DIÁLOGOS E INTERFACES DO DIREITO

REVISTA CIENTÍFICA DO CURSO DE DIREITO
CENTRO UNIVERSITÁRIO FAG

A RESPONSABILIDADE CIVIL DO ESTADO NA QUEBRA DE SEGURANÇA DAS INFORMAÇÕES EM SISTEMAS GOVERNAMENTAIS

SANTOS, Cleber Shiguero Ueda [1]
SILVA JUNIOR, José Roberto Martins da[2]

RESUMO: Este trabalho visa trazer a exposição de um dos possíveis problemas jurídicos oriundos reflexamente dos avanços tecnológicos. Visando a melhoria nos serviços prestados à população, em especial pelo ganho em celeridade e economicidade, o governo passa a adotar diversas tecnologias, as quais podem, consequentemente, apresentar vulnerabilidades. Neste compasso, o presente artigo traz os resultados de uma pesquisa predominantemente bibliográfica, na qual buscou-se relacionar a responsabilidade civil do Estado com o vazamento de informações pessoais das pessoas do povo, as quais se encontram armazenadas em seus sistemas informatizados. Em especial, aqueles dados fornecidos ao governo para o usufruto de serviços necessários à vida civil, como por exemplo, o Cadastro de Pessoa Física (CPF). Para isso, foi necessária a pesquisa e apresentação dos princípios da segurança da informação, além de normas e padrões de segurança, como por exemplo, a norma internacional ISO 27002, ou NBR ISO 27002. Também foram apresentados aqueles diplomas legais que se destacam na regulação ao tratamento e acesso a dados informatizados, como a Lei 12.737/2012, também conhecida como "Lei Carolina Dieckmann", e a Lei Geral de Proteção de Dados (LGPD). Já de outro lado, foram apresentadas as principais teorias do direito administrativo que tratam do tema responsabilidade civil do Estado, além de jurisprudências que abordem a temática ora apresentada, em casos quotidianos.

PALAVRAS-CHAVE: Responsabilidade, Civil, Estado, Segurança, Informações.

THE CIVIL RESPONSIBILITY OF THE STATE FOR BREAKING INFORMATION SECURITY IN GOVERNMENT SYSTEMS

ABSTRACT: This work aims to expose one of the possible legal problems arising as a result of technological advances. Aiming to improve the services provided to the population, especially through gains in speed and economy, the government starts to adopt several technologies, which may, consequently, present vulnerabilities. In this context, this article brings the results of a predominantly bibliographical research, in which we sought to relate the civil liability of the State with the leakage of personal information of people, which is stored in its computerized systems. In particular, data provided to the government to benefit from services necessary for civil life, such as the Individual Taxpayer Registry (CPF). To achieve this, it was necessary to research and present the principles of information security, in addition to security norms and standards, such as the international standard ISO 27002, or NBR ISO 27002. Those legal diplomas that stand out in regulation were also presented. to the processing and access to computerized data, such as Law 12,737/2012, also known as the "Carolina Dieckmann Law", and the General Data Protection Law (LGPD). On the other hand, the main theories of administrative law that deal with the issue of State civil liability were presented, as well as jurisprudence that addresses the topic presented here, in everyday cases.

KEYWORS: Liability, Civil, State, Security, Information.

[1]Acadêmico do curso de Direito do Centro Universitário Fag, e-mail: cleberueda@gmail.com
[2] Docente orientador do curso de Direito do Centro Universitário Fag, e-mail: josejr@fag.edu.br

1 INTRODUÇÃO

A tecnologia da informação oferece diversas facilidades, como celeridade, economia, redução na utilização de papel físico e encurtamento de distâncias. Entretanto, consequentemente trouxe algumas desvantagens e preocupações, como a vulnerabilidade das informações digitais (as quais podem ser acessadas de qualquer lugar do mundo por meio da internet) e a possibilidade de acesso indevido de informações, inclusive, confidenciais, respectivamente. Nesse sentido, há necessidade de proteção dos direitos e garantias fundamentais do cidadão pelo Estado.

Em conformidade com essa necessidade, a Lei Geral de Proteção de Dados (LGPD) estipula, em seu artigo 23, que o poder público deve tratar os dados pessoais com o objetivo de cumprir sua missão, sempre em busca do interesse público. Ademais, o exercício de suas funções deve observar os princípios gerais da Administração Pública estabelecidos no caput do artigo 37 da Constituição Federal, cuja redação foi modificada pela Emenda Constitucional nº 19 de 1998, incluindo o princípio da Eficiência.

A aparente sensação de segurança que os cidadãos têm em relação às suas informações pessoais, quando estas estão submetidas a custódia dos poderes governamentais, está intrinsecamente ligada ao exercício dos direitos constitucionais. Um exemplo disso é o Cadastro de Pessoas Físicas - CPF, que se tornou um documento vital para o cumprimento de obrigações cotidianas. A sociedade confia na premissa de que seus dados estão resguardados, uma vez que estão protegidos pela administração do Estado, cujo compromisso com o interesse público é presumido como prioridade. Contudo, tecnicamente, nenhum sistema é imune a ataques cibernéticos, o que significa que os indivíduos estão suscetíveis a possíveis prejuízos.

Diante do cenário atual, torna-se essencial discutir a responsabilidade do Estado na guarda das informações pessoais dos cidadãos, dado que o termo "responsabilidade" deriva do latim "*respondere*," implicando a ideia de restituição ou compensação pelo interesse sacrificado (Gonçalves, 2022). Com essa perspectiva, é pertinente abordar a questão da responsabilização das entidades de direito público. Conforme disposto no artigo 37, parágrafo 6, da Constituição Federal, o Estado adota o princípio da responsabilidade objetiva, baseado no critério do risco administrativo. Isso significa que, em casos de violações de dados, a vítima precisa apenas demonstrar o dano ocorrido e o nexo causal, simplificando significativamente o processo de responsabilização do Estado.

Portanto, apesar da aparente confiança na segurança dos dados pessoais submetidos a tutela governamental, a realidade revela a persistência de riscos, de forma que a legislação foi concebida com o intuito de agilizar o processo de reparação em situações de danos. Esse cenário ressalta a importância de equilibrar a proteção dos dados pessoais dos cidadãos com a necessidade de responsabilização eficaz das instituições de direito público diante de eventuais incidentes de segurança.

Este trabalho justifica-se pela necessidade de se averiguar a responsabilidade do Estado, visto que por vezes os gestores e responsáveis pelos sistemas podem não ter uma compreensão completa da importância da segurança da informação e dos riscos associados à sua falha. Em comparação com a iniciativa privada, o setor público normalmente é caracterizado pela burocracia e pela lentidão na tomada de decisões. Isso se dá não apenas por uma possível ineficiência técnica dos envolvidos, mas também pela imposição de limites que a própria lei define para as atividades administrativas do Estado.

Essa irresponsabilidade pode ser materializada na falta de qualificação técnica de seus servidores, falta de regulamentação adequada, falta de transparência com os administrados e falta de prioridade no enfrentamento da situação. Um exemplo evidente das consequências dessas omissões é o fato do Governo Federal ter se tornado alvo de ataques cibernéticos, o grupo formado por hackers, intitulado como Monte Everest, teria disponibilizado, por meio de sua plataforma na *deep web*, acesso à rede de dados do governo brasileiro, contendo uma quantidade substancial de informações, totalizando cerca de mais de 3 *terabytes* de diversas pastas do governo brasileiro.

Sendo assim, é possível observar que, embora a Lei Geral de Proteção de Dados (LGPD) estabeleça em seu artigo 46, que a proteção de dados pessoais é fundamental para garantir a privacidade dos cidadãos e regular o tratamento de informações pessoais pelas organizações no Brasil, a segurança cibernética nem sempre é considerada uma prioridade para o Estado. Isso ocorre especialmente quando existem demandas concorrentes por recursos financeiros e humanos no sistema, como, por exemplo, em relação às despesas obrigatórias que a Constituição impõe ao governo. Nesse contexto, enfrentar os ataques cibernéticos constantes aos sistemas governamentais apresenta inúmeros desafios políticos e administrativos, que podem sobrecarregar os recursos disponíveis para a defesa cibernética.

Com base no exposto supra, esta pesquisa intenta, de uma forma geral, analisar se há responsabilidade do Estado, com fundamento nas teorias administrativistas que permeiam o assunto, em situações de quebra de segurança das informações dos cidadãos nos sistemas

governamentais, tendo em vista a complexidade dos desafios tecnológicos e a necessidade de recursos que tornam a melhoria da segurança cibernética um desafio contínuo. Além do mais, na mesma toada, buscou-se descrever os benefícios e dificuldades encontradas na segurança das informações nos sistemas informatizados do Estado Brasileiro. Também é importante mencionar as possíveis formas de vazamentos dos dados e informações da população, bem como suas respectivas consequências aos indivíduos que são lesados. Por fim, o presente trabalho também busca avaliar medidas de segurança atualmente utilizadas pelo Estado e suas respectivas exigências legais.

Desta forma, foi realizada uma extensa pesquisa bibliográfica multidisciplinar, cujos resultados serão apresentados a seguir. Inicialmente são apresentados conceitos, princípios e normas relacionadas à segurança da informação, os quais se aplicam, principalmente, a sistemas informatizados. Logo após adentra-se na temática da responsabilidade civil do Estado, onde serão evidenciados os principais diplomas legais, incluindo a nossa Carta Magna de 1988, além das principais teorias sobre o assunto, bem como jurisprudências afetas ao tema. Enfim, buscando a concatenação dos assuntos, abordamos o direito do administrado à indenização, caso ele seja prejudicado em decorrência da omissão do Estado na segurança das informações.

2 A SEGURANÇA DA INFORMAÇÃO

A segurança da informação representa um fenômeno social no qual os usuários, incluindo os gestores, dos sistemas de informação possuem um conhecimento considerável sobre a utilização desses sistemas. Isso abrange a compreensão das implicações e obrigações estabelecidas por meio de regras, bem como a percepção de seus respectivos papéis na execução dessa utilização (Marciano, 2006, p. 115).

Conforme definido pela ABNT (2005), a segurança da informação envolve resguardar a informação de diversas ameaças, visando assegurar a continuidade das operações de negócio, minimizar riscos, otimizar o retorno de investimentos e aproveitar oportunidades comerciais. A ABNT também ressalta que a segurança da informação é crucial tanto para entidades públicas quanto privadas, incluindo a proteção de infraestruturas críticas.

Em ambos os setores, a segurança da informação desempenha o papel de viabilizar iniciativas como o governo eletrônico (e-gov) e o comércio eletrônico (e-*business*), ao mesmo tempo em que mitiga riscos significativos (ABNT, 2005).

Ademais, a segurança da informação, uma área em constante evolução no contexto atual, está intrinsecamente ligada à tecnologia da informação (TI), especialmente aos sistemas

de informação, bem como à guarda e manipulação de dados. Nesse contexto, a segurança da informação assume um papel crucial na operação de organizações de todos os tipos e tamanhos, sendo, em alguns casos, uma exigência obrigatória para o desempenho das atividades empresariais. Um exemplo disso é a Resolução nº 4.658, de 26 de abril de 2018, na qual o Banco Central do Brasil (BACEN) regulamenta a política de segurança cibernética e estabelece requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem pelas instituições financeiras.

2.1 PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Dentre as normativas a serem seguidas pelos setores públicos e privados em relação à segurança da informação estão os princípios. Estes também são conhecidos como pilares e possuem importância para o tema haja vista que auxiliam na compreensão do assunto, bem como na consecução dos objetivos propostos pela área. Os princípios mais aplicados formam a chamada tríade CIA, formada pelos princípios da Confidencialidade, Integridade e Disponibilidade (Machado, 2014, p. 19).

Os princípios em questão encontram-se expressamente fixados na norma ISO/IEC 27032, intitulada "Orientações para a cibersegurança". Essa norma está ligada a filosofia da segurança da informação que permeia as normas internacionais ISO 27000. Estabelecendo um conjunto uniforme de procedimentos de segurança cibernética. Adicionalmente, nesse mesmo contexto, outras qualidades como autenticidade, responsabilidade, não repúdio e confiabilidade também podem desempenhar um papel de relevância na segurança de dados, conforme a norma ISO/IEC 27032 (Vianna; Fernandes, 2015).

O princípio da Confidencialidade garante que a informação seja acessível apenas por pessoas autorizadas, protegendo-a contra divulgação não autorizada. Dentre os métodos utilizados para a garantia deste princípio, pode-se citar a criptografia, a autenticação e o controle de acesso a dados por meio de senhas (Vianna; Fernandes, 2015).

Já o princípio da Integridade busca assegurar que a informação não seja alterada de maneira não autorizada, mantendo sua precisão e confiabilidade. Nesse aspecto, o referido pilar busca garantir que os dados não sejam adulterados, mantendo a confiabilidade. São exemplos de técnicas que buscam a garantia da Integridade: o *hashing*, a assinatura digital e o certificado digital (Martins; Santos, 2005).

Há, ainda, o princípio da Disponibilidade. Este assevera que a informação esteja disponível quando necessária, evitando interrupções indesejadas ou indisponibilidade. Dentre

as soluções que visam garantir este pilar, os serviços de redundância (como geradores e links redundantes), os backups e as atualizações de sistema (Vianna; Fernandes, 2015).

Essa tríade serve como a base para a análise de riscos e a implementação de controles de segurança. Entretanto, conforme afeiçoa Fontes (2008, p.57), também se apresentam alguns princípios dito complementares, os quais auxiliam no entendimento do assunto:

> **Não-repúdio:** Busca-se métodos que permitam determinar quem executou determinada ação.
> **Autenticação:** Deve haver métodos que comprovem que o usuário é quem ele alega ser.
> **Legalidade:** O sistema deve atender à legislação em vigor, como por exemplo a Lei Geral de Proteção de Dados (LGPD).
> **Privacidade:** É a característica na qual uma informação privada deve ser vista, lida e alterada somente pelo seu dono.
> **Auditoria:** É a possibilidade de se rastrear todas as etapas na qual a informação passou identificando os participantes deste processo (Fontes, 2008).

Em suma, os princípios da segurança da informação servem como base para a proteção de dados pessoais e sistemas. A preservação da confidencialidade, integridade e disponibilidade das informações são procedimentos fundamentais para a garantia da privacidade de dados pessoais compartilhados com entidades governamentais. Além disso, esses princípios não apenas sustentam a segurança de dados, mas também definem as bases para a conformidade legal e a proteção aos direitos individuais dos cidadãos.

1.1.1 Ameaças, Vulnerabilidades e Ataques

Ainda acerca da importância da conceituação sobre a segurança da informação, deve-se compreender alguns elementos-chave envolvidos, quais sejam, ameaças, vulnerabilidades, ataques e riscos.

Ameaça é um evento indesejável que pode danificar um ativo, causando impacto nos resultados do negócio. Peltier (2013, p.17) categoriza as ameaças em três grupos fundamentais com base na origem do agente causador. Sendo elas: as ameaças naturais, que compreendem fenômenos da natureza como inundações, terremotos e tempestades elétricas; as ameaças humanas, que abrangem incidentes que são desencadeados ou facilitados por seres humanos, seja de forma intencional ou não, como *malware*, ocorrências de fraude e outros equívocos comuns na área de Tecnologia; por último, figuram as ameaças ambientais, que envolvem condições climáticas adversas, poluição e umidade (Peltier, 2013, p.18).

Vulnerabilidades são fraquezas em sistemas ou processos que podem ser explorados pelas ameaças. Isso inclui brechas de segurança, falhas de software e políticas inadequadas (Mascarenhas, Neto, 2019, p. 36).

Já ataques são definidos como ações deliberadas realizadas por ameaças para explorar vulnerabilidades e comprometer a segurança. Isso inclui ataques de força bruta, *phishing* e ataques de negação de serviço, conhecido como ataque DDoS (Mascarenhas, Neto, 2019, p. 13).

Risco é conceituado como a probabilidade de ocorrência de um evento adverso ou indesejado. É uma medida que combina a chance de algo ruim acontecer com o impacto negativo que esse evento pode causar. Para entender e quantificar as incertezas e os potenciais eventos adversos que podem afetar negativamente, é realizado o processo chamado análise de risco (Hintzbergen, 2018, p.28).

2.2 NORMAS E PADRÕES DE SEGURANÇA DA INFORMAÇÃO

A segurança da informação é frequentemente regulamentada por padrões e leis, em diversos setores. Dentre os instrumentos normativos, apresenta-se a Lei nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD).

A LGPD representa um marco importante na legislação brasileira, estabelecendo princípios, direitos e obrigações para o tratamento de dados pessoais no país. Um dos aspectos cruciais dessa lei é a garantia da segurança da informação, que visa proteger os dados pessoais de indivíduos contra riscos de vazamento, acesso não autorizado, alteração ou destruição indevida.

2.3 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO AOS DADOS

A Lei nº 13.709/2018 (Lei Geral de Proteção aos dados), estabelece princípios que devem guiar o tratamento de dados pessoais, como o princípio da finalidade, da necessidade, da transparência e da responsabilização. Neste bojo, a segurança da informação é fundamental para a implementação desses princípios, uma vez que a inadequada proteção dos dados pode comprometer a finalidade legítima do tratamento, a necessidade dos dados coletados e a transparência no uso deles. (Carloto; Almirão, 2021, p.120)

Para além disso, é importante destacar que a legislação estipula que a manipulação de informações pessoais deve seguir uma série de princípios norteadores. Portanto, é fundamental

que os responsáveis, tanto controladores quanto os operadores, estejam em conformidade com todas as disposições legais em todas as suas ações.

Um dos princípios fundamentais dessa legislação que merece destaque inicialmente, é o princípio da finalidade. Este princípio possibilita que o indivíduo assegure a conformidade legal no tratamento de seus dados por meio da obtenção prévia de informações, o que, por sua vez, viabiliza a restrição da finalidade do referido tratamento (Machado; Marconi, 2020, p. 195).

Posteriormente o princípio da adequação estabelece que o processamento de informações pessoais só é admissível quando está alinhado com as finalidades previamente comunicadas ao titular, levando em consideração o contexto específico desse tratamento (Machado; Marconi, 2020, p. 195).

Além destes, pode-se citar como norteadores da Lei Geral de Proteção aos Dados, os princípios da necessidade, do livre acesso, da qualidade dos dados, da transparência, da segurança, da prevenção, da não discriminação e da responsabilização e prestação de contas (Machado; Marconi, 2020, p. 196).

Outra norma relevante na proteção de dados é a Lei 12.737/2012, conhecida como "Lei Carolina Dieckmann." Similar à LGPD, a Lei Carolina Dieckmann se aplica tanto a indivíduos quanto ao poder público, estabelecendo regras e penalidades para crimes cibernéticos (Lei nº 12.737/2012). Esta legislação foi promulgada no Brasil em resposta ao caso da atriz Carolina Dieckmann, que teve fotos íntimas divulgadas na internet sem autorização, marcando um ponto de inflexão na conscientização sobre a necessidade de regulamentação nessa área. A lei introduziu mudanças significativas na legislação brasileira, visando proteger indivíduos e a sociedade contra abusos e crimes digitais (Evangelista, 2020, p. 69).

Além disso, a Lei Carolina Dieckmann trata da proteção da privacidade e dos dados pessoais, garantindo que informações sensíveis não sejam acessadas, divulgadas ou utilizadas sem autorização. Isso reflete a importância da segurança da informação como um direito fundamental dos cidadãos em um mundo digitalizado, atendendo ao já mencionado pilar da Confidencialidade.

Ainda no bojo do assunto, apresenta-se a norma internacional ISO 27002, ou NBR ISO 27002, a qual estabelece diretrizes e práticas recomendadas para a gestão de segurança da informação em organizações (Hintzbergen, 2018, p.106). A introdução da NBR ISO 27002 estabelece que a segurança da informação é essencial para o funcionamento das organizações e a proteção de seus ativos. Essa norma reconhece que a informação é um ativo valioso que

precisa ser protegido contra ameaças diversas, como acesso não autorizado, roubo, vazamento, entre outros (Fontes, 2012, p.5)

Além do mais, A NBR ISO 27002 também considera a importância da conformidade legal, que é crucial no cenário brasileiro, especialmente após a entrada em vigor da supracitada Lei Geral de Proteção de Dados (LGPD). Por fim, a norma ISO 27002 enfatiza a importância do gerenciamento de riscos como parte integrante da segurança da informação. Isso evidencia que, na esfera teórica, há normativas em funcionamento que demandam a adoção de diversas condutas com o propósito de assegurar a segurança dos dados pessoais.

O Instituto Brasileiro de Defesa da Proteção de Dados Pessoais, *Compliance* e Segurança da Informação (SIGILO) iniciou uma ação civil pública contra a União Federal, Caixa Econômica Federal, Empresa de Tecnologia e Informações da Previdência (DATAPREV) e a Autoridade Nacional de Proteção de Dados Pessoais (ANPD). Na ação, o SIGILO solicita diversas medidas, incluindo a comunicação aos titulares dos dados afetados, divulgação pública dos incidentes de segurança, remoção dos dados vazados da internet, auditoria do vazamento, suspensão temporária de créditos consignados, condenações por condutas ilícitas, pagamento de indenizações por danos morais individuais e coletivos, e outras providências, com a apresentação de provas necessárias para a resolução do caso.

A ação civil pública nº 5028572-20.2022.4.03.6100, teve como decisão do Ilustríssimo Ministro Marco Aurelio De Mello Castrianni, da 1ª Vara Cível Federal de São Paulo, inicialmente em caráter liminar a imposição de medidas técnicas e tecnológicas necessárias para retirarem os dados vazados da internet, a fim de que cessem os prejuízos aos titulares dos direitos violados, sob pena de multa diária de R$ 10.000,00 (dez mil reais), além disso determinou que seja realizada uma auditoria sobre o vazamento em questão, com posterior apresentação de seu relatório, bem como a comunicação a todos os titulares sobre o vazamento ocorrido, também submetida a pena de multa diária no valor supracitado, por fim condenou os réus ao pagamento de indenização por danos morais individuais homogêneos e ao pagamento de indenização coletiva por lesão a direitos difusos, determinando que sejam julgados procedentes todos os pedidos requeridos na respectiva ação.

3 A RESPONSABILIDADE CIVIL DO ESTADO

3.1 FUNDAMENTAÇÃO LEGAL

A responsabilidade civil do Estado frente a danos a terceiros resultantes de suas intervenções, quer sejam administrativas, legislativas ou judiciais, constitui um fundamento

jurídico crucial. Enquadrado no Direito Administrativo do Brasil, este tópico abrange elementos essenciais que tocam os direitos dos cidadãos, a função estatal e a consolidação de um contexto social equitativo e justo (Carvalho, 2018, p.339).

A Constituição Federal de 1988 serve como alicerce legal para essa obrigação no Brasil, especificamente em seu artigo 37, § 6º, que responsabiliza o Estado por prejuízos causados por seus representantes a terceiros, decorrentes de suas ações ou inações. Este artigo é extremamente significativo para a apreensão da responsabilidade civil do Estado brasileiro (Oliveira, 2021, p.1364).

O Código Civil brasileiro (Lei nº 10.406/2002), em alinhamento com a Constituição, estipula normas gerais sobre a responsabilidade civil. Segundo o artigo 43, entidades públicas têm responsabilidade civil pelos prejuízos ocasionados por seus agentes. Adicionalmente, a Lei nº 9.784/1999, que trata do Processo Administrativo Federal, define os trâmites para a responsabilização administrativa de agentes estatais e delegados, em situações onde os direitos dos administrados são violados por atos ilícitos ou autoritários da administração pública, assegurando a possibilidade de ressarcimento dos danos sofridos.

3.2 TEORIAS ACERCA DA RESPONSABILIDADE CIVIL DO ESTADO

No contexto jurídico brasileiro, a responsabilidade civil estatal é objeto de profundo estudo, destacando-se por sua pluralidade teórica e metodológica que facilita a elucidação da matéria. Neste panorama, ganham proeminência as teorias do Risco Administrativo e do Risco Integral, que serão adiante detalhadas.

A Teoria do Risco Administrativo, que se assenta na premissa da responsabilidade objetiva do Estado, goza de ampla aceitação no ordenamento jurídico brasileiro. Conforme essa teoria, o Estado tem o dever de indenizar os prejuízos infligidos a terceiros decorrentes de suas ações administrativas, dispensando-se a necessidade de demonstração de falha. A responsabilização estatal, nesse caso, é objetiva e fundamenta-se no nexo causal entre o comportamento do Estado — seja por ação ou omissão — e o prejuízo experimentado pelo cidadão. Contudo, admite-se a possibilidade de exclusão ou mitigação dessa responsabilidade em situações de força maior, caso fortuito ou culpa exclusiva do ofendido, conforme apontado por Mello (2012, p.1056).

Por outro lado, a Teoria do Risco Integral amplia a responsabilidade estatal para abarcar situações onde o dano advém de força maior, caso fortuito ou culpa exclusiva da vítima. Sob

essa ótica, o Estado seria responsável por quaisquer danos oriundos de sua atuação, sem considerar as circunstâncias envolventes, como discutido por Tartuce (2019, p. 592).

Por fim, é imperioso mencionar a teoria da Irresponsabilidade do Estado, prevalente durante os regimes absolutistas, que se origina da noção de que o monarca era infalível e, portanto, inquestionável — uma concepção que permitia ao Estado evadir-se da obrigação de reparar danos causados aos súditos, conforme elucidado por Pereira (2013).

3.3 JURISPRUDÊNCIA ACERCA DA RESPONSABILIDADE CIVIL DO ESTADO

A atuação do judiciário brasileiro tem sido crucial na delimitação dos aspectos da responsabilidade civil estatal. Decisões dos tribunais têm criado precedentes fundamentais e direcionam a implementação da responsabilidade civil em situações concretas, notadamente em casos que tangem áreas delicadas do exercício estatal, tais como saúde, educação e segurança pública, conforme aponta Saddy (2023, p.78).

Nesse contexto, as decisões do Supremo Tribunal Federal (STF) e do Superior Tribunal de Justiça (STJ) têm sido vitais para a consolidação dessa norma constitucional. Por meio de decisões inovadoras, essas cortes supremas têm sido pilares na definição dos contornos e extensão da responsabilidade objetiva do Estado, sobretudo em situações habituais e na ausência de legislação específica.

Como ilustração, pode-se citar o julgamento do Recurso Extraordinário nº 841.526, oriundo do Rio Grande do Sul, analisado pelo STF, que abordou a responsabilidade objetiva estatal em contextos de inação governamental. O Ministro Luiz Fux, relator do caso, destacou em seu parecer a necessidade de clareza sobre a matéria, dada a sua complexidade e relevância:

> A jurisprudência do Supremo Tribunal Federal vem se orientando no sentido de que a responsabilidade civil do Estado por omissão também está fundamentada no artigo 37, § 6º, da Constituição Federal, ou seja, configurado o nexo de causalidade entre o dano sofrido pelo particular e a omissão do Poder Público em impedir a sua ocorrência - quando tinha a obrigação legal específica de fazê-lo - surge a obrigação de indenizar, independentemente de prova da culpa na conduta administrativa. (RE 841526, Relator: Min. LUIZ FUX, Tribunal Pleno, j. 30/03/2016, Repercussão geral).

Logo, foram realizadas buscas aos acervos do judiciário brasileiro, em especial das cortes superiores, com o objetivo de encontrar informações correlatas ao tema deste artigo, em especial, aquelas que já se encontram consolidadas.

3.4 A SEGURANÇA DA INFORMAÇÃO EM ORGANIZAÇÕES PÚBLICAS FEDERAIS

No dia 27 de março de 2024, analisou em sessão plenária, o processo nº 017.413/2023-0, o qual tem em seu cerne a avaliação de aspectos relacionados à segurança da informação nas organizações públicas federais. No bojo do processo, foi realizada auditoria, cujo objetivo era identificar falhas em serviços de hospedagem web, correio eletrônico e resolução de nomes.

Segundo o relatório de auditoria, as deficiências descobertas dentro do processo utilizado, tornam a maioria das instituições e seus usuários vulneráveis a ataques online. Desta forma, isso teria o potencial de comprometer tanto a confidencialidade quanto a integridade de uma ampla variedade de serviços digitais oferecidos ao público pelo governo federal e suas divisões regionais.

O documento supra, detectou algumas ameaças que indicam a viabilidade de manipulação do tráfego de rede, violação de contas de usuários, furto, extravio e perda de dados ou, até mesmo, interrupção dos sistemas de organizações públicas. Ainda conforme análise do TCU, tais questões podem afetar programas, medidas e metas das organizações, além de diminuir reflexamente a confiança da população e possíveis penalidades legais.

Ao final, a análise constatou de que existem falhas na configuração de controles sugeridos pelas melhores diretrizes para os serviços de hospedagem na web, correio eletrônico e DNS (Serviço de Nomes de Domínio). Além disso, também se conclui que a maior parte dos índices medianos das políticas de segurança da informação demonstra um grau de maturidade baixo ou intermediário.

4 DIREITO DO ADMINISTRADO À INDENIZAÇÃO

O direito à indenização do cidadão em decorrência de erros do Estado é uma questão central no campo do Direito Administrativo brasileiro, pois envolve a citada responsabilidade estatal por ações ou omissões que resultem em prejuízos para os indivíduos. Este direito está previsto no artigo 37 da Constituição Federal de 1988, o qual estabelece que a Administração Pública deve pautar-se pela observância da lei e pela busca do interesse público.

A Constituição Federal também assevera que o Estado brasileiro tem o dever de proteger os direitos fundamentais dos cidadãos. Desta forma, quando ocorrem violações desses direitos devido a ações estatais, o direito do cidadão na responsabilidade civil do Estado entra em jogo, permitindo que os indivíduos busquem reparação e justiça (Brasil, 1988).

Ainda em relação à responsabilidade de natureza civil, é importante mencionar a forma na qual a indenização é fixada. Pois bem, o artigo 944, do Código Civil de 2002, afirma que a

indenização deve ser medida pela extensão do dano. Neste sentido, Farias (2016, p.248) preconiza que se deve aplicar a regra da reparação integral visando o ressarcimento dos danos patrimoniais ou na compensação dos danos extrapatrimoniais de acordo com a intensidade de lesão sobre o bem jurídico protegido.

Nesta monta, o direito do cidadão à responsabilidade civil do Estado abrange o direito à reparação integral dos danos sofridos. Isso não engloba apenas os danos materiais, como despesas médicas ou perda de bens, mas também danos morais, como o sofrimento emocional, a perda de qualidade de vida e o constrangimento pelo qual foi vítima (Faria, 2007, p.623).

A responsabilidade civil, que para o desembargador do Tribunal do Rio de Janeiro, Marco Aurélio Bezerra de Melo, é o dever de reparar o dano. E arremata: "podemos definir a responsabilidade civil como a obrigação patrimonial de reparar o dano material ou compensar o dano moral causado ao ofendido pela inobservância por parte do ofensor de um dever jurídico legal ou convencional".

Além disso, José dos Santos Carvalho Filho (2019, p.807), diz que a responsabilidade pode ocorrer em diferentes ramos do direito. Se a norma que tipifica a conduta tem natureza penal, a consumação do fato gerador provoca responsabilidade penal; se a norma é de natureza civil a responsabilidade terá natureza civil, e por fim, sendo de norma de caráter administrativo, nascerá responsabilização na esfera administrativa para o Estado.

Ressalta-se que as esferas de responsabilização supramencionadas possuem natureza distinta e autônoma, de modo que uma conduta poderá ser enquadrada isolada ou cumulativamente, com possibilidade de decisões contraditórias entre si.

Portanto, impõe-se ao Estado, através da legislação em vigor as três finalidades da responsabilidade civil. A qual, a compensatória se aplica no caso de vazamento dos dados pessoais do cidadão, na qual caberá ao Estado reparar os danos provocados a vítima. Já a punitiva pode ser observada resposta a falta de zelo por parte estatal frente aos direitos violados e, por fim, mas não menos relevante, a preventiva busca a adoção de métodos e técnicas mais seguras para tratamento de dados íntimos dos indivíduos (Lopez, 2006).

Logo, em uma interseção de toda esta carga teórica trazida alhures, vislumbra-se a possibilidade do cidadão pleitear a responsabilização do Estado, e uma consequente indenização, em decorrência de prejuízos causados por incidentes de segurança de informação em sistemas governamentais.

5 CONSIDERAÇÕES FINAIS

Consoante foi apresentado este trabalho buscou, por meio de análises, demonstrar se há responsabilidade do Estado, com fundamento nas teorias administrativistas que permeiam o assunto, em situações de quebra de segurança das informações dos cidadãos nos sistemas governamentais, tendo em vista a complexidade dos desafios tecnológicos e a necessidade de recursos que tornam a melhoria da segurança cibernética um desafio contínuo.

Neste sentido, foi realizada uma abordagem específica sobre a matéria, resultante da omissão do Estado pela segurança das informações nos sistemas Governamentais. Assim, o enfoque foi a omissão ou a incapacidade do Estado em concretizar a segurança das informações, deixando de cumprir o dever imposto pela legislação pertinente, cuja consequência é o prejuízo para o cidadão. Desta forma, foram apontados os benefícios e dificuldades encontradas na segurança das informações nos sistemas informatizados do Estado Brasileiro.

Com isso, o problema ora analisado foi confirmado por meio dos vários pontos enfrentados. Dentre eles, destacaram-se: o dever de cuidado do Estado com os dados pessoais do cidadão; as imposições feitas pela Lei Ordinária nº 13.709/2018 (Lei Geral de Proteção de Dados); e os acordos de serviços *on-line* cujo aceite se mostra obrigatório para a utilização de determinado serviço estatal.

Assim, em uma análise das diversas matérias apresentadas, foi possível perceber uma forte tendência no sentido de se reconhecer o direito do cidadão que demonstrou prejuízo decorrente do uso indevido de seus dados, os quais foram confiados à guarda do Estado.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS NBR. **ISO/IEC 2002:2013: Tecnologia da Informação - Técnicas de segurança - Código de prática para controle de segurança da informação**. Rio de Janeiro, 2013.

BRASIL. **Emenda Constitucional nº 115**, de 10 de fevereiro de 2022. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm#:~:text=EMENDA%20CONSTITUCIONAL%20N%C2%BA%20115%2C%20DE,e%20tratamento%20de%20dados%20pessoais. Acesso em: 17 out. 2023.

BRASIL. **Lei Geral de Proteção de Dados**, de 14 de agosto de 2018. Diário Oficial da União. 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 18 set. 2023.

BRASIL. **Constituição da República Federativa do Brasil**, de 5 de outubro de 1988. Diário Oficial da União. 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicaocompilado.htm. Acesso em: 18 set. 2023.

BRASIL. **Lei nº 12.737, de 30 de novembro de 2012**. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Publicado no Diário Oficial da União, de 3 de dezembro de 2012. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm. Acesso em 01 ago. 2023.

BRASIL, Supremo Tribunal Federal (Plenário). **Ação Direta de Inconstitucionalidade 6649/DF**. Diário de Justiça Eletrônico, Brasília, 19 de jun. de 2023. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur482122/false. Acesso em: 07 out. 2023.

BRASIL, Tribunal de Contas da União. **Acórdão nº 523/2024**. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 27/03/2024. Disponível em: https://pesquisa.apps.tcu.gov.br/documento/processo/*/NUMEROSOMENTENUMEROS%253A1741320230/DTAUTUACAOORDENACAO%2520desc%252C%2520NUMEROCOMZEROS%2520desc/0. Acesso em: 11 mai. 2024.

CARLOTO, Selma; ALMIRÃO, Mariana. **Lei Geral de Proteção de Dados Comentada.** 1.ed. São Paulo: LTr, 2021

CARVALHO FILHO, José dos Santos. **Manual de Direito Administrativo**. 33.ed. Rio de Janeiro: Atlas, 2019.

CARVALHO, Matheus. **Manual de Direito Administrativo**. 5.ed. Salvador: Editora Juspodivm, 2018.

COSTA, Elson Santos da; GALVÃO, Wiliam Carlos. **Segurança da Informação e Proteção dos Dados: Aplicação Web.** 2023. Disponível em: http://www.jtni.com.br/index.php/JTnI/article/view/61/76. Acesso em: 30 set. 2023.

DAVIS, Royce. **Pentest em Redes de Computadores**. 1.ed. São Paulo: Editora Novatec, 2021.

DI PIETRO, Maria Sylvia Zanella. **Direito Administrativo**. 12.ed. São Paulo: Atlas, 2000.

EVANGLISTA, Thalyta França. **Crimes Virtuais e o Ordenamento Jurídico Brasileiro: Análise Dogmática**. 1.ed. João Pessoa: Clube de Autores, 2020.

FARIA, Edimur Ferreira de. **Curso de Direito Administrativo Positivo**. 6.ed. Belo Horizonte: Del Rey, 2007.

FARIAS, Cristiano Chaves de, et al. **Curso de Direito Civil: Responsabilidade Civil.** 3.ed. Salvador: Juspodivm. 2016.

FERRI, José Augusto Zen. **Os Criminosos da Era da Informação**. 2004. Disponível em: https://core.ac.uk/display/79070084?utm_source=pdf&utm_medium=banner&utm_campaign=pdf-decoration-v1. Acesso em: 01 out. 2023.

FONTES, Edison. **Políticas e Normas para a Segurança da Informação. Como Desenvolver, Implantar e Manter Regulamentos para a Proteção da Informação nas Organizações.** 1.ed. Rio de Janeiro: Brasport, 2012.

GONÇALVES, Carlos Alberto. **Direito Civil 1 - Parte Geral, Obrigações, Contratos.** 12. ed. São Paulo: Saraiva, 2022.

HINTZBERGEN, Jule, et al. **Fundamentos de Segurança da Informação**. 3.ed. São Paulo: Brasport, 2019.

MACHADO, Luciana Cristina Pinto; MARCONI, Licia Pimentel. **"Estudos Preliminares sobre os Princípios Aplicados ao Tratamento de Dados Pessoais na Lei nº 13.709/2018 - LGPD."**. Universidade do Oeste Paulista – UNOESTE, Presidente Prudente, SP, 2020, Disponível em: https://www.unoeste.br/Areas/Eventos/Content/documentos/EventosAnais/564/anais/Sociais%20Aplicadas/Direito.pdf#page=190. Acesso em: 13 abr. 2024.

MACHADO, Felipe Nery Rodrigues. **Segurança Da Informação – Princípios e Controle de Ameaças.** 1.ed. São Paulo: Saraiva: Érica. 2014.

MASCARENHAS NETO, Pedro Tenório; **Segurança da Informação: Uma Visão Sistêmica para Implantação em Organizações**. João Pessoa: Editora UFPB, 2019.

MARCIANO, João Luiz Pereira. **Segurança da informação: uma abordagem social**. 2006. 212 f. Tese (Doutorado em Ciência da Informação)-Universidade de Brasília, Brasília, 2006. Disponível em: https://repositorio.unb.br/handle/10482/1943. Acesso em: 18 out. 2023.

MARTINS, Alaíde Barbosa; SANTOS, Celso Alberto Saibel. **Uma metodologia para implantação de um sistema de gestão de segurança da informação.** JISTEM-Journal of Information Systems and Technology Management, v. 2, p. 121-136, 2005.

MELLO, Celso Antônio Bandeira de. **Curso de Direito Administrativo**. 30.ed. São Paulo: Malheiros, 2012.

MCCLURE, Stuart; SCAMBRAY, Joel; KURTZ George. **Hackers Expostos – 7.ed. Segredos e Soluções para a Segurança de Redes**. Tradução: João Eduardo Nóbrega Tortello. Porto Alegre: Bookman Editora Ltda. 2014. 760 p. Título original: *Hacking Exposed™ 7: Network Security Secrets & Solutions.* ISBN 9788582601426, 8582601425.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. **Segurança de Redes em Ambientes Cooperativos.** 1.ed. São Paulo: Novatec, 2007.

OLIVEIRA, Rafael Carvalho Rezende. **Curso de direito administrativo.** 9. ed. Rio de Janeiro: Forense; MÉTODO, 2021.

PELTIER, Thomas R. **Information Security Risk Analysis, Second Edition**. Boca Raton: Auerbach Publications, 2005.

PEREIRA, Fábio Soares. Responsabilidade extracontratual do Estado: das origens históricas à objetivação. **Revista de Doutrina da 4ª Região**, Porto Alegre, n. 56, out. 2013. Edição especial 25 anos da Constituição de 1988. (Grandes temas do Brasil contemporâneo). Disponível em: https://revistadoutrina.trf4.jus.br/artigos/edicao056/Fabio_Pereira.html Acesso em: 22 out. 2023.

SADDY, André. **Curso de Direito Administrativo Brasileiro: Volume 1**. 2.ed. Rio de Janeiro: CEEJ, 2023.

TANENBAUM, Andrew S., **Sistemas Operacionais Modernos**. 3.ed. São Paulo: Person, 2010.

TARTUCE, Flávio. **Direito Civil: Direito das Obrigações e Responsabilidade Civil**. 14.ed. Rio de Janeiro: Forense, 2019. 701 p. v. 2.

VIANNA, E. W.; FERNANDES, J. H. C. O gestor da segurança da informação no espaço cibernético governamental: grandes desafios, novos perfis e procedimentos. **Brazilian Journal of Information Science: research trends**, *[S. l.]*, v. 9, n. 1, 2015. DOI: 10.36311/1981-1640.2015.v9n1.05.p65. Disponível em: https://revistas.marilia.unesp.br/index.php/bjis/article/view/5216. Acesso em: 18 out. 2023.