Informationssicherheit und Datenshutz systematishc und nachhaltig gestalten : Eine komparke Einfuhrung in die Praxis. Wiesbaden : Springer, 2019.

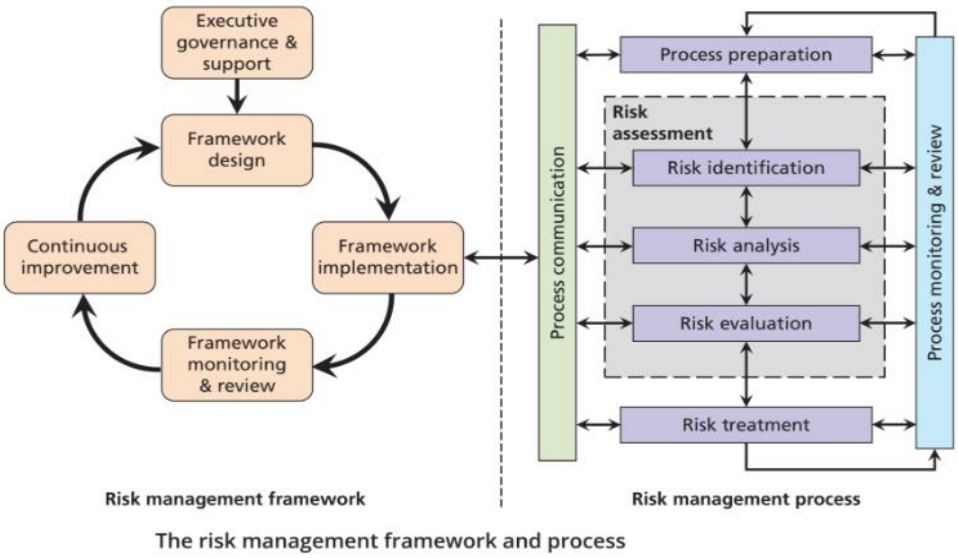
[90] WHITMAN, Michael E ; MATTORD, Herbert J. *Principles of Information Security*. Editora Cengage. 7ª Ed. Boston USA, 2022. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Hwk1EAAAQBAJ&oi=fnd&pg=PP1&dq=the+origin+of+information+security%22&ots=VirNfOfYMk&sig=eP_5xUio9nT1R7rDQImFd4KA1M0&redir_esc=y#v=onepage&q=the%20origin%20of%20information%20security%22&f=false. . p. 123

[91] *Ibidem*

[92] *Ibidem*

Figura 2.2. : The risk management framework and process

(A estrutura e o processo de gerenciamento de risco)



Fonte: Principles of Information Security[93]

Explicam Hintzbergen *et. al.* que o ciclo de um incidente possui os seguintes estágios: (i) ameaça, (ii) incidente, (iii) dano e (iv) recuperação[94].

Medidas de segurança visam um certo momento no ciclo de incidentes. As medidas objetivam prevenir incidentes (preventivas) ou reduzir as ameaças (redutivas), detectar incidentes (detectivas), responder a incidentes, parar ameaças (repressivas) e corrigir danos (corretivas)[95].

As medidas são tomadas a fim de garantir a disponibilidade, a integridade e a confidencialidade da informação da empresa, conforme já mencionado neste trabalho. Sendo assim, os autores explicam que, ocorrido o incidente, é necessário recolher provas

[93] WHITMAN, Michael E ; MATTORD, Herbert J. *Principles of Information Security*. Editora Cengage. 7ª Ed. Boston USA, 2022. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Hwk1EAAAQBAJ&oi=fnd&pg=PP1&dq=the+origin+of+information+security%22&ots=VirNfOfYMk&sig=eP_5xUio9nT1R7rDQImFd4KA1M0&redir_esc=y#v=onepage&q=the%20origin%20of%20information%20security%22&f=false. p. 124

[94] HINTZBERGEN, Jule. HINTZBERGEN, Kees; SMULDERS, André ; BAARS, Hans. Fundamentos da Segurança da Informação com base na ISO 27001 e na ISO 27002. Tradução de Alan de Sá. Bransport: Rio de Janeiro, 2018. Edição Biblioteca Pearson, p. 145.

[95] *Ibidem*

seguindo procedimentos internos, para poder investigar o incidente de segurança da informação de forma que o agente de tratamento possa se certificar de que todas as etapas são registradas para ajudar na análise do próprio incidente e para se aprender com a resposta ao incidente de segurança da informação[96].

Figura 2.3.: Ciclo de um incidente

Fonte: Fundamentos da Segurança da Informação com base na ISO 27001 e na ISO 27002[97]. p. 145.

No prisma da norma 27001, a avaliação dos riscos é feita por meio de um processo contínuo que produz resultados comparáveis, válidos e consistentes. Além disso, os riscos devem ser identificados, assim como seus responsáveis, e analisados, quanto às suas consequências potenciais, probabilidades realísticas e seus níveis de riscos[98].

Em caráter exemplificativo, a norma 27001 relaciona os riscos às dimensões da qualidade de dados, tais como a perda de confidencialidade, integridade e disponibilidade da informação[99].

Podemos então fazer um comparativo entre os riscos e a qualidade de dados, a confidencialidade dos dados, a integridade dos dados e a sua disponibilidade. Sendo assim, o risco é aquilo que pode afetar quaisquer uma dessas esferas durante o tratamento do dado.

2.1.5.2.1. Relatório de Impacto a Proteção de Dados

Um segundo aspecto presente na LGPD e tratado pelo conjunto de normas ISO 27001/27701 é a gestão de riscos. Alguns artigos da lei chegam a definir documentos e mecanismos a serem produzidos ou adotados que comprovam a adoção de práticas de

[96] *Ibidem*
[97] *Ibidem*.
[98] *Ibidem*
[99] *Ibidem*

gestão de riscos. Um desses documentos é o Relatório de Impacto a Proteção de Dados Pessoais (RIPD)[100].

O art. 10 §3º e no art. 38 da LGPD a norma determina que a Autoridade de Proteção de dados pode solicitar aos controladores e operadores a apresentação ou elaboração de um RIPD. A Lei assim define:

> "Art. 5º Para os fins desta Lei, considera-se:
> [...]
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco"[101]

Sendo assim, o RIPD, explicam Frazão, Carvalho e Milanez, nada mais é do que uma documentação do controlador que contém a descrição do processo de tratamento de dados que podem gerar riscos aos direitos e segurança do titular, bem como às liberdades civis e aos direitos fundamentais desses sujeitos ao mesmo tempo em que delimita quais ações de mitigação estão sendo tomadas para proteger esses dados[102].

Em princípio, explicam os autores, esse documento está sujeito à discricionariedade do controlador, salvo quando a ANPD previr sua obrigatoriedade[103]. Ainda assim, é recomendada a sua adoção quando o tratamento de dados evidentemente representa um risco ao titular, como é o caso de coleta de biometria e reconhecimento facial.

O Relatório de Impacto auxilia o agente de tratamento a examinar o risco que um certo tratamento de dados pode gerar ao titular de dados. Nesse sentido, apesar de não ser propriamente um mecanismo de segurança ou prevenção, ele auxilia o agente de tratamento na avalição das melhores medidas que devem ser adotadas para a proteção dos dados conforme a importância da informação protegida.

Para este trabalho, é relevante esse ponto pois, a princípio, para identificar que em atividades de alto risco é esperado que os agentes de tratamento saibam os riscos e possam

---

[100] BRACKETT, M., AND EARLEY, P. S. The DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Estados Unidos: Technics Publications (2009) p. 18

[101] BRASIL. Lei Federal n.º 13,709 de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

[102] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ed. Rio de Janeiro: Forense, 2022. p. 264.

[103] *Ibidem.*

avaliar corretamente como mitigá-los. Isso é particularmente importante ao escopo deste trabalho pois incidentes de segurança envolvendo instituições financeiras são comuns e costumam se repetir em seu *modus operandi*, sendo esperado que essas instituições soubessem como mitigá-los.

Dessa forma, verifica-se ante o exposto neste trabalho até o momento que existe, na legislação e fora dela, tanto sob um aspecto regulatório quanto de boas práticas de mercado, um arcabouço robusto de práticas que visam prevenir e remediar incidentes de segurança.

No próximo capítulo, serão analisadas decisões que partem da alegação, por um titular de dados, de que houve um incidente de segurança (quebra de confidencialidade, acesso indevido, vazamento de dados e etc.) e como os Tribunais tem decidido esses casos quando a parte contrária é uma instituição financeira.

CAPÍTULO 3 | O processo decisório dos Tribunais em face dos incidentes de segurança: A evolução do entendimento dos tribunais sobre LGPD e incidentes de segurança

3.1. Incidentes de segurança em instituições financeiras

Ante a todo o exposto, verifica-se que existe um arcabouço robusto quando se trata de incidentes de segurança. Para além das obrigações legais trazidas pela legislação de proteção de dados, os ditames da segurança da informação e as determinações regulatórias são suficientes para o entendimento de que as informações pessoais, em especial, as informações detidas por instituições financeiras podem representar elevado risco aos interesses e direitos dos titulares e, consequentemente, resultar em dano relevante quando da ocorrência de um incidente de segurança.

As instituições financeiras carregam uma responsabilidade ímpar quando se trata de proteção dos dados dos seus clientes e prevenção de incidentes de segurança. Ocorre que as instituições são detentoras de informações que, ainda que não sensíveis segundo as definições da LGPD, tem o potencial de causar prejuízo material aos titulares.

Já foi abordado anteriormente neste trabalho que os dados financeiros não foram incluídos expressamente na LGPD como dados pessoais, no entanto, a ANPD tem estudado incluí-los como parâmetro para determinação da gravidade do incidente, caso esse evento envolva esse tipo de dado.

Ainda assim, o que se percebe é que organizações, no geral, não tem relegado à segurança da informação o cuidado que deveria ser esperado dela, seja pelo seu porte, tipo de informação tratada ou pela natureza do negócio. Sanches, ao analisar as práticas de compliance por sociedades do "novo mercado", verificou que as sociedades não necessariamente apresentam um nível adequado quando se trata de proteção de dados. O autor argumentou que ainda que pudesse ser alegado que a LGPD estava em período de *vacacio legis* quando foi realizada a pesquisa, muitas das companhias eram multinacionais que já estavam submetidas ao regime do GDPR. Sendo assim, era esperado que esse fato fosse o suficiente para justificar a adoção de boas práticas corporativas para resguardar os direitos do titular de dados pessoais[104].

[104] SANCHES, Alexandre. O Compliance de dados Pessoais das sociedades do "novo mercado". In: PINHEIRO, Caroline da Rosa. Compliance entre teoria e prática: Reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado. Idaiatuba,SP: Editora Foco, 2022. p. 45

Ainda que a adoção de um programa de conformidade interna à LGPD não seja um exercício de *checkbox*, conforme observado em relação ao GDPR por Karen Lawrence em seu livro "*GDPR Compliance is not a tick box exercise"*, o argumento de que as novidades da LGPD ainda não puderam ser implementadas em razão do tempo não se sustenta quando trata-se de instituições financeiras. Antes da regulamentação mais recente tratada neste trabalho, já havia orientações pelo BACEN sobre a adoção de medidas de segurança cibernética. Além disso, as orientações sobre segurança da informação estão disponíveis e os conceitos foram desenvolvidos desde 1960.

Portanto, é esperado que instituições financeiras tenham a capacidade, devido ao seu porte, natureza de negócio e tipos de ativos informacionais, de gerir riscos e proteger os dados pessoais e financeiros de seus clientes.

West notou que, infelizmente, mesmo um setor altamente tecnológico como o bancário ainda vê a segurança como burocracia, despesa supérflua ou entrave para avanços na área da tecnologia[105].

Uma pesquisa realizada pela ANBIMA[106] revelou que 85% das instituições associadas a ela já possuem um programa formal de cibersegurança. Os números refletem um avanço significativo em relação a 2017, quando apenas 71% das empresas afirmaram já ter diretrizes formais. Esse número parece grande, porém, considerando que diretrizes que obrigam as instituições a dotarem de política de segurança cibernética já existiam anteriormente a essa data demonstra um cenário preocupante. Soma-se a isso que a pesquisa não aborda detalhes dos programas de conformidade, apenas a existência de uma política de cibersegurança e sua revisão periódica.

O que se observa é que, em questões de segurança, novas tecnologias e novas ameaças aparecem a todo momento, demandando dos agentes econômicos uma capacidade de resposta a essas alterações[107]. Ainda que a velocidade da inovação não possa ser acompanhada com paridade pelos agentes econômicos, é esperado que o agente

---

[105] WEST, Ethienne Chaves. *Teste de Vulnerabilidade como Ferramenta de Segurança Financeira*. 2019. f. 14 Trabalho de Conclusão do Curso de Especialização em Gestão de Segurança da Informação, da Universidade do Sul de Santa Catarina, como requisito parcial para a obtenção do título de Especialista em Gestão de Segurança da Informação – Unisul.

[106]ANBIMA. *Cibersegurança: Informações sobre segurança cibernética em empresas do mercado financeiro.* Disponível em: https://www.anbima.com.br/pt_br/especial/ciberseguranca.htm. Último acesso: 30 de junho de 2023.

[107] PINTO, Mariana; FRAZÃO, Ana. *Compliance de Dados e Incidentes de Segurança.* In: PINHEIRO, Caroline da Rosa. *Compliance entre teoria e prática: Reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado.* Idaiatuba,SP: Editora Foco, 2022. p. 45

esteja atento e procure cumprir com seu dever de diligência para combater as ameaças que podem afetar o tratamento de dados.

Ainda que se considere que a quantidade diminuta de contornos regulatórios e legais precisos dificulte ou impeça a implementação de um padrão de conformidade para as instituições financeiras, existem outros diplomas legais que aludem a essa obrigação. São eles: a Lei de Sigilo Bancário (Lei Complementar 105/2001); o Código de Defesa do Consumidor[108] (Lei Federal nº 8.078/1990 ou "CDC") e o Marco Civil da Internet[109] (Lei Federal n.º 12.965, 2014 ou "MCI").

O contorno do sigilo de informações financeiras é delimitado pela Lei Complementar 105/2001 (Lei do Sigilo Bancário). Essa lei determina que instituições financeiras devem conservar "operações ativas e passivas e serviços prestados" em sigilo.

A "quebra do sigilo" é, entretanto, autorizada "quando necessária para apuração de ocorrência de qualquer ilícito, em qualquer fase do inquérito ou do processo judicial". Ademais, delimita uma série de atividades que não constituiriam "violação do dever de sigilo": troca de informações cadastrais com outras instituições financeiras, revelação de dados mediante consentimento, e "a comunicação, às autoridades competentes, da prática de ilícitos penais ou administrativos, abrangendo o fornecimento de informações sobre operações que envolvam recursos provenientes de qualquer prática criminosa", entre outras[110].

Importante mencionar que dados sigilosos, segredo e dados pessoais sensíveis não são termos intercambiáveis e não devem ser usados como tal haja vista que dados sensíveis tem definição legal específicas e dados sob sigilo ou segredo não necessariamente precisam ser dados pessoais. Essa diferenciação é importante pois verifica-se uma confusão em relação a esses termos no judiciário e na sociedade em geral.

O Código de Defesa do Consumidor (CDC) estabelece vetores e princípios de proteção ao consumidor e, portanto, acabou concentrando uma grande parte das demandas relacionadas a dados pessoais, que muitas vezes também se caracterizam como relações de consumo, em uma tendência que segue até hoje – a doutrina aponta, inclusive,

---

[108] BRASIL. Código de Defesa do Consumidor (Lei Federal nº 8.078/1990). Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.html . Acesso em 15 de junho de 2023.

[109] BRASIL. Marco Civil da Internet (Lei Federal nº 12.965, 2014). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 15 de junho de 2023

[110] ABREU, Jaqueline de Souza. *Tratamento de Dados Pessoais para Segurança Pública: Contornos do Regime Jurídico Pós-LGPD. In:* BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 15 jun. 2023. p. 590

a possibilidade de que vários dos princípios de proteção de dados possam ser observados a partir do próprio Código de Defesa do Consumidor. Particularmente, explica Doneda, o art. 43 do mencionado Código, que se aplica aos bancos de dados de proteção ao crédito, foi e é largamente utilizado de forma a consolidar o entendimento acerca da existência do direito do consumidor sobre seus dados pessoais de maneira, inclusive, a fomentar outro debate, acerca do registro de dados sobre operações financeiras do consumidor, que acabou canalizado para a edição de legislação específica, a Lei 12.414/2011, conhecida como a Lei do Cadastro Positivo[111].

Como mencionado no Recurso Especial 1.348.532, a partir da exposição de dados financeiros do consumidor abre-se possibilidade para intromissões diversas em sua vida: "Conhecem-se seus hábitos, monitoram-se a maneira de viver e a forma de efetuar despesas"[112]

A Lei Federal n.º 12.965/2014 chamada de Marco Civil da Internet estabeleceu princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Ainda que instituições financeiras não pareçam estar dentro do escopo do Marco, haja vista que não são necessariamente provedores de aplicação ou conexão, elas podem estar sujeitas ao Marco já que a maioria oferece serviços por meio de aplicações na internet.

O MCI estabelece no seu art. 3º, a proteção da privacidade (inciso II), dos dados pessoais (inciso III) e da segurança da rede por meio de técnicas compatíveis com os padrões internacionais e estímulo ao uso de boas práticas (inciso V). O diploma também faz outras menções sobre segurança e sigilo de dados, mas o Decreto 8771/2016, que regulamenta o MCI, apresenta em seu art. 13[113] as diretrizes dos padrões de segurança a

---

[111] DONEDA, Danilo. *Panorama Histórico da Proteção De Dados Pessoais* In: BIONI, Bruno. *Tratado de Proteção de Dados Pessoais*. São Paulo: Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 jun. 2023. p. 22.

[112] STJ. REsp 1.348.532 – SP. Rel. Min. Luis Felipe Salomão. DJe: 30/11/2017.

[113] "Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
I - o estabelecimento de controle estrito sobre o acesso aos dados mediante a definição de responsabilidades das pessoas que terão possibilidade de acesso e de privilégios de acesso exclusivo para determinados usuários;
II - a previsão de mecanismos de autenticação de acesso aos registros, usando, por exemplo, sistemas de autenticação dupla para assegurar a individualização do responsável pelo tratamento dos registros;
III - a criação de inventário detalhado dos acessos aos registros de conexão e de acesso a aplicações, contendo o momento, a duração, a identidade do funcionário ou do responsável pelo acesso designado pela empresa e o arquivo acessado, inclusive para cumprimento do disposto no art. 11, § 3º, da Lei nº 12.965, de 2014 ; e
IV - o uso de soluções de gestão dos registros por meio de técnicas que garantam a inviolabilidade dos dados, como encriptação ou medidas de proteção equivalentes.

serem observados por provedores de aplicação na guarda, armazenamento e tratamento de dados e comunicações privadas.

Montanaro afirma que o ditado popular "não é uma questão de "se" mas de "quando" o incidente vai acontecer" é aplicável aos incidentes de segurança. É o que se chama de "*Assume Breach*" que em português quer dizer assumir que o vazamento ou incidente irá acontecer. Isso porque, no momento de preparar o programa de conformidade e as medidas de segurança, deve ser considerado que o incidente irá a acontecer e o que será feito após a sua ocorrência[114].

Sendo assim, é ideal que as instituições financeiras e instituições no geral adotem o conceito de "*Zero Trust*" que é um modelo desenvolvido por John Kindervag em 2010, enquanto atuava como analista principal da Forrester Research. Segundo esse modelo, uma arquitetura de confiança zero é uma estrutura ampla que promete oferecer proteção eficaz dos ativos mais valiosos de uma organização. Funciona a partir do pressuposto de que cada conexão e *endpoint*[115] representam uma ameaça. O a estrutura de gerenciamento de risco deve proteger contra essas ameaças, sejam internas ou externas, mesmo que as conexões já tenham sido estabelecidas.

Em poucas palavras, uma rede *zero trust*: (i) registra e fiscaliza todo o tráfego da rede corporativa; (ii) limites e controles de acessar à rede; (iii) verifica e protege os recursos de rede. Esse modelo se refere primordialmente interno, ou seja, de uma rede corporativa. No entanto, esses mesmos conceitos podem ser aplicados também a arquitetura voltada para proteger os dados dos titulares, haja vista que eles também estão

---

§ 1º Cabe ao CGIbr promover estudos e recomendar procedimentos, normas e padrões técnicos e operacionais para o disposto nesse artigo, de acordo com as especificidades e o porte dos provedores de conexão e de aplicação.
§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014 , os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
I - tão logo atingida a finalidade de seu uso; ou
II - se encerrado o prazo determinado por obrigação legal." BRASIL. Decreto n.º 8771,2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/decreto/d8771.htm . Acesso em: 15 de junho de 2023.

[114] MONTANARO, Domingo. *Pelo amor ou pela dor – lições aprendidas pelas instituições brasileiras depois de milhares de incidentes cibernéticos.* In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. *Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética.* 1ª ed. São Paulo: Thomson Reuters Brasil, 2020.

[115] Em termos de desenvolvimento de software, um *endpoint* refere-se a um ponto de extremidade em uma API (Interface de Programação de Aplicativos). É basicamente uma URL específica que representa uma entidade ou uma função em um sistema. Quando você faz uma solicitação HTTP para um *endpoint* específico, você está essencialmente interagindo com um determinado recurso ou realizando uma ação específica. Por exemplo, em uma API de mídia social, você pode ter *endpoints* para obter informações do perfil do usuário, publicar um novo tweet ou buscar os seguidores de um usuário. Mozilla Developer Network (MDN). Endpoint. Disponível em: https://developer.mozilla.org/en-US/docs/Glossary/Endpoint

inseridos nas bases internas dos agentes de tratamento, ainda que sejam acessados fora dela[116].

O que se constata, portanto, é que ainda que não haja orientação específica sobre o tema por parte da ANPD, não faltam parâmetros para balizar um programa de conformidade minimente capaz de proteger os dados pessoais dos titulares e clientes de instituições financeiras.

Nesse sentido, considerando a inevitabilidade de um incidente de segurança e a existência de um arcabouço legal, regulatório e de boas práticas de mercado que estabelecem obrigações às instituições financeiras, faz-se mister analisar os tipos de incidentes que podem ocorrer, e identificar aqueles que tem a tendência de ser mais comuns em instituições financeiras.

Segundo Frazão, Carvalho e Milanez as ameaças mais prováveis à segurança da informação consistem em:

(a) Falhas humanas
(b) Falhas de hardware
(c) Falhas de Software
(d) Obsolescência tecnológica
(e) Ataques externos e software
(f) Qualidade dos serviços empregados
(g) Fenômenos da natureza
(h) Violações de propriedade intelectual
(i) Furto de informações
(j) Invasões físicas
(k) Sabotagem ou vandalismo de estruturas físicas
(l) Sabotagem quanto às informações.

Quando se trata de incidentes de segurança e a definição trazida pela lei e pela Autoridade, verifica-se que o (i) acesso não autorizado[117]; (iii) situação acidental ou ilícita

[116] IBM. O que é zero trust?. Disponível em: https://www.ibm.com/br-pt/topics/zero-trust . Último acesso em: 15 de junho de 2023.
[117] "Quando uma pessoa acessa os dados pessoais sem ter permissão do agente de tratamento para tanto" FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD.* 1ed. Rio de Janeiro: Forense, 2022. p. 378

de alteração[118] e (iii) a situação acidental ou ilícita de comunicação[119] parecem ser os tipos principais de incidentes que as instituições financeiras enfrentam hoje, como se verá nos próximos itens. Isso ocorre porque a grande maioria dos incidentes estudados por este trabalho se originam de uma quebra de confidencialidade dos dados dos clientes das instituições financeiras, de forma que o agente permitiu (ou não foi capaz de impedir) o acesso não autorizado a informações privadas, em especial, financeiras de indivíduos[120].

Sendo assim, verifica-se que a grande maioria dos casos enfrentados no âmbito das instituições financeiras origina-se de fraudes de terceiros. Esses casos são particularmente difíceis porque não é possível confirmar se houve um incidente de segurança na ponta da instituição financeira.

É possível que o terceiro tenha tido acesso às informações do titular por outros meios, como quebra de confidencialidade nos parceiros comerciais da instituição, *e-commerces* que sofreram quebra de confidencialidade, invasão de sistemas ou mesmo informações divulgadas na *dark web*[121]. Ainda assim, a partir do momento em que um terceiro acessa a conta de um titular, há um acesso indevido de dados pessoais e informações protegidas do titular.

Portanto, faz sentido que o titular assuma que a instituição financeira, com a qual ele tem contato próximo em termos de dados financeiros e bancários e a qual reconhece com a controladora desses, seja a responsável por permitir ou deixar de impedir esse acesso indevido aos seus dados pessoais de caráter financeiro ou bancário, assumindo, por vezes, a ocorrência de um vazamento.

Além disso, é natural que o titular também assuma que, ainda que a divulgação dos dados bancários (número de conta, nome completo, senha e outros), ou seja, a causa raiz da fraude, não tenha decorrido da ação direta da instituição, o acesso indevido e a decorrente divulgação indevida dos dados, ocorre no momento em que o fraudador tem acesso à conta bancária do titular para a realização de um empréstimo bancário, por

---

[118] Quando o dado é modificado por pessoas não autorizadas ou, ainda que por pessoas autorizadas, de forma indevida" FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. *Curso de Proteção de Dados: fundamentos da LGPD.* 1ed. Rio de Janeiro: Forense, 2022. p.379

[119] "Quando o dado é transmitido, informado, divulgado, revelado, exposto, difundido acidentalmente ou ilicitamente" *Op. Cit.* p. 379.

[120] *Op. Cit*. p. 379.

[121] "A Dark Web é o coletivo oculto de sites da Internet que só podem ser acessados com um navegador de Internet especializado. Ela é usada para manter atividades anônimas e privadas na Internet, algo que pode ser útil em contextos legais e ilegais. Embora algumas pessoas a utilizem para evitar a censura do governo, sabe-se que ela também é empregada para atividades altamente ilegais." KAPERSKY. O que é a Deep Web e a Dark Web?. Disponível em: https://www.kaspersky.com.br/resource-center/threats/deep-web. Último acesso em: 10 de julho de 2023.

exemplo. Para o titular, é normal assumir que esse momento da fraude também é um incidente de segurança envolvendo suas informações.

Segundo Becker *et. al.* os tipos de fraude podem ser caracterizados como:

> "**1. Fraude de Subscrição:** ocorre quando o fraudador assina um serviço como o usuário legítimo, sem a intenção de pagar pelo uso;
>
> **2**. **Fraude de Intrusão:** ocorre quando o fraudador consegue acesso a uma conta outrora legítima e assina serviços através dela. Difere-se da anterior porque o usuário legítimo pode estar consumindo os serviços legítimos de forma simultânea à intrusão;
>
> **3. Fraudes baseadas em lacunas tecnológicas**: geralmente envolve a exploração de uma má configuração de um serviço tecnológico como uma senha inadequada ou sistemas de defesa permissivos;
>
> **4. Engenharia Social:** ocorre em contraponto à exploração de lacunas tecnológicas, sondando a interação humana, convencendo as pessoas que operam os sistemas a flexibilizar controles e regras de segurança;
>
> **5. Fraudes baseadas em novas tecnologias:** ocorre quando os fraudadores exploram o desconhecimento de suas vítimas de tecnologias recentes, obtendo vantagem da ignorância de suas vítimas;
>
> **6. Fraudes baseadas em novas regulações:** por vezes, regras e normas que buscam a igualdade e justiça acabam sendo exploradas por fraudadores para obter vantagens (em sua maioria, econômicas);
>
> **7. Fraude de identidade de usuário:** representada como o roubo de perfis em redes sociais, cópias de números de cartão de crédito, clonagem de chip da telefonia móvel, hackeamento de sistemas de identificação biométricas ou qualquer artifício que possibilite o fraudador simular a identidade de um usuário legítimo"[122]

As fraudes bancárias costumam se encaixar nas hipóteses 1, 2, 4 e 7. Em geral, o fraudador consegue acesso à conta bancária já existente de uma pessoa ou cria uma conta passando-se pelo titular e utiliza-a para a contratação de empréstimo. Ainda, uma fraude comum relacionada à Engenharia Social (item 4) refere-se ao "golpe do motoboy" que consiste em convencer a vítima a entregar seu cartão de crédito, fazendo-a acreditar que o solicitante da ação é a própria instituição financeira, em razão da detenção de informações que, no entendimento do titular de dados, deveriam ser de conhecimento

[122] CARVALHO, A. P. (2021). *Proposta de um Framework de Compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): Um estudo de caso para prevenção a fraude no contexto de Big Data.* Dissertação de Mestrado Profissional, Publicação: PPEE.MP.012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 200 p.

apenas da instituição financeira como: nome completo, número do cartão de crédito, número de Cadastro de Pessoa Física ("CPF") e outras.

O titular que sofre dano, como parte vulnerável da relação, precisa procurar reparação no judiciário, haja vista que a reparação à pessoa física não cabe à Autoridade Nacional de Proteção de Dados. O judiciário, no entanto, vê-se na posição de precisar decidir em meio à novidade da LGPD, sem ter de forma fácil todos os parâmetros para análise sob a ótica de proteção de dados.

Explica Carneiro que, após a chegada da pandemia do Covid-19, foi vista uma quantidade grande de processos judiciários envolvendo golpes de toda espécie, tais como: golpe do Pix, golpe do motoboy, golpe do QRcode, além de empréstimos bancários, compras de automóveis e até mesmo, aquisição de imóveis envolvendo transações fraudulentas. Observa Carneiro que nos golpes citados acima, pode-se observar frequentemente a alegação de "vazamento de dados bancários ou facilitação da empresa" devido a alegada fragilidade bancária, como também se verá na análise de casos abaixo[123].

O judiciário é então incumbido da função de decidir esses casos, sob a alegação de incidente de segurança. No entanto, nota-se uma falta de critério para as avaliações desses casos, lacuna que deve ser preenchida pela jurisprudência e doutrina.

Ainda que exista um debate sobre a existência ou não de incidente de segurança neste caso, é razoável supor que o titular assumirá que o incidente ocorreu já que não tem conhecimento de como essas informações poderiam ter chegado ao fraudador, haja vista que são, em sua visão, detidas apenas pela instituição financeira. Sendo assim, ainda que de forma não expressa, o titular assume que houve uma quebra de confidencialidade ou, ainda, de integridade dos dados.

O objetivo deste trabalho não é debater, neste momento, se essas situações são ou não são incidentes de segurança ou, ainda, se são passíveis de responsabilização por parte do controlador. No entanto, ainda que para afastar a ocorrência do incidente ou da própria aplicação da LGPD do caso concreto, é necessária a análise desses questionamentos, mesmo que de forma superficial.

Segundo, Menke e Goulart um incidente pode causar uma série de danos extrapatrimoniais, em razão da sensação de medo e receio em face da divulgação ou, até mesmo, se se tratar de dados sensíveis, o vazamento pode constituir também uma violação

[123] CARNEIRO, Luana Cruz. *Aplicação da LGPD em contratos bancários envolvendo fraudes?*. MIGALHAS, 2022. Disponível em: https://www.migalhas.com.br/depeso/370163/aplicacao-da-lgpd-em-contratos-bancarios-envolvendo-fraudes. Acesso em: 15 de junho de 2023.

da privacidade e intimidade dos titulares. Já os danos patrimoniais podem acontecer quando terceiros mal-intencionados utilizam os dados para cometimento das mais variadas fraudes, no que se costuma chamar de *identity theft*[124] (ou roubo de identidade, em português). Fato é que não se pode ignorar a alegação de um incidente de segurança, ainda que para rejeitá-la e, mais do que isso, deve haver uma avaliação sob a ótica de proteção de dados, ainda que para afastar a incidência dela.

Sendo assim, falar de prevenção de incidentes de segurança é uma análise casuística, como evidenciado pela própria ANPD ao determinar que nem toda fraude é um incidente. A análise deve ser capaz de avaliar as medidas tecnológicas e organizacionais que, ajustadas ao perfil e ao porte do agente econômico, bem como ao grau de risco que o tratamento realizado pelo seu negócio representa, podem ser consideradas suficientes para prevenção dos riscos aos titulares de dados[125].

E é por esse motivo que se faz mister a análise minuciosa desses casos pelo judiciário para acolher a existência de incidente, afasta-la ou, ainda, afastar a própria aplicação da LGPD.

Portanto, analisar-se-á neste trabalho as decisões proferidas em ações movidas por um titular de dados nas quais há a alegação de vazamento, incidente de segurança ou quebra de confidencialidade, envolvendo instituições financeiras para avaliar a sofisticação da análise dos tribunais neste caso.

O objetivo não é analisar o mérito da decisão sob uma perspectiva de dano, ainda que sejam tecidos comentários sobre a responsabilidade civil originada de um incidente de segurança ao final deste capítulo. O objetivo é analisar tão somente como os tribunais têm tratado a questão, se as discussões apresentadas anteriormente têm sido debatidas pelo judiciário e, se não, se essas decisões têm sido revestidas de maior sofisticação com o passar do tempo de vigência da LGPD e o aumento das lides envolvendo esse tema.

3.2. Análise de casos concretos

[124] MENKE, Fabiano. GOULART, Guilherme Damasio. BIONI, Bruno. *Tratado de Proteção de Dados Pessoais*. São Paulo: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 15 jun. 2023. P. 364.
[125] FRAZÃO, Ana; PINTO, Mariana. *Compliance de Dados e Incidentes de Segurança*, 2022 In: PINHEIRO, Carolina da Rosa. *Compliance entre teoria e prática: reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado*. Indaiatuba,SP: Editora Foco, 2022.P. 40

Por todo o exposto, entende-se que as instituições financeiras, além de estarem sujeitas aos mesmos riscos que quaisquer outros tipos de agente de tratamento, também enfrentam o risco aumentado de dano financeiro direto ao titular de dados.

É por isso que diversas ações são movidas pelos titulares de dados contra instituições financeiras, em especial, bancos e cadastros positivos.

Nesse sentido, esse item examinará um arcabouço de decisões judiciais em segunda instância em que houve alegações de algum tipo de incidente de segurança, sendo considerados os conceitos apresentados neste trabalho.

Em primeiro lugar, será apresentada a metodologia de escolha das decisões para análise. Em seguida, serão analisadas as decisões conforme os critérios estabelecidos na metodologia e, por fim, serão tecidos os comentários acerca da sofisticação das decisões levando em consideração todo o arcabouço de parâmetros apresentado ao longo deste trabalho.

3.2.1. Metodologia de Análise e Escolha de Casos

A metodologia de escolha das decisões utilizou como ponto de partida as pesquisas realizadas pelo Centro de Direito, Internet e Sociedade (CEDIS-IDP) do Instituto Brasileiro de Ensino, Desenvolvimento e Pesquisa (IDP) e o Jusbrasil que elaboraram o *Painel LGPD nos Tribunais*, que consiste em uma seleção das mais importantes decisões judiciais que envolvem a Lei Geral de Proteção de Dados (Lei nº 13.709/18). A parceria deu-se no âmbito do IDP Privacy Lab, um projeto que visa promover estudos avançados sobre Proteção de Dados e Direitos Fundamentais[126].

O tema central do projeto é a análise da jurisprudência sobre LGPD no primeiro ano de vigência da Lei e no segundo ano de vigência da Lei. Por sua vez, este trabalho utilizou a amostra inicial desses dois anos de pesquisa a fim de selecionar as decisões que envolviam instituições financeiras e alegações de vazamento de dados ou incidentes de segurança.

A escolha por utilizar as pesquisas do grupo resulta da impossibilidade, em razão do tempo e do volume de decisões, de realizar uma pesquisa exploratória completamente independente.

Sendo assim, na pesquisa relativa ao primeiro ano de vigência da LGPD, a análise dos casos por parte do Privacy Lab partiu da filtragem do banco de decisões da Jusbrasil

[126] PRIVACY LAB. Painel LGPD nos Tribunais. Disponível em: https://painel.jusbrasil.com.br/. Último acesso: 30 de junho de 2023.

que, com sua tecnologia, identificou aquelas que contemplavam os assuntos: LGPD; Lei Geral de Proteção de Dados Pessoais; Lei Geral de Proteção de Dados; e Lei 13.709. Após a aplicação desse filtro foram encontradas 584 (quinhentas e oitenta e quatro) decisões, publicadas entre setembro de 2020 e agosto de 2021[127].

Em seguida essas decisões foram analisadas qualitativamente pelos pesquisadores do IDP PrivacyLab, conforme os filtros definidos pelo grupo e acessíveis por meio do Painel LGPD nos Tribunais. Desse montante, os pesquisadores encontraram **274 decisões** que efetivamente aplicam a LGPD, nos seus mais diversos aspectos.

Este trabalho analisou, desse montante, todas as 274 decisões e filtrou delas as principais decisões nas quais as partes eram um titular de dados pessoais e uma instituição financeira (bancos, cadastros positivos ou administradoras de crédito).

No segundo ano de pesquisa do Privacy Lab, entre setembro de 2021 e setembro de 2022, foi identificado o total de 1789 documentos com menção ao tema utilizando os mesmos filtros do primeiro ano. No entanto, em seu segundo ano de atuação, o Painel LGPD nos Tribunais desenvolveu 5 (cinco) critérios de relevância, para permitir uma identificação aprimorada pelos pesquisadores sobre a qualidade dos documentos encontrados. A saber: (0) não é decisão judicial; (1) não possui relação com a LGPD; (2) apenas menciona a LGPD; (3) a LGPD é debatida de forma importante, mas não é o ponto central do caso; (4) a LGPD é a questão central do caso. Foram colacionadas ao Painel todas as 629 decisões de nível 3 (debate importante, mas não central sobre a LGPD) e nível 4 (em que a LGPD é a questão central) que foram identificadas pelos pesquisadores.

Dessas 629 decisões, foram utilizados os filtros por problema disponíveis no painel: (i) incidente de segurança; (ii) responsabilidade civil e (iii) as combinações disponíveis com incidente de segurança[128]. Depois disso foram excluídas todas as

[127] PRIVACY LAB. Painel LGPD nos Tribunais 2021. Disponível em: https://painel.jusbrasil.com.br/2021. Último acesso: 30 de junho de 2023.

[128] (i) incidente de segurança e responsabilidade civil; (ii) incidente de segurança, princípios; (iii) incidente de segurança, responsabilidade civil, tratamento; (iv) incidente de segurança, princípios, responsabilidade civil, tratamento; (v) incidente de segurança, princípios, responsabilidade civil; (c) base legal, incidente de segurança, responsabilidade civil; (vii) base lega, incidente de segurança; (viii) incidente de segurança, tratamento; (ix) base legal, incidente de segurança, princípios, responsabilidade civil; (x) incidente, princípios, responsabilidade civil, medidas de segurança [...], tratamento; (xi) base legal, incidente, princípios; (xii) base legal, incidente, tratamento; (xiii) incidente de segurança, princípios, tratamento; (xiv) incidente de segurança, medidas técnicas[...]; (xv) base legal, incidente de segurança, responsabilidade civil, medidas técnicas [...], tratamento; (xvi) autodeterminação, incidente de segurança, perfil, princípios, tratamento; (xvii) discriminação incidente de segurança; (xviii) discriminação, incidente de segurança, responsabilidade civil; (xix) autodeterminação; base legal; incidente de segurança, responsabilidade civil, tratamento; (xx) base, incidente de segurança, princípios, tratamento; (xxi) base legal, incidente de segurança, RIPD; (xxii) base legal, incidente de segurança responsabilidade civil, tratamento; (xxiii)

decisões que se referiam a Tribunais Regionais do Trabalho (TRTs); Tribunais Regionais Federais (TRFs), Tribunais Regionais Eleitorais (TREs) e do Superior Tribunal de Justiça (STJ), restando apenas decisões em segunda instância dos Tribunais de Justiça (TJs) de diversos Estados, contabilizando 148 decisões. Dessas, foram excluídas as decisões que não se referiam a instituições financeiras.

No total, as decisões filtradas totalizaram 38 (trinta e oito), sendo esse o montante de decisões analisadas neste trabalho. Dessas 21 (vinte e uma) decisões foram julgadas em 2021 e 17 (dezessete) em 2022[129].

Haja vista a mudança de metodologia de seleção do Privacy Lab entre o primeiro e o segundo ano, faz-se a ressalva, neste trabalho, que as decisões escolhidas não contemplam a totalidade das decisões sobre o assunto. No entanto, entendemos que este trabalho fornece um panorama suficiente para uma discussão inicial sobre o tema de incidentes de segurança em instituições financeiras.

3.2.2. Análise das Decisões

3.2.2.1. Decisões proferidas em 2021

Foram encontradas, como mencionado no item anterior, 21 (vinte e uma) decisões que foram julgadas e publicadas no ano de 2021.

Dessas, 14 (quatorze) relacionavam-se com um suposto compartilhamento indevido de dados pessoais e inscrição indevida no cadastro positivo. A maioria dessas decisões eram ajuizadas contra securitizadoras de crédito e uma delas foi ajuizada diretamente contra a Serasa. Essas ações se referiam a um suposto compartilhamento indevido de dados e não se encaixavam nas noções de incidente de segurança adotadas por este trabalho, sendo mais pertinentes sob um ponto de vista de direitos dos titulares e de transparência, haja vista que a lide girava em torno da cobrança de débito por controlador legítimo, mas não informado ao titular no momento da contração da dívida.

autodeterminação, base legal, incidente de segurança, perfil, princípios, responsabilidade civil; (xxiv) base legal, incidente de segurança, princípio, responsabilidade civil, sanção administrativa; (xxv) base legal; incidente de segurança, princípios, RIPD, responsabilidade civil, tratamento; (xxvi) base legal, incidente de segurança, medidas técnicas [...]; (xvii) incidente de segurança, responsabilidade civil, sanção administrativa; (xvii) base legal, incidente de segurança, princípios, responsabilidade civil, medidas técnicas [...]; (xviii) incidente de segurança, responsabilidade civil, medidas técnicas [...], transferência internacional; (xxix)base legal, incidente de segurança, princípios, medidas técnicas [...]; (xxx) base legal, incidente de segurança, princípios, responsabilidade civil, medidas técnicas [...], tratamento; (xxxi) base legal, incidente de segurança, princípios, responsabilidade civil e tratamento.

[129] Todas as decisões analisadas foram acostadas ao Anexo deste trabalho.

Sendo assim, essas decisões não foram consideradas relevantes para o escopo deste trabalho.

Além delas, 2 (duas) ações foram ajuizadas pelo Ministério Público contra plataformas de cadastro positivo, fugindo ao escopo deste trabalho, já que se concentra a atenção em ações ajuizadas por titulares de dados.

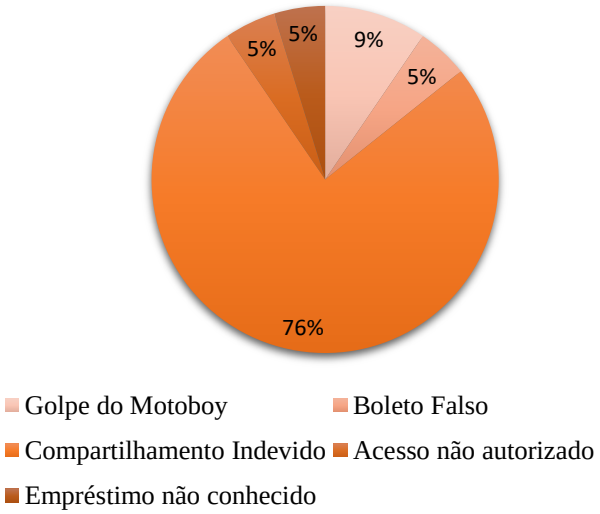
Essas duas categorias de ações anteriormente detalhadas serão nomeadas de "Compartilhamento Indevido" e serão excluídas da análise.

Outras, 4 (quatro) decisões estavam relacionadas com fraude de terceiros, sendo 2 (duas) relacionadas ao "golpe do motoboy", 1(uma) relacionada ao "golpe do boleto falso" e 1 (uma) relacionada a abertura de conta e empréstimo não conhecido tomado por terceiros.

Por fim, 1 (uma) ação foi ajuizada em razão de um acesso indevido por terceiros, sem a posse de cartões ou celular da vítima, à conta da parte autora e realização de pagamentos indevidos sem seu conhecimento. No entanto, não ficou comprovado que esse terceiro tenha sido um invasor remoto ou *hacker*. Apenas essas 5 (cinco) decisões serão consideradas para a análise, pois encaixam-se no escopo deste trabalho.

Ressalta-se que 100% das decisões consideradas válidas para a análise consistiam em lides envolvendo instituições bancárias.

Gráfico 1: Decisões envolvendo "Incidentes" em 2021



Das cinco decisões consideradas para análise, apenas uma não menciona expressamente a LGPD. Essa decisão, ainda que sem mencionar a legislação de proteção

de dados, menciona o dever de reparação em razão do não cumprimento de um dever de proteção aos dados do autor. No entanto, não menciona de onde se origina esse dever ou de que forma é aplicável ao caso concreto.

Duas decisões mencionam a LGPD brevemente, sem qualquer elaboração sobre o tema:

> "Nessa esteira, constata-se que os transtornos refugiram do mero aborrecimento, observando-se, além da perda de tempo útil para evitar que o fraudador realizasse transações, mas também falha na proteção de dados pessoais e de sigilo, ao permitir de terceiros tivessem acesso ao cadastro do correntista, em total infringência ao disposto na Lei Geral de Proteção de Dados e no Marco Civil da Internet, leis nº 12.965/2014 e 13.709/2018"[130]

> "A responsabilidade do banco recorrente decorre da falha na prestação de serviços à recorrida, o que restou devidamente comprovado nos autos. O recorrente não forneceu a segurança necessária no âmbito da relação havida entre as partes para evitar que fraudes como essa viessem a acontecer. Isto em razão de que os golpistas possuíam informações de caráter sigiloso da recorrida (nome, telefone, dados bancários). Pode-se afirmar, neste aspecto, que houve violação das normas da Lei Geral de Proteção de Dados (especialmente arts. 2º, 6º, I, 7º e 8º) o que implica, também por este prisma, a configuração do ato ilícito e da responsabilidade da instituição financeira"[131]

Constata-se que há uma indefinição sobre o que seria a violação à legislação de proteção de dados e, ainda, a indiferenciação entre dados pessoais e dados sigilosos. No entanto, em ambas as decisões, as considerações sobre a LGPD não foram importantes para a decisão de mérito, que foi tomada em função do art. 14 do CDC e da Súmula 479 do STJ[132].

As outras duas decisões dedicam um pouco mais de cuidado à análise dos aspectos de proteção de dados:

> "A Lei 13.709/2019, Lei Geral de Proteção de Dados Pessoais, que regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o

[130] BRASIL. TJ-SP - AC: 10242857020198260003 SP 1024285-70.2019.8.26.0003, Relator: Carlos Abrão, Data de Julgamento: 20/04/2021, 14ª Câmara de Direito Privado, Data de Publicação: 20/04/2021
[131] BRASIL. TJ-SP - RI: 00009688420208260016 SP 0000968-84.2020.8.26.0016, Relator: Tonia Yuka Kôroku, Data de Julgamento: 17/11/2021, Segunda Turma Cível, Data de Publicação: 17/11/2021
[132] "As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias."

> objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, em seu artigo 42, prevê que: "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". Além disso, na mesma norma legal, é previsto hipóteses de exclusão da responsabilidade (artigo 43 e seguintes) além de tratar sobre hipóteses de irregularidade no tratamento de dados pessoais.
>
> Pelo que se tem dos autos, revela-se que, de fato, houve falha na segurança bancária do recorrente réu. Explica-se. Houve três bloqueios de compras no valor de R$ 50,00 no dia dos fatos, em tentativa realizadas por terceiros, e, em seguida, na tentativa de compra de R$ 3.000,00 não houve o bloqueio, sendo todas compras no mesmo estabelecimento."[133]

Verifica-se que essa decisão faz considerações um pouco mais detidas sobre o dever de diligência do controlador e sobre a possibilidade de responsabilização deste. No entanto, a decisão de mérito ainda é realizada com base do CDC, sendo desconsiderada a LGPD ainda que reconhecida a possibilidade de responsabilização em função dela.

> "Ressalta-se que em razão da gravidade dos fortuitos que envolvem vazamentos de dados que a Lei n.º 13.709/2018, a chamada LGPD, estabelece práticas mínimas de segurança a pessoas naturais ou jurídicas que realizem operações de tratamento de dados.
>
> É prevista, a partir disto, a responsabilidade do agente que, em razão da não observância dos parâmetros de segurança, causar dano a outrem:
>
> Art. 44. 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, consideradas as circunstâncias relevantes, entre as quais:
>
> I - o modo pelo qual é realizado;
>
> II - o resultado e os riscos que razoavelmente dele se esperam;
>
> III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
>
> Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."[134]

[133] BRASIL. TJ-DF 07155856320208070007 DF 0715585-63.2020.8.07.0007, Relator: ARNALDO CORRÊA SILVA, Data de Julgamento: 22/11/2021, Segunda Turma Recursal, Data de Publicação: Publicado no DJE : 01/12/2021 . Pág.: Sem Página Cadastrada.

[134] BRASIL. TJ-BA - APL: 80252764420218050001, Relator: JOANICE MARIA GUIMARAES DE JESUS, TERCEIRA CAMARA CÍVEL, Data de Publicação: 17/12/2021

Essa decisão também é importante pois refere-se especificamente à segurança que o controlador deve adotar em relação aos dados pessoais do titular. A menção ao artigo 44 é um passo a frente quando se trata de situações em que pode ter ocorrido um incidente de segurança. Ainda assim, essa também foi uma lide no qual o mérito foi decidido com base no CDC.

3.2.2.2. Decisões proferidas em 2022

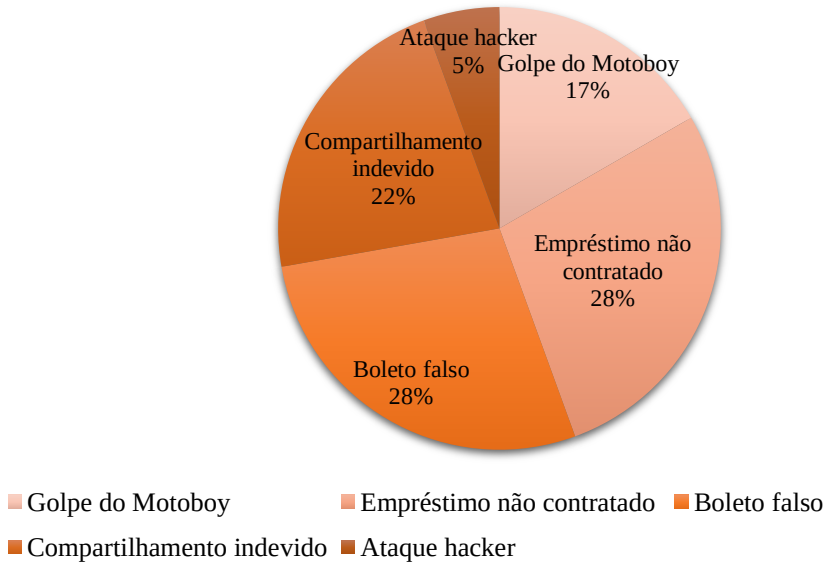
Em 2022, foram identificadas 18 ações pertinentes ao escopo deste trabalho, conforme critérios definidos na metodologia.

Dessas, 13 (treze) decisões estavam relacionadas à fraude de terceiros, sendo 3 (três) relacionadas ao "golpe do motoboy", 5 (cinco) relacionadas ao "golpe do boleto falso" e 5 (cinco) relacionadas a abertura de conta e empréstimo não conhecido tomado por terceiros. Além dessas, 1 (uma) decisão refere-se a um ataque *hacker* configurando um incidente de segurança confirmado pela própria instituição.

Quatro decisões estavam relacionadas com compartilhamento indevido e inscrição em cadastros de proteção ao crédito, e foram desconsideradas do escopo deste trabalho, seguindo o padrão das decisões analisadas referentes ao período de 2021.

Novamente, a maioria das decisões refere-se a instituições bancárias.

Gráfico 2: Decisões envolvendo "Incidentes" em 2022



Constata-se, mais uma vez, que há uma indefinição sobre o que seria a violação à legislação de proteção de dados e, ainda, uma ocasional indiferenciação entre conceitos. No entanto, verifica-se alguns avanços de sofisticação nas decisões dos tribunais:

> "A Lei nº 13.709/2018 Lei Geral de Proteção de Dados, ainda que não qualifique os dados documentais, a priori, como "sensíveis", a teor de seu artigo 5º, II, (dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural) disciplina, como fundamento da proteção dos dados pessoais" a inviolabilidade da intimidade, da honra e da imagem", em seu artigo 2º, IV. Como os dados utilizados pelo fraudador são concernentes à esfera íntima do autor e estavam sob estrita guarda do réu, a responsabilidade civil do banco pelo ocorrido é patente."[135]

Nessa decisão é possível observar a clara diferenciação que o julgador faz em relação a dados sensíveis dos dados documentais do titular e, apesar disso, atribuir importância para fins de responsabilização aos dados documentais do titular, mesmo que não abarcados pela tutela dos dados sensíveis.

> "Logo, restando caracterizada a existência de fraude em nome da autora, em razão de vazamento de dados, resta evidenciado o dever de indenizar, a teor do que dispõem os artigos 42, 44, parágrafo único, e 45, todos da Lei Geral de Proteção de Dados Pessoais (LGPD).
>
> Portanto, considerando o vazamento de dados da autora, que culminou com a contratação indevida, tem-se que, a teor do dispositivo acima transcrito, a responsabilidade do réu/apelado é objetiva, independentemente da existência de culpa."[136]

Neste outro julgado o tribunal também fez considerações sobre a relação entre um suposto vazamento de dados e a responsabilidade do agente, bem como menciona vários dispositivos da LGPD diretamente relacionados com esse problema. Ainda assim, estava ausente a análise casuística e de provas que (i) pudessem comprovar a existência de vazamento bem como (ii) o cumprimento dos princípios de segurança e prevenção e a adoção de medidas capazes de manter os dados pessoais seguros por parte do controlar.

---

[135] BRASIL. TJ-SP - AC: 10052734020218260637 SP 1005273-40.2021.8.26.0637, Relator: César Zalaf, Data de Julgamento: 30/08/2022, 14ª Câmara de Direito Privado, Data de Publicação: 30/08/2022

[136] BRASIL. TJ-MT 10002015920208110044 MT, Relator: SERLY MARCONDES ALVES, Data de Julgamento: 06/04/2022, Quarta Câmara de Direito Privado, Data de Publicação: 07/04/2022

Ainda assim, demonstra-se um maior aprofundamento na questão de segurança e proteção de dados.

> "Vale destacar que, com a vigência da Lei Geral de Proteção de Dados (Lei 13.709/2018), foi explicitada a responsabilidade das instituições financeiras pela proteção aos dados pessoais de seus correntistas.
>
> Desde 2018, o Banco Central já adotara a Resolução nº 4.658, de 26/04/2018, que obriga as instituições financeiras a:
>
> "Art. 2º (...) implementar e manter política de segurança cibernética formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados".
>
> Ademais, os criminosos realizaram várias transações que fogem de seu perfil de cliente e somam a quantia de mais de R$ 50.000,00. A instituição financeira deveria verificar que a compras fugiam do padrão do consumidor e adotar postura no sentido de evitar a ocorrência da fraude, como buscar confirmação das transações perante o cliente ou bloquear o cartão, sendo certo que sua inércia revela seu descontrole na prestação dos serviços."[137]

O julgado acima vai além e passa a considerar até mesmo as disposições específicas de ordem regulatória setorial para balizar o entendimento sobre a obrigação de proteção de dados do agente.

Por fim, na decisão que especificamente trata sobre um ataque *hacker*, como evento confirmado, há até mesmo a determinação de dano *in re ipsa*: "Trata-se de acontecimento que, por si só, causa sofrimento moral no titular dos dados armazenados, razão pela qual dispensa-se a demonstração do dano efetivamente sofrido. Em outras palavras, o dano moral é presumido (*in re ipsa*)"[138], relata o magistrado.

Verifica-se um aumento na sofisticação das decisões se comparadas com as decisões proferidas em um momento anterior de vigência da legislação, também mencionadas neste trabalho, o que parece indicar que o judiciário tem incorporado entendimentos cada vez mais sofisticados sobre o tema. Ainda assim, falta a análise probatória e fática bem como a melhor elaboração sobre a ocorrência de incidentes, para acolher a alegação ou afastá-la.

---

[137] BRASIL. TJ-RJ - APL: 00959893020208190001, Relator: Des(a). CHERUBIN HELCIAS SCHWARTZ JÚNIOR, Data de Julgamento: 03/03/2022, DÉCIMA SEGUNDA CÂMARA CÍVEL, Data de Publicação: 07/03/2022

[138] BRASIL. TJ-SP - RI: 10155178220208260016 SP 1015517-82.2020.8.26.0016, Relator: Gustavo Henrique Bretas Marzagão, Data de Julgamento: 11/04/2022, Quarta Turma Cível, Data de Publicação: 11/04/2022

Portanto, ainda que haja um avanço tímido, há muitas questões a serem dirimidas pela doutrina e pela jurisprudência. O intuito aqui não é confirmar nem negar que essas lides realmente envolviam incidentes de segurança, mas evidenciar que há crescimento, mas também espaço para melhora por parte do judiciário, até mesmo para saber diferenciar incidentes de segurança, de tratamentos ilegais ou irregulares, de lides consumeristas sem relação com a proteção de dados sob a ótica da responsabilização.

3.3. Responsabilização Civil no âmbito da LGPD

É cediço que a violação dos direitos relativos à proteção de dados pessoais provoca repercussões de ordem individual e coletiva de relevantes que não são abarcadas pelo direito administrativo sancionador[139].

Ainda que o objetivo deste trabalho não seja examinar ou fornecer respostas ao problema da responsabilização civil em relação a essa violação, é imprescindível que algumas considerações sobre o tema sejam feitas para o melhor entendimento da importância de uma fundamentação baseada em proteção de dados nas decisões envolvendo incidentes de segurança.

É importante destacar que não é só o incidente de segurança que pode causar dano. Qualquer violação de direitos pode causar dano ao titular, porém o foco deste trabalho é em incidentes de segurança e, portanto, é sobre eles que faremos as considerações neste item.

Segundo Frazão, Carvalho e Milanez, a responsabilidade civil é um conjunto de institutos jurídicos dotados do dinamismo necessário para acompanhar as mudanças provocadas pela intensa utilização de metodologias e técnicas de tratamento de dados[140].

O art. 186 e o art. 927 do Código Civil[141] delineiam a responsabilização civil ao, em termos gerais, determinarem que quem causar dano estará obrigado a ressarci-lo em razão de ter cometido ato ilícito, seja por dolo ou culpa. Afirmam Frazão, Carvalho e Milanez que essa redação é ampla, mas suficiente para endereçar os danos materiais ou

[139] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ª ed. Rio de Janeiro: Forense, 2022.p. 423

[140] *Ibidem* p. 424

[141] "Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito."
"Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo." BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, ano 139, n.

morais que decorrem do tratamento de dados pessoais, mesmo na dificuldade de encontrar diplomas voltados especificamente para a tutela da responsabilização civil relativa ao tratamento dos dados pessoais[142].

A comunidade europeia, que em grande parte possui um mecanismo de responsabilidade civil similar ao brasileiro, optou por determinar que seus integrantes assegurassem que seria cabível a reparação de danos em virtude da violação às normas protetivas dos dados pessoais, garantindo-se também que o responsável pelo tratamento se exima da responsabilidade caso demonstre que o dano não lhe é imputável de forma reprovável, ou seja, que não agiu com **culpa**[143]. Ainda assim, há dissenso em relação a natureza da responsabilidade civil, se objetiva ou subjetiva.

Em que pese esse dissenso, Tepedino, Terra e Guedes afirmam que não faz sentido o legislador criar deveres de cuidado se não para implementar um regime de responsabilidade subjetiva[144]. Se o GDPR é semelhante em linguagem e princípios ao texto da LGPD, faz sentido pensar que também há uma tendência no direito brasileiro de adotar um regime de responsabilidade subjetiva.

A inteligência dos arts. 43 e 44[145] da LGPD são fundamentais para o entendimento da previsão da responsabilidade civil por incidentes de segurança na lei. O art. 43 determina as hipóteses de exclusão de responsabilidade e o art. 44 determina que responde pelos danos decorrentes da violação de segurança quem lhe der causa. Isso é especialmente relevante para os casos envolvendo instituições financeiras pois é difícil (i) confirmar a ocorrência de um incidente e (ii) confirmar se foi realmente a instituição financeira que deu causa ao incidente.

---

[142] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ª ed. Rio de Janeiro: Forense, 2022. p. 425

[143] FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ed. Rio de Janeiro: Forense, 2022.p. 426

[144] TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio. Fundamentos do Direito Civil – Responsabilidade Civil. Rio de Janeiro: Forense, 2021, p. 286.

[145] "Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro."
"Art. 44. 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, consideradas as circunstâncias relevantes, entre as quais:
I - o modo pelo qual é realizado;
II - o resultado e os riscos que razoavelmente dele se esperam;
III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado.
Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."

Por isso, é importante considerar o art. 45[146] do diploma legal que mantém a responsabilidade objetiva nas relações de consumo, já que, na dificuldade de encontrar parâmetros para a responsabilidade subjetiva em proteção de dados, as decisões acabam sendo tomadas em face do direito do consumidor, o que protege os titulares de dados em certa medida, ainda que não diretamente quanto aos seus direitos relacionados à proteção de dados.

A grande questão que permanece em aberto é a identificação do descumprimento do dever que dependerá de matéria probatória em análise casuística já que a ilicitude pode ser constatada a partir do descumprimento dos deveres dispostos na LGPD, ainda que amplos. Porém, se considerada a vulnerabilidade e disparidade informacional dos titulares de dados, bem como a dificuldade de prova de conformidade, essa tarefa torna o trabalho do judiciário difícil. Como se demonstrou neste trabalho, há parâmetros técnicos mais específicos na segurança da informação, bem como regulatórios e legais, mais inespecíficos, que podem balizar essa matéria probatória. No entanto, o titular dificilmente terá a condição informacional de pleitear essas provas, muito menos obtê-las, o que parece inviabilizar a configuração da responsabilidade subjetiva em demandas individuais, que são a maioria das lides, haja vista que demandas coletivas parecem ser mais prováveis em situações de vazamento de dados, propriamente ditas, massivas e amplamente noticiadas, o que não é o caso da maioria das ações.

Sendo assim, este trabalho não tem a intenção de levantar respostas a este ponto, mas é fundamental que essas lacunas sejam endereçadas no futuro para que as decisões tenham condições de serem cada vez mais sofisticadas em termos de mérito, especificamente, quanto à proteção de dados pessoais.

3.4. Incorporação das mudanças trazidas pela LGPD na legislação e regulamentação brasileira de cibersegurança e segurança da informação voltada para o setor financeiro nas decisões dos Tribunais de Justiça.

Conforme o descrito neste trabalho, existem, quando se trata de instituições financeiras, três esferas de lides que aparentemente envolvem incidentes de segurança dentre as decisões analisadas:

[146] "Art. 45. As hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente."

- **Fraudes de Terceiros** (Golpe do Motoboy, Fraude de Boletos, Golpes em geral) que compõe a esmagadora maioria dos casos;
- **Cadastro Positivo e Securitizadoras de Crédito**, com ou sem inscrição indevida dos devedores nos sistemas - uma parcela significativamente menor dos casos e, nos casos analisados por este trabalho, não configuram uma amostra relevante para incidentes de segurança; e
- **Ataques hacker** e vazamentos confirmados de dados e seus desdobramentos - compondo uma quantidade ínfima das decisões, tendo sido identificada apenas um evento confirmado na análise das decisões da amostra.

O que se observa é que a maioria dos casos menciona a LGPD, a maior parte também não elabora ou incorpora quaisquer considerações mais profundas sobre proteção de dados e, mais especificamente sobre incidentes de segurança.

Além disso, há, frequentemente, confusão de conceitos. Sigilo, dados sensíveis, dados pessoais e outros termos acabam sendo utilizados como intercambiáveis.

No entanto, a tendência é que quanto mais perto do final de 2022, menos confusões e mais robustas se tornavam as fundamentações, ainda que de forma lenta e tímida.

Vale ressaltar, que muitos casos conhecidos de incidentes não foram encontrados na amostra analisada para este trabalho. No entanto, alguns breves comentários sobre casos notórios são necessários.

Um exemplo de caso notório de vazamento de dados é, por exemplo, o incidente de vazamento das chaves Pix noticiado em 16 de setembro de 2022 pelo BACEN. Neste incidente, cerca de 137,3 mil chaves Pix de clientes da Abastece Ai Clube Automobilista Payment Ltda. (Abastece Aí) tiveram seus dados vazados. O incidente ocorreu entre 1º de julho e 14 de setembro de 2022 e teria exposto os seguintes dados dos usuários: nome do usuário, Cadastro de Pessoas Físicas (CPF), instituição de relacionamento, agência, número e tipo da conta, data de criação da chave Pix[147].

[147] MÁXIMO, Wellton. Banco Central comunica vazamento de dados de 137,3 mil chaves Pix. Ag~encia Brasil, Brasília, 16 de setembro de 2022. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2022-09/banco-central-comunica-vazamento-de-dados-de-1373-mil-chaves-

Esse evento teria sido o quarto incidente de vazamentos de dados do Pix desde a criação do sistema, em novembro de 2020. Em agosto de 2021, ocorreu o vazamento de dados 414,5 mil chaves Pix por número telefônico do Banco do Estado de Sergipe (Banese). Inicialmente, o BACEN alegou que o vazamento no Banese teria atingido 395 mil chaves, mas o número foi revisado posteriormente[148].

Em 21 de agosto de 2022, 160,1 mil clientes da Acesso Soluções de Pagamento tiveram suas informações pessoais vazadas. Ainda, no início de fevereiro 2022, 2,1 mil clientes da Logbank pagamentos também tiveram dados expostos[149].

É interessante verificar que, ainda que julgados sobre esses eventos não tenham aparecido nas amostras analisadas, esses eventos também ensejaram litigância no judiciário, no entanto, apesar da confirmação do incidente pelo BACEN, foram encontradas decisões em que a proteção de dados pessoais não é mencionada em momento algum na decisão:

> "Conforme demonstrado anteriormente, tem-se que houve conduta ilícita por parte da instituição financeira, haja vista ter sido negligente ao permitir que terceiro fraudador obtivesse dados pessoais da parte autora, efetuado ligação telefônica solicitando dados bancários para implementar a fraude bancária[150]"

No entanto, a Relatora do caso categoricamente afirma que houve culpa da instituição financeira, neste caso, ao permitir acesso do terceiro aos dados do titular, em razão de vazamento confirmado. Sendo assim, há o reconhecimento pelo juízo de que teria havido um incidente. Ainda assim, o direito à proteção de dados ou qualquer menção à responsabilização em razão da negligência, sob uma ótica de proteção de dados, não são mencionados como fundamentação no acórdão.

O caso citado não se propõe paradigma e este trabalho não analisou as hipóteses desses casos em específico, porém uma análise pormenorizada desses casos poderia complementar os achados deste trabalho no futuro.

No entanto, ainda neste caso, a consideração sobre o vazamento dos dados ou a responsabilidade da instituição sobre essa quebra de um dever de diligência não é aprofundada.

---

pix#:~:text=Cerca%20de%20137%2C3%20mil,pagamentos%2C%20em%20novembro%20de%202020. Último acesso em: 28 de junho de 2023

[148] *Ibidem*

[149] *Ibidem*

[150] BRASIL. TJ-SE - AC: 00293338920218250001, Relator: Iolanda Santos Guimarães, Data de Julgamento: 17/11/2022, 1ª CÂMARA CÍVEL

CONCLUSÃO

Após a análise das decisões apresentadas neste trabalho, verifica-se que o judiciário tem avançado quando se trata de sofisticação nas decisões relacionadas a incidentes de segurança. No entanto, a velocidade do avanço é insuficiente.

Conforme afirmado neste trabalho[151], o fator humano é a maior causa de incidentes de segurança da informação. Uma das causas da ocorrência de incidentes de segurança é também a inação do componente humano das organizações ao deixar de relegar a devida importância à segurança da informação e à proteção de dados.

A todo momento surgem no mundo da tecnologia novas ameaças que põem os direitos dos titulares em riscos e seus dados fora da margem de segurança. Quando se trata das instituições financeiras, se a proteção do titular não for adequada os resultados de um incidente de segurança podem ser catastróficos.

Ainda que seja possível alegar que os parâmetros decisórios para casos envolvendo incidentes de segurança não possuem contornos bem definidos, há, como demonstrado no presente trabalho, requisitos de segurança a serem observados desde 1970. Sendo assim, problemas já conhecidos como a vulnerabilidade da estrutura de senhas, a falta de procedimentos de segurança para conexões, a inexistência de identificação de usuários e de autorizações[152] já deveriam estar mapeados como risco e alvos conhecidos de agentes maliciosos.

As instituições financeiras têm o dever de implementar e manter uma política de segurança cibernética e, consequentemente uma estrutura de governança de dados, formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados. Além disso, há a obrigação regulatória de que o nível de complexidade que a Política de Segurança Cibernética deve obedecer deve levar em conta as características particulares de cada uma das instituições, sendo relevantes para tanto: (i) o porte, perfil de risco e modelo de negócios da instituição; (ii) a natureza das operações a complexidade dos produtos, serviços, atividades e processos da instituição; e (iii) a sensibilidade dos dados e das informações sob responsabilidade da instituição.

---

[151] MITNICK, Kevin, D.; SIMON, Willian L. Mitnick. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Makron Books, 2003.
[152] *Ibidem*

Ainda assim, nenhum desses aspectos é levado em consideração até o momento para entender se houve o cumprimento do dever de diligência das instituições financeiras.

Portanto, para que a discussão sobre a existência de responsabilidade civil originada por incidentes de segurança envolvendo dados pessoais possa avançar para além de outras esferas do direito, como a consumerista, é preciso começar a analisar essas alegações de forma mais profunda, sob a ótica das evidências do cumprimento do dever de diligência que já existe, ainda que sem os contornos precisos.

Vale ressaltar que o judiciário enfrentava essas lides antes da vigência da Lei Geral de Proteção de Dados. As lides eram majoritariamente resolvidas com base no Código de Defesa do Consumidor e, até aquele momento, as soluções eram satisfatórias. No entanto, com a vigência da legislação de proteção de dados, há todo um arcabouço de direitos que extrapolam o direito do consumidor e situações que antes não eram discutidas haja vista que não eram legalmente disciplinadas, hoje possuem relevância jurídica e devem ser enfrentadas para que haja uma efetiva solidificação dos direitos dos titulares de dados pessoais, de forma autônoma, como preconiza a lei[153].

Como demonstrado, não são poucos os parâmetros de segurança considerados como requisito, tanto pela legislação de proteção de dados, quanto pela segurança da informação como prática de mercado. Sendo assim, não estão ausentes os parâmetros de análise técnica, como subsídio para a análise legal.

As instituições financeiras, em particular, são alvos frequentes de ataques, golpes e outras formas de violações ou tentativa de violação de dados financeiros e dados pessoais. Essas instituições também estão constantemente inovando em termos de tecnologia, haja vista que promover facilidades ao cliente, por meio da tecnologia, costuma ser um atrativo relevante para esse segmento. Sendo assim, tecnologias como o *open banking ou open finance*[154], identificação biométrica e reconhecimento facial,

[153] "Art. 64. Os direitos e princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte."

[154] "O *open finance*, ou sistema financeiro aberto, é a possibilidade de clientes de produtos e serviços financeiros permitirem o compartilhamento de suas informações entre diferentes instituições autorizadas pelo Banco Central e a movimentação de suas contas bancárias a partir de diferentes plataformas e não apenas pelo aplicativo ou site do banco, sendo que o *open finance* é uma versão ampliada do *open banking"* BRASIL. Banco Central do Brasil . Open Finance. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/openfinance. Último acesso em: 10 de julho de 2023.

criptografia[155], instituições inteiramente digitais e a facilidade da interconexão de serviços complexificam o cenário e demandam uma segurança robusta. É por isso que se espera das instituições financeiras um elevado nível de segurança que, talvez, seja particular do seu modelo de negócios.

Ainda assim, o judiciário não tem se detido sobre o assunto de maneira contundente e decidido de forma a criar um lastro jurisprudencial que seja suficiente para debater o conceito de incidentes de segurança e seus meios de prova, quanto mais as especificidades de instituições financeiras.

Uma análise menos aprofundada sobre os aspectos da proteção de dados, ainda que em gradual progressão, resulta ultimamente em uma indefinição sobre a responsabilidade civil do controlador em relação ao incidente, já que nem a análise sobre a existência ou inexistência desse incidente tem sido feita.

Sendo assim, o judiciário tem se furtado de munir suas decisões com a robustez necessária para que as discussões de proteção de dados deixem de ser laterais, e passem a figurar em polo de igualdade com a seara consumerista, por exemplo.

Em suma, o judiciário tem avançado na sofisticação de suas decisões sobre esses casos, no entanto, essa sofisticação ainda está longe de alcançar o nível necessário para que haja realmente uma discussão séria sobre a proteção de dados como direito autônomo e, consequentemente, a responsabilização civil por incidentes de segurança.

Portanto, é crucial que o judiciário continue evoluindo, juntamente com os entendimentos sobre a proteção de dados pessoais e da segurança da informação no arcabouço legal e regulatório brasileiro para que a distância entre a inovação e a satisfação das demandas judiciais não seja tão grande a ponto de prejudicar o direito do titular de dados.

[155] "A criptografia é usada para provar a integridade e autenticidade das informações usando o que é conhecido como assinaturas digitais. A criptografia é uma parte essencial do gerenciamento de direitos digitais e proteção contra cópias. A criptografia pode ser usada para apagar dados." KAPERSKY. O que é criptografia de dados? Definição e explicação. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Último acesos em: 10 de julho de 2023.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, Jaqueline de Souza. Tratamento de Dados Pessoais para Segurança Pública: Contornos do Regime Jurídico Pós-LGPD. *In:* BIONI, Bruno. Tratado de Proteção de Dados Pessoais. Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 15 jun. 2023.

ALEXANDRIA, João C. S de. Gestão de Segurança da Informação: uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica. São Paulo, 2009. 193f. Tese (Doutorado em Tecnologia Nuclear) – Universidade de São Paulo, São Paulo, 2009.

BENNETT, Colin; RAAB, Charles D. The governance of privacy: Policy instruments in global perspective. Cambridge : The MIT Press, 2006

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRACKETT, M., AND EARLEY, P. S. The DAMA guide to the data management body of knowledge (DAMA-DMBOK guide). Estados Unidos: Technics Publications , 2009.

CARNEIRO, Luana Cruz. Aplicação da LGPD em contratos bancários envolvendo fraudes?. MIGALHAS, 2022. Disponível em: https://www.migalhas.com.br/depeso/370163/aplicacao-da-lgpd-em-contratos-bancarios-envolvendo-fraudes. Acesso em: 15 de junho de 2023.

CARVALHO, A. P. (2021). Proposta de um Framework de Compliance à Lei Geral de Proteção a Dados Pessoais (LGPD): Um estudo de caso para prevenção a fraude no contexto de Big Data. Dissertação de Mestrado Profissional, Publicação: PPEE.MP.012, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 200 p.

CATELLI, Maria Augusta Peres ; IDIE, Renata Yumi. Prevenir para mitigar: a importância do desenvolvimento de uma cultura de segurança cibernética nas organizações. 2020 In: MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020.

DONEDA, Danilo. Panorama Histórico da Proteção De Dados Pessoais In: BIONI, Bruno. **Tratado de Proteção de Dados Pessoais**. São Paulo: Grupo GEN, 2020. *E-book.* ISBN 9788530992200. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 16 jun. 2023. p. 22.

FRAZÃO, Ana; CARVALHO, Angelo Prata de; MILANEZ, Giovanna. Curso de Proteção de Dados: fundamentos da LGPD. 1ed. Rio de Janeiro: Forense, 2022.

FRAZÃO, Ana; PINTO, Mariana. Compliance de Dados e Incidentes de Segurança, 2022 In: PINHEIRO, Carolina da Rosa. Compliance entre teoria e prática: reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado, 2022. Indaiatuba,SP: Editora Foco, 2022.

HINTZBERGEN, Jule. HINTZBERGEN, Kees; SMULDERS, André ; BAARS, Hans. Fundamentos da Segurança da Informação com base na ISO 27001 e na ISO 27002. Tradução de Alan de Sá. Bransport: Rio de Janeiro, 2018. Edição Biblioteca Pearson

MARCIANO, João Luiz Pereira. Segurança da informação: uma abordagem social. Tese de Doutorado em Ciência da Informação – Universidade de Brasília, 2006.

MASCARENHAS NETO, Pedro Tenório; ARAÚJO, Wagner Junqueira. Segurança da informação: uma visão sistêmica para implantação em organizações. João Pessoa: Editora da UFPB, 2019.

MÁXIMO, Wellton. Banco Central comunica vazamento de dados de 137,3 mil chaves Pix. Ag~encia Brasil, Brasília, 16 de setembro de 2022. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2022-09/banco-central-comunica-vazamento-de-dados-de-1373-mil-chaves-pix#:~:text=Cerca%20de%20137%2C3%20mil,pagamentos%2C%20em%20novembro%20de%202020. Último acesso em: 28 de junho de 2023

MENKE, Fabiano. GOULART, Guilherme Damasio. BIONI, Bruno. Tratado de Proteção de Dados Pessoais. [Digite o Local da Editora]: Grupo GEN, 2020. E-book. ISBN 9788530992200. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9788530992200/. Acesso em: 15 jun. 2023.

MITNICK, Kevin, D.; SIMON, Willian L. Mitnick. **A arte de enganar:** ataques de hackers: controlando o fator humano na segurança da informação. São Paulo: Makron Books, 2003.

MONTANARO, Domingo; GIOVA, Giuliano ; OPICE BLUM, Renato. Cyber Risk: Estratégias nacionais e corporativas sobre riscos e segurança cibernética. 1ª ed. São Paulo: Thomson Reuters Brasil, 2020.

NAKAMURA, Emílio; GEUS, Paulo. Segurança de redes em ambientes corporativos. São Paulo: Berkeley Brasil, 2002.

PELTIER, T. R. Information security policies, procedures, and standards: Establishing an Essential Code of Conduct. USA: Aurebach Publications, 2001.

PINHEIRO, Carolina da Rosa. Compliance: entre Teoria e Prática. Editora Foco, 1ª ed., 2022.

SANCHES, Alexandre. O Compliance de dados Pessoais das sociedades do "novo mercado". In: PINHEIRO, Caroline da Rosa. Compliance entre teoria e prática: Reflexões contemporâneas e análise dos programas de integridade das companhias listadas no novo mercado. Idaiatuba,SP: Editora Foco, 2022.

SÊMOLA, Marcos. Gestão da segurança da informação: uma visão executiva. 2 ed. Rio de Janeiro: Elsevier, 2014.

SOLOV, Daniel J; HARTZOG, Woodrow. BREACHED!: Why data security law fails and how to improve it. Nova Iorque: Oxford University Press, 2022.

TEPEDINO, Gustavo; TERRA, Aline de Miranda Valverde; GUEDES, Gisela Sampaio. Fundamentos do Direito Civil – Responsabilidade Civil. Rio de Janeiro: Forense, 2021

WHITMAN, Michael E ; MATTORD, Herbert J. *Principles of Information Security*. Editora Cengage. 7ª Ed. Boston USA, 2022. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=Hwk1EAAAQBAJ&oi=fnd&pg=PP1&dq=the+origin+of+information+security%22&ots=VirNfOfYMk&sig=eP_5xUio9nT1R7rDQImFd4KA1M0&redir_esc=y#v=onepage&q=the%20origin%20of%20information%20security%22&f=false

REFERÊNCIAS JURISPRUDENCIAIS

BRASIL. TJ-SP - AC: 10242857020198260003 SP 1024285-70.2019.8.26.0003, Relator: Carlos Abrão, Data de Julgamento: 20/04/2021, 14ª Câmara de Direito Privado, Data de Publicação: 20/04/2021

BRASIL. TJ-SP - RI: 00009688420208260016 SP 0000968-84.2020.8.26.0016, Relator: Tonia Yuka Kôroku, Data de Julgamento: 17/11/2021, Segunda Turma Cível, Data de Publicação: 17/11/2021

BRASIL. TJ-DF 07155856320208070007 DF 0715585-63.2020.8.07.0007, Relator: ARNALDO CORRÊA SILVA, Data de Julgamento: 22/11/2021, Segunda Turma Recursal, Data de Publicação: Publicado no DJE : 01/12/2021 . Pág.: Sem Página Cadastrada.

BRASIL. TJ-BA - APL: 80252764420218050001, Relator: JOANICE MARIA GUIMARAES DE JESUS, TERCEIRA CAMARA CÍVEL, Data de Publicação: 17/12/2021

BRASIL. TJ-SP - AC: 10052734020218260637 SP 1005273-40.2021.8.26.0637, Relator: César Zalaf, Data de Julgamento: 30/08/2022, 14ª Câmara de Direito Privado, Data de Publicação: 30/08/2022

BRASIL. TJ-MT 10002015920208110044 MT, Relator: SERLY MARCONDES ALVES, Data de Julgamento: 06/04/2022, Quarta Câmara de Direito Privado, Data de Publicação: 07/04/2022

BRASIL. TJ-RJ - APL: 00959893020208190001, Relator: Des(a). CHERUBIN HELCIAS SCHWARTZ JÚNIOR, Data de Julgamento: 03/03/2022, DÉCIMA SEGUNDA CÂMARA CÍVEL, Data de Publicação: 07/03/2022

BRASIL. TJ-SP - RI: 10155178220208260016 SP 1015517-82.2020.8.26.0016, Relator: Gustavo Henrique Bretas Marzagão, Data de Julgamento: 11/04/2022, Quarta Turma Cível, Data de Publicação: 11/04/2022

BRASIL. TJ-SE - AC: 00293338920218250001, Relator: Iolanda Santos Guimarães, Data de Julgamento: 17/11/2022, 1ª CÂMARA CÍVEL

ANEXO | Tabela de Jurisprudência

NÚMERO DO PROCESSO	TIPO DE INSTITUIÇÃO FINANCEIRA	TIPO DE INCIDENTE	CONFIRMAÇÃO DO INCIDENTE	MENCIONA A LEI GERAL DE PROTEÇÃO DE DADOS (“LGPD”)?	COMO?	MENCIONA O CÓDIGO DE DEFESA DO CONSUMIDOR (“CDC”)?	COMO?	INCLUÍDA NO ESCOPO
RI 0000968-84.2020.8.26.0016 SP 0000968-84.2020.8.26.0016	Banco	Fraude de Terceiros (Motoboy)	Não	Sim (apenas menção)	Lei Geral de Proteção de Dados (especialmente arts. 2º, 6º, I, 7º e 8º)	Sim	Houve efetiva falha na prestação de serviços à consumidora-recorrida. Incide no presente caso o art. 14 do Código de Defesa do Consumidor	**Sim**
APL 50011024720208215001	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Artigo 6º, inciso X, do Código de Defesa do Consumidor.	**Não**
AC 50006565520218210039 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem	**Sim**	Assim, o referido sistema, tal como o "Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em	**Não**

					razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.		verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	
AC 50018730420208212001 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o "Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	**Não**

AC 50337842020208210001 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	**Não**
AC 50007504720208210165 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do	**Não**

							artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	
AC 50064635320208210019 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.		Assim, o referido sistema, tal como o "Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	**Não**
AC 50057138820208210039 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s	Sim	Assim, o referido sistema, tal como o "Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a	

					3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.		determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	
AC 50398069420208210001 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	**Não**
AC 50057181320208210039 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados,	**Não**

					pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.		apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	
AC 50030542120208210035 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a	**Não**

							notificação prévia do consumidor	
AC 50496645220208210001 RS	Cadastro Positivo	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	**Não**
AC 50051757020208210019 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a	**Não**

							observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	
AC 50006582520218210039 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	**Não**
AC 50002130720218210039 RS	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, mesmo que a ré fosse considerada como mero provedor de informações, caso esta não seja fidedigna, responde pelo dado lançado sem razão jurídica, a teor do que estabelece o art. 5º, incisos I e X, combinado	Sim	Assim, o referido sistema, tal como o"Serasa Limpa Nome", não são cadastros ou bancos de dados, apresentando-se, em verdade, no que toca ao primeiro, como um modelo estatístico que	**Não**

					com os artigos 6º, incisos I e V, e 7º, incisos I e X, §s 3º e 5º, e art. 17, todos da lei 13.853/2020 - LGPD.		avalia o risco médio de crédito relativo a determinado conjunto de informações, não sendo pessoal, o que torna dispensável a observância do artigo 43, § 2º, do CDC e do artigo 4º da Lei 12.414/2011, ou seja, desnecessária a autorização e a notificação prévia do consumidor	
ED 0749765-29.2020.8.07.0000 DF 0749765-29.2020.8.07.0000	Cadastro Positivo	Compartilhamento indevido/falta de transparência	Não	Sim	Por sua vez, no que diz respeito à análise do artigo 7º da Lei nº 13.709/2018, e seus incisos e parágrafos, basta a leitura atenta do acórdão para se observar que foram expostas de forma clara as razões pelas quais a tutela recursal foi mantida, tendo o aresto expressamente afastado a tese exposta pela embargante, no sentido de que seria suficiente para a dispensa do consentimento a constatação de que o controlador tem interesse legítimo (artigo 7º, inciso IX) ou que o compartilhamento dos dados tenha finalidade de proteção do crédito (inciso X), ante uma alegada ausência de hierarquia no	Não	N/A	**Não**

					rol de hipóteses do art. 7º da LGPD. Desse modo, e não obstante o esforço argumentativo empreendido, nota-se que a recorrente, sob a pecha de omissão, insiste na reanálise da questão alusiva à ausência de hierarquia no rol de hipóteses do artigo 7º da LGPD, o que desafia recurso próprio.			
RI 0715585-63.2020.8.07.0007 DF 0715585-63.2020.8.07.0007	Banco	Acesso indevido de terceiros (pagamento não conhecido)	Não	Sim	"A Lei 13.709/2019, Lei Geral de Proteção de Dados Pessoais, que regulamenta o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, em seu artigo 42, prevê que: "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado	Sim	A relação jurídica estabelecida entre as partes é de consumo, devendo a controvérsia ser solucionada sob o prisma do sistema jurídico autônomo instituído pelo Código de Defesa do Consumidor (Lei n. 8.078/1990). Conforme Súmula n. 479 do e. STJ: As instituições financeiras respondem objetivamente pelos danos gerados por fortuito interno relativo a fraudes e delitos praticados por terceiros no âmbito de operações bancárias.	**Não**

					a repará-lo". Além disso, na mesma norma legal, é previsto hipóteses de exclusão da responsabilidade (artigo 43 e seguintes) além de tratar sobre hipóteses de irregularidade no tratamento de dados pessoais." "Desse modo, considerando a responsabilidade da instituição bancária e a falha no tratamento de dados pessoais (Art. 42 da Lei 13.708/2019), o dano material é evidente e deve ser estabelecido no valor do prejuízo da parte recorrida, o qual deve ser reparado.			
AI 0749765-29.2020.8.07.0000 DF 0749765-29.2020.8.07.0000	Cadastro Positivo	Compartilhamento indevido/falta de transparência	Não	Sim	Portanto, à luz da LGPD, conforme o artigo 5º acima transcrito, referidos dados não constituem dados sensíveis. Não obstante, o fato de dar tratamento específico aos dados sensíveis não exclui a proteção aos demais dados pessoais, conforme se extrai da interpretação do artigo 7º da LGPD. Com efeito, não há como acolher, como sustenta a agravada, o entendimento de que seria bastante para	Não	N/A	**Não**

					dispensa do consentimento a constatação de que o controlador tem interesse legítimo (artigo 7º, inciso IX) ou que o compartilhamento dos dados tenha finalidade de proteção do crédito (inciso X), ante uma alegada ausência de hierarquia no rol de hipóteses do art. 7º da LGPD.			
RI 0081878-31.2020.8.05.0001	Banco	Fraude de Terceiro (Motoboy)	Sim*	Não (no entanto, menciona a reparação do dano)	N/A	Sim	Art. 14, caput do CDC	**Sim**
AC 1024285-70.2019.8.26.0003 SP 1024285-70.2019.8.26.0003	Banco	Fraude de Terceiro (abertura de conta)	Não	Sim (menção)	N/A	Sim	Art. 14 caput do CDC	**Sim**
APL 8025276-44.2021.8.05.0001	Banco	Fraude de Terceiro (Boleto Falso)	Sim*	Sim	"Ressalta-se que em razão da gravidade dos fortuitos que envolvem vazamentos de dados que a Lei n.º 13.709/2018, a chamada LGPD, estabelece práticas mínimas de segurança a pessoas naturais ou jurídicas que realizem operações de tratamento de dados. É prevista, a partir disto, a responsabilidade do agente que, em razão da não observância dos parâmetros de segurança, causar dano a outrem: Art. 44. O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou	Sim	Art. 14 caput do CDC	**Sim**

					quando não fornecer a segurança que o titular dele pode esperar, consideradas as circunstâncias relevantes, entre as quais: I - o modo pelo qual é realizado; II - o resultado e os riscos que razoavelmente dele se esperam; III - as técnicas de tratamento de dados pessoais disponíveis à época em que foi realizado. Parágrafo único. Responde pelos danos decorrentes da violação da segurança dos dados o controlador ou o operador que, ao deixar de adotar as medidas de segurança previstas no art. 46 desta Lei, der causa ao dano."			
RI 0000903-85.2021.8.05.0001	Banco	Fraude de Terceiro (Boleto Falso)	Não*	Sim	Para além do diploma consumerista, aplicável ao caso concreto, a Lei Geral de proteção de Dados possui aplicação ao caso: Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de	Sim	Art. 14 caput do CDC	**Sim**

					proteção de dados pessoais, é obrigado a repará-lo. [...] Assim, concluo que há, no caso concreto, elementos que evidenciam culpa concorrente de ambas as partes.			
AC 1037949-19.2021.8.26.0224 SP 1037949-19.2021.8.26.0224	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	6º, IX e 7º, X, da Lei nº 13.853/2019	Sim	art. 43, § 5º, do CDC	**Não**
AC 1031994-34.2021.8.26.0506 SP 1031994-34.2021.8.26.0506	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	6º, IX e 7º, X, da Lei nº 13.853/2019	Sim	art. 43, § 5º, do CDC	**Não**
AC 1000752-48.2021.8.26.0024 SP 1000752-48.2021.8.26.0024	Securitizadora de créditos financeiros	Compartilhamento indevido/falta de transparência	Não	Sim	6º, IX e 7º, X, da Lei nº 13.853/2019	Sim	art. 43, § 5º, do CDC	**Não**
AC 1005273-40.2021.8.26.0637 SP 1005273-40.2021.8.26.0637	Banco	Fraude de Terceiro (Empréstimo não contratado)	Não	Sim	A Lei nº 13.709/2018 Lei Geral de Proteção de Dados, ainda que não qualifique os dados documentais, a priori, como"sensíveis", a teor de seu artigo 5º, II, (dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural) disciplina, como fundamento da proteção dos dados pessoais" a	Sim	Art. 14 do CDC.	**Sim**

					inviolabilidade da intimidade, da honra e da imagem", em seu artigo 2º, IV. Como os dados utilizados pelo fraudador são concernentes à esfera íntima do autor e estavam sob estrita guarda do réu, a responsabilidade civil do banco pelo ocorrido é patente.			
RI 0149420-32.2021.8.05.0001	Banco	Fraude de Terceiro (Boleto falso)	Não	Sim	Analisando os autos, percebo que o fraudador possuía dados da parte autora, que esta não forneceu, relativas ao contato objeto do financiamento. Assim, fica claro que o fraudador conseguiu acesso aos dados do empréstimo junto ao banco acionado. Para além do diploma consumerista, aplicável ao caso concreto, a Lei Geral de proteção de Dados possui aplicação ao caso: Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados	Não	N/A	**Sim**

					pessoais, é obrigado a repará-lo. [...] Assim, concluo que há, no caso concreto, elementos que evidenciam culpa concorrente de ambas as partes.			
1000201-59.2020.8.11.0044 MT	Banco	Fraude de Terceiro (Boleto Falso)	Sim	Sim	Ademais, a ré Aymoré Crédito, Financiamento e Investimento S.A. efetuou cobrança relativa a contrato ilegal negociado em nome da autora, sendo, portanto, responsável solidária pela reparação dos danos causados à autora. 3. Logo, restando caracterizada a existência de fraude em nome da autora, em razão de vazamento de dados, resta evidenciado o dever de indenizar, a teor do que dispõem os artigos 42, 44, parágrafo único, e 45, todos da Lei Geral de Proteção de Dados Pessoais (LGPD).	Sim	Art. 14 do CDC.	**Sim**
APL 0095989-30.2020.8.19.0001	Banco	Fraude de Terceiro (Motoboy)	Não	Sim (menção)	Apenas menção	Sim	Arts. 8º, 9º e 10 do CDC e, em se tratando da prestação de serviços bancários e financeiros, estende-se à segurança no uso dos meios de pagamento, no compartilhamento de	**Sim**

							informações pessoais e no atendimento telefônico.	
APL 0007499-94.2021.8.19.0066	Banco	Fraude de Terceiro (Boleto Falso)	Não	Sim	Com o objetivo de trazer maior segurança no tratamento de informações pessoais, foi editada a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados (LGPD)– a qual prevê a responsabilidade das instituições financeiras pela proteção e tratamento de dados pessoais de seus correntistas armazenados em seus bancos. Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: (...)	Sim	Art. 14, CDC	**Sim**
AC 1000479-16.2020.8.26.0150 SP 1000479-16.2020.8.26.0150	Banco	Fraude de Terceiro (Empréstimo não contratado)	Não	Sim	A Lei nº 13.709/2018 Lei Geral de Proteção de Dados, ainda que não qualifique os dados documentais, a priori, como "sensíveis", a teor de seu artigo 5º, II, (dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual,	Sim	Art. 14, CDC	**Sim**

					dado genético ou biométrico, quando vinculado a uma pessoa natural) disciplina, como fundamento da proteção dos dados pessoais "a inviolabilidade da intimidade, da honra e da imagem", em seu artigo 2º, IV. Como os dados utilizados pelo fraudador são concernentes à esfera íntima da autora e estavam sob estrita guarda do réu, a responsabilidade civil do banco pelo ocorrido é patente. Por outro lado, mesmo que o contrato bancário fraudulento tenha sido feito por terceiro que se utilizou dos dados da autora, não é admissível a exclusão da responsabilidade pelas consequências negativas do negócio que entabulou com o estelionatário. No presente caso, a responsabilidade é objetiva, com base no risco atividade, que encontra amparo legal no art. 927, par. único, do Código Civil de 2002 e no artigo 14 do CDC, sem a necessidade do exame da culpa. E os demais pressupostos estão			

					presentes na hipótese pois houve nexo de causalidade entre a conduta do apelante e o dano causado ao apelado, no caso, os descontos promovidos no benefício previdenciário percebido pela demandante e a angústia por uma dívida não reconhecida.			
AC 1001697-36.2021.8.26.0347 SP 1001697-36.2021.8.26.0347 -	Banco	Fraude de Terceiro (Empréstimo não contratado)	Não	Não	N/A	Não	N/A	**Sim**
AC 1002590-11.2021.8.26.0320 SP 1002590-11.2021.8.26.0320	Banco	Fraude de Terceiro (Motoboy)	Não	Sim	Apenas menção	Sim	N/A	**Sim**
AC 1003439-57.2021.8.26.0554 SP 1003439-57.2021.8.26.0554	Banco	Fraude de Terceiro (Motoboy)	Não	Sim	A Lei nº 13.709/2018 Lei Geral de Proteção de Dados, ainda que não qualifique os dados documentais, a priori, como "sensíveis", a teor de seu artigo 5º, II, (dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural) disciplina, como fundamento da proteção dos dados pessoais "a inviolabilidade da intimidade, da honra e da	Sim	Art. 14, § 3º, II	**Sim**

					imagem", em seu artigo 2º, IV. Como os dados utilizados pelo fraudador são concernentes à esfera íntima da apelada e estavam sob estrita guarda dos apelantes, a responsabilidade civil das casas bancárias pelo ocorrido é patente.			
AC 1004656-59.2020.8.26.0526 SP 1004656-59.2020.8.26.0526	Banco	Fraude de Terceiro (Empréstimo não contratado)	Não	Sim	Apenas menção	Não	N/A	**Sim**
AC 1009507-51.2021.8.26.0577 SP 1009507-51.2021.8.26.0577	Cadastro Positivo	Compartilhamento Indevido	Não	Sim	Art. 7º, inciso I e § 4º, da Lei Geral de Proteção de Dados.	Sim	Apenas menção	**Não**
Recurso Inominado Cível: RI 1015517-82.2020.8.26.0016 SP 1015517-82.2020.8.26.0016	Banco (Seguradora)	Ataque Hacker	Sim	Sim	A responsabilidade do controlador de dados está prevista no art. 44 da LGPD Trata-se de acontecimento que, por si só, causa sofrimento moral no titular dos dados armazenados, razão pela qual dispensa-se a demonstração do dano efetivamente sofrido. Em outras palavras, o dano moral é presumido (in re ipsa).	Sim	Art. 14, CDC	**Sim**
1023587-64.2019.8.11.0041 MT	Banco	Fraude de Terceiros (Empréstimo não Contratado)	Não	Sim	"Importa lembrar que a questão em voga foi tratada pela Lei 13.709/18, Lei Geral de Proteçâo de Dados Pessoais (LGPD), que entrou em vigor em agosto de 2020 como forma de	Sim	[...] informação adequada e clara sobre os diferentes produtos, especificando corretamente as características do contrato (art. 4º IV e art. 6º, III, do CDC),	**Sim**

					proteção aos dados pessoais dos titulares que sofrem abusos, inclusive pelos meios digitais. Dado pessoal é toda informação relativa à pessoa natural identificada ou identificável (art. 5º, I); titular é a pessoa natural a quem se referem os dados pessoais objetos de tratamento (art. 5º, II), e tratamento é 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 (art. 5º, X). Um dos princípios que regem as atividades do tratamento de dados pessoais é o princípio da segurança, que prevê, conforme art. 6º, VII, "utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não		observando-se a possibilidade de convalidação do negócio anulável, segundo os princípios da conservação dos negócios jurídicos (CC, art. 170).	

					autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão". Frente a isso, de acordo com 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" (Sem destaques no original)."			
AC 5004351-12.2021.8.13.0145 MG	Banco	Fraude de Terceiros (Falso Boleto)	Não	Não	N/A	Sim	"O STJ, por seu turno, também já pacificou sua jurisprudência. É a Súmula 297: ""O Código de Defesa do Consumidor é aplicável às instituições financeiras."" É, portanto, objetiva a responsabilidade da apelante, como resulta do art. 14 CDC	**Sim**