PONTIFÍCIA UNIVERSIDADE CATÓLICA DE GOIÁS
ESCOLA DE DIREITO, NEGÓCIOS E COMUNICAÇÃO
NÚCLEO DE PRÁTICA JURÍDICA
COORDENAÇÃO ADJUNTA DE TRABALHO DE CURSO
ARTIGO CIENTÍFICO

A PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: IMPLICAÇÕES DOS CRIMES DIGITAIS E O PAPEL DA LEI GERAL DE PROTEÇÃO DE DADOS.

ORIENTANDO (A) – RAPHAEL FERREIRA SIQUEIRA

ORIENTADOR (A) - PROF. (A) CLAUDIA LUIZ LOURENÇO

GOIÂNIA-GO
2026

RAPHAEL FERREIRA SIQUEIRA

A PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: IMPLICAÇÕES DOS CRIMES DIGITAIS E O PAPEL DA LEI GERAL DE PROTEÇÃO DE DADOS

Artigo Científico (ou Monografia Jurídica) apresentado à disciplina Trabalho de Curso II, da Escola de Direito, Negócios e Comunicação da Pontifícia Universidade Católica de Goiás(PUCGOIÁS).
Prof. (a) Orientador (a) – Dra. Claudia Luiz Lourenço.

GOIÂNIA-GO
2026

AGRADECIMENTOS

Agradeço, primeiramente, a Deus, por me dar forças, sabedoria e perseverança ao longo de toda a trajetória acadêmica, permitindo que eu superasse os desafios e chegasse até aqui.

Aos meus familiares, expresso minha profunda gratidão pelo apoio incondicional, incentivo e compreensão durante todo o período de estudos, sendo fundamentais para minha formação pessoal e acadêmica.

Aos meus amigos, agradeço pela parceria, apoio e motivação, que tornaram essa caminhada mais leve e significativa.

Aos meus professores e mentores, registro meu reconhecimento pela dedicação, orientação e compartilhamento de conhecimentos, que foram essenciais para o desenvolvimento deste trabalho e para minha evolução acadêmica.

Por fim, agradeço a todos que, de alguma forma, contribuíram para a realização deste trabalho.

SUMÁRIO

A PROTEÇÃO DE DADOS PESSOAIS NA ADMINISTRAÇÃO PÚBLICA: IMPLICAÇÕES DOS CRIMES DIGITAIS E O PAPEL DA LEI GERAL DE PROTEÇÃO DE DADOS

Raphael Ferreira Siqueira[1]

RESUMO

Este estudo analisou a proteção de dados pessoais no âmbito da Administração Pública, com foco nos impactos dos crimes digitais e na aplicação da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) como mecanismo de mitigação de riscos e fortalecimento da segurança da informação. A pesquisa foi desenvolvida por meio de abordagem qualitativa, com caráter exploratório e descritivo, utilizando-se de revisão bibliográfica e documental, além do método dedutivo para análise da legislação, doutrinas e casos relacionados ao tema. Os resultados evidenciaram que a crescente digitalização dos serviços públicos ampliou a eficiência administrativa, mas também aumentou a exposição a vulnerabilidades cibernéticas, como vazamentos de dados, fraudes eletrônicas e ataques a sistemas governamentais. Constatou-se que, embora a LGPD represente um importante avanço normativo na proteção de dados pessoais, sua efetividade ainda enfrenta desafios relacionados à infraestrutura tecnológica, capacitação de servidores e fiscalização. Concluiu-se que a proteção de dados na Administração Pública depende não apenas da aplicação da legislação vigente, mas também do fortalecimento das políticas de segurança da informação e da conscientização institucional, visando garantir maior confiabilidade, integridade e proteção das informações dos cidadãos.

Palavras-chave: Proteção de dados pessoais; LGPD; crimes cibernéticos; Administração Pública; segurança da informação.

ABSTRACT

This study analyzed the protection of personal data within the Public Administration, focusing on the impacts of digital crimes and the application of the General Data Protection Law (LGPD) as a mechanism for mitigating risks and strengthening information security. The research was developed using a qualitative approach, with an exploratory and descriptive character, employing bibliographic and documentary review, as well as the deductive method for analyzing legislation, doctrines, and cases related to the topic. The results

[1]Acadêmico do Curso de Direito na Pontifícia Universidade Católica de Goiás. Email: rapha78905@gmail.com.

showed that the increasing digitalization of public services has increased administrative efficiency, but has also increased exposure to cyber vulnerabilities, such as data leaks, electronic fraud, and attacks on government systems. It was found that, although the LGPD represents an important normative advance in the protection of personal data, its effectiveness still faces challenges related to technological infrastructure, training of public servants, and oversight. It was concluded that data protection in Public Administration depends not only on the application of current legislation, but also on strengthening information security policies and institutional awareness, aiming to guarantee greater reliability, integrity, and protection of citizens' information.

Keywords: Data protection; LGPD (Brazilian General Data Protection Law); cybercrimes.

INTRODUÇÃO

Nos últimos anos, a digitalização da Administração Pública tem aumentado, permitindo um acesso mais ágil e eficiente aos serviços prestados aos cidadãos. No entanto, essa mudança para um ambiente digital traz desafios significativos, em relação à proteção de dados pessoais. Em um cenário em que as informações sensíveis de milhões de cidadãos estão armazenadas em bancos de dados governamentais, a vulnerabilidade a crimes digitais torna-se uma preocupação premente. Casos como vazamentos de dados, fraudes eletrônicas e ataques de ransomware demonstram que a segurança da informação é crucial para a confiança do público nas instituições governamentais

A presente pesquisa tem por objeto a análise da proteção de dados pessoais na Administração Pública, focando nas consequências dos crimes digitais e no papel da Lei Geral de Proteção de Dados (Brasil, 2018) como instrumento de mitigação de riscos e garantia da segurança da informação. O tema revela-se atual e relevante diante da crescente digitalização dos serviços públicos, que, ao mesmo tempo em que promove eficiência, acessibilidade e transparência, também expõe os órgãos públicos a vulnerabilidades relacionadas à segurança e à privacidade dos dados dos cidadãos.

Nesse contexto, a Administração Pública enfrenta desafios significativos no tratamento de dados pessoais, uma vez que lida com grande volume de

informações sensíveis. A exposição indevida desses dados pode resultar em prejuízos à privacidade, fraudes, roubos de identidade e comprometimento da confiança da população nas instituições públicas. Ademais, o crescimento dos crimes digitais, como invasões de sistemas, vazamentos de informações e ataques cibernéticos, evidencia a necessidade de mecanismos eficazes de proteção e governança de dados.

A promulgação da Lei Geral de Proteção de Dados (LGPD), em 2018, representa um marco regulatório no ordenamento jurídico brasileiro, estabelecendo diretrizes para o tratamento, a coleta, armazenamento e tratamento de informações. A LGPD (Brasil, 2018) visa garantir não apenas a privacidade dos indivíduos, mas também a responsabilização de entidades que manejam dados tanto na Administração Pública quanto na privada. Entretanto, a implementação efetiva da lei enfrenta desafios, como a falta de recursos adequados e a escassez de profissionais capacitados em segurança da informação. Contudo, sua implementação na Administração Pública ainda enfrenta entraves, como a falta de capacitação técnica dos servidores, deficiências na infraestrutura tecnológica e dificuldades na adaptação dos procedimentos administrativos às exigências legais.

Diante desse cenário, surgem questionamentos relevantes a serem analisados no decorrer da pesquisa, problemas que precisam ser abordados com profundidade para compreender o impacto dos crimes digitais e a aplicação da Lei Geral de Proteção de Dados (LGPD). Esses desafios estão envolvendo aspectos técnicos, jurídicos e institucionais, tais como: a) falta de capacitação técnica; b) infraestrutura tecnológica; c) dificuldade na implementação da LGPD; d) ameaças cibernéticas crescentes; e) vazamento de dados sensíveis; f) responsabilização e fiscalização ineficientes; g) dificuldade na integração entre órgãos públicos. Esses problemas demonstram a complexidade da implementação da LGPD no âmbito da Administração Pública e a necessidade de políticas públicas mais eficientes e de investimentos em infraestrutura e a capacitação para mitigar os impactos dos crimes digitais.

Para tanto, podem ser formuladas as seguintes hipóteses: a) falta de capacitação técnica e de infraestrutura adequada abalam a proteção dos dados

pessoais; b) os crimes digitais impactam diretamente a confiança da população e a segurança institucional; c) a implementação da LGPD ainda ocorre de forma parcial e desigual entre os órgãos públicos; d) existem dificuldades estruturais e burocráticas que dificultam a plena adequação à legislação; e) as políticas de cibersegurança ainda são insuficientes para prevenir incidentes de grande escala; e f) os mecanismos de responsabilização e fiscalização são, em muitos casos, ineficientes ou pouco aplicados.

Utiliza-se, para o desenvolvimento deste trabalho, uma metodologia de natureza qualitativa, exploratória e descritiva, baseada em pesquisa bibliográfica e documental. Adota-se o método dedutivo, a partir da análise da legislação pertinente, especialmente a Lei Geral de Proteção de Dados, bem como o exame de doutrinas e estudos acadêmicos relacionados ao tema. Além disso, emprega-se o método comparativo e o estudo de casos concretos envolvendo crimes digitais na Administração Pública, contribuindo para uma compreensão mais aprofundada da aplicação prática das normas.

Ter-se-á por objetivo geral investigar as implicações dos crimes digitais na proteção de dados pessoais no âmbito da Administração Pública, analisando a eficácia da Lei Geral de Proteção de Dados na prevenção de incidentes e na promoção da segurança da informação.

Como desdobramento, estabelecem-se os seguintes objetivos específicos no primeiro momento, identificar as principais vulnerabilidades na proteção de dados pessoais no setor público; em seguida, analisar o impacto dos crimes digitais nas instituições públicas; posteriormente, examinar o grau de implementação da LGPD nos órgãos governamentais; além disso, estudar casos práticos de incidentes cibernéticos; e, por fim, propor medidas e recomendações para o aprimoramento das práticas de proteção de dados na Administração Pública.

Diante da complexidade do tema e das constantes ameaças decorrentes da evolução tecnológica, torna-se relevante, pertinente e necessário analisar a proteção de dados pessoais na Administração Pública em conjunto com os mecanismos de combate aos crimes digitais e a efetividade da LGPD, buscando contribuir para uma interpretação mais sistemática e eficiente da

legislação, bem como para o fortalecimento da segurança da informação no setor público.

A escolha deste tema é, portanto, justificada pela necessidade urgente de abordar esses desafios, contribuir para a melhoria das práticas de proteção de dados e de entender como a Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) pode ajudar pode auxiliar na redução desses riscos mantendo a integridade e confiança das informações geridas pelos serviços governamentais.

1.CONCEITO DE PROTEÇÃO DE DADOS PESSOAIS.

A proteção de dados pessoais é o conjunto de normas, princípios e práticas que visam garantir o tratamento adequado de informações das pessoas garantindo a preservação de direitos fundamentais, especialmente os direitos à privacidade.

No Brasil, a proteção de dados ganhou mais importância com a Lei nº 13.709/2018 (LGPD), que estabelece regras para a coleta, o armazenamento, o uso e o compartilhamento de dados, impondo limites e responsabilidades aos agentes de tratamento.

Segundo Danilo Doneda (2020), a proteção de dados pessoais vai além da simples segurança da informação, estando diretamente relacionada à garantia da liberdade e da dignidade da pessoa humana diante do uso massivo de tecnologias digitais.

Além disso, conforme leciona Laura Schertel Mendes (2014), a proteção de dados deve assegurar que o tratamento das informações ocorra de forma transparente, legítima e proporcional, respeitando a finalidade para a qual os dados foram coletados.

Dessa forma, a proteção de dados pessoais configura-se como um instrumento essencial na sociedade da informação, visando prevenir abusos, como o uso indevido de dados, vazamentos e práticas ilícitas no ambiente digital, reforçando o papel do Estado na regulamentação e fiscalização dessas atividades, especialmente na Administração Pública.

1.1 LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (Brasil, Lei nº 13.709/2018), conhecida como LGPD, representa um marco normativo no ordenamento jurídico brasileiro e estabelece regras específicas para o tratamento de dados pessoais, tanto no âmbito público quanto no privado. Sua criação surgiu em razão do crescente avanço das tecnologias digitais e da necessidade de proteger os direitos fundamentais de liberdade, privacidade e direitos dos indivíduos

A LGPD (Brasil, 2018) tem como principal objetivo garantir controle dos indivíduos sobre suas informações pessoais, impondo limites e responsabilidades aos agentes que realizam o tratamento desses dados. Nesse contexto, a lei define como dado pessoal qualquer informação relacionada a pessoa natural identificada ou identificável, abrangendo desde dados básicos, como nome e CPF (Cadastro de Pessoa Física), até dados mais sensíveis, como informações sobre saúde, orientação sexual, convicções religiosas e opiniões políticas.

No que diz respeito aos princípios, a LGPD (Brasil, 2018) estabelece diretrizes fundamentais que devem ser observadas pelos agentes de tratamento. Dentre eles, destaca-se o princípio da finalidade, utilizado para propósitos legítimos, específicos e previamente informados ao titular. Já o princípio da necessidade determina que o tratamento das informações ocorra apenas na medida indispensável para atingir sua finalidade. Por sua vez, o princípio da transparência garante ao titular acesso claro, preciso e facilitado às informações relacionadas ao tratamento de seus dados pessoais; e o princípio da transparência, que assegura ao titular o acesso claro e facilitado às informações sobre o tratamento de seus dados. Além disso, o princípio da segurança impõe a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas.

Outro aspecto relevante da LGPD (Brasil, 2018) é a previsão de direitos assegurados aos titulares dos dados, como o direito de acesso, correção,

anonimização, portabilidade e eliminação de dados pessoais. Tais direitos reforçam a autonomia do indivíduo sobre suas próprias informações e contribuem para a construção de um ambiente digital mais seguro e confiável.

No âmbito da Administração Pública, a LGPD (Brasil, 2018) assume papel ainda mais relevante, uma vez que o Estado atua como grande detentor e gestor de dados pessoais da população. Dessa forma, a observância dos princípios e regras estabelecidos pela lei torna-se essencial para evitar abusos, vazamentos e o uso indevido dessas informações, garantindo a proteção dos cidadãos frente ao avanço das tecnologias digitais.

Por fim, destaca-se que o descumprimento das disposições da LGPD (Brasil, 2018) pode acarretar sanções administrativas, civis e, em determinados casos, até mesmo penais, evidenciando a importância da sua efetiva aplicação como instrumento de proteção de direitos fundamentais no contexto da sociedade da informação.

1.2 PRINCÍPIOS DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

A Lei Geral de Proteção de Dados Pessoais (Brasil, 2018) estabelece um conjunto de princípios fundamentais que orientam o tratamento de dados pessoais no Brasil. Estas diretrizes são essenciais para garantir a privacidade, a segurança e a proteção dos direitos dos titulares. Tais princípios, previstos no artigo 6º da referida lei, devem ser observados por todos os agentes de tratamento, tanto no setor público quanto no privado.

Nesse contexto, a LGPD (Brasil, 2018) baseia-se em dez princípios centrais: finalidade, necessidade, adequação, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas. Esses princípios atuam como parâmetros normativos que limitam e direcionam o uso de dados pessoais, assegurando que seu tratamento ocorra de forma legítima, proporcional e segura, em conformidade com os direitos fundamentais do indivíduo.

O princípio da finalidade (Brasil, 2018) determina que o tratamento de dados deve ocorrer para propósitos legítimos, específicos e informados ao titular, sendo vedada a utilização posterior de forma incompatível com essas

finalidades. Em complemento, o princípio da adequação exige que o tratamento seja compatível com as finalidades informadas, respeitando o contexto em que os dados foram coletados.

O princípio da necessidade (Brasil, 2018) estabelece que o tratamento deve se limitar ao mínimo indispensável para a realização de suas finalidades, evitando a coleta excessiva de informações. Já o princípio do livre acesso garante ao titular a consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.

De sua vez, o princípio da qualidade (Brasil, 2018) dos dados impõe que as informações tratadas sejam exatas, claras, relevantes e atualizadas, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento. O princípio da transparência assegura aos titulares informações claras, precisas e facilmente acessíveis acerca da realização do tratamento de dados e dos respectivos agentes envolvidos.

No que se refere à proteção propriamente dita, o princípio da segurança (Brasil, 2018) determina a adoção de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas. Já o princípio da prevenção orienta a atuação dos agentes no sentido de evitar a ocorrência de danos em virtude do tratamento de dados pessoais.

Por fim, destacam-se os princípios da não discriminação (Brasil, 2018), que veda o tratamento de dados para fins discriminatórios ilícitos ou abusivos, e da responsabilização (Brasil, 2018) e prestação de contas, que impõe aos agentes de tratamento o dever de demonstrar a implementação de medidas capazes de comprovar o cumprimento das normas de proteção de dados pessoais.

Assim, os princípios da LGPD (Brasil, 2018) formam a base do sistema de proteção de dados no Brasil, orientando a interpretação e a aplicação da lei, especialmente no contexto da Administração Pública, onde o tratamento de dados pessoais deve observar rigorosamente tais diretrizes, a fim de garantir a proteção dos direitos fundamentais dos cidadãos.

1.3 IMPLANTAÇÃO DE SISTEMAS DIGITALIZADOS NA ADMINISTRAÇÃO PÚBLICA

A implantação de sistemas digitalizados na Administração Pública reflete a evolução rumo à digitalização dos serviços, possibilitando maior eficiência, transparência e acessibilidade na prestação dos serviços. Esse movimento está diretamente relacionado ao conceito de governo digital, que busca utilizar tecnologias da informação para aprimorar a gestão pública e o atendimento ao cidadão. A experiência internacional demonstra que a digitalização da Administração Pública pode alcançar elevados níveis de eficiência quando implementada de forma planejada e integrada. Um dos principais exemplos é a Estônia, que se consolidou como referência mundial em governo digital ao implementar, desde a década de 1990, sistemas integrados de serviços públicos eletrônicos (OCD, 2019).

Nesse país, praticamente todos os serviços governamentais são realizados de forma online, incluindo votação, acesso a prontuários médicos, abertura de empresas e assinatura de documentos digitais. Esse modelo evidencia que a modernização tecnológica, aliada a políticas robustas de segurança da informação, pode proporcionar maior eficiência administrativa e fortalecimento da confiança entre o Estado e os cidadãos.

Nesse contexto, a Lei nº 14.129/2021(Brasil, 2021) estabelece diretrizes para a digitalização dos serviços públicos, enfatizando a simplificação dos processos administrativos, a ampliação do acesso às informações e a garantia da proteção de dados pessoais.

Paralelamente, a Lei nº 13.709/2018 (LGPD) (Brasil, 2018) determina que o tratamento de dados pessoais, inclusive no âmbito da Administração Pública devendo observar princípios como segurança, prevenção e responsabilização, reforçando a necessidade de medidas eficazes de proteção da informação.

Conforme destaca o Tribunal de Contas da União (2020), a transformação digital no setor público não se limita à implementação de tecnologias, sendo igualmente necessária a adoção de práticas de governança

de dados, gestão de riscos e capacitação dos agentes públicos, com o objetivo de reduzir vulnerabilidades e prevenir incidentes de segurança.

Dessa forma, verifica-se que a implantação de sistemas digitalizados, quando realizada sem planejamento adequado, pode ampliar a exposição a riscos cibernéticos, como vazamentos de dados e ataques a sistemas institucionais. Portanto, é fundamental que a digitalização no setor público seja conduzida em conformidade com as normas de segurança da informação e os preceitos legais, garantindo a tutela dos direitos fundamentais.

1.4 CRIMES DIGITAIS E SEUS IMPACTOS

Os crimes digitais, também denominados crimes cibernéticos, correspondem a condutas ilícitas praticadas por meio de sistemas informáticos, dispositivos eletrônicos e redes de computadores, com o objetivo de obter vantagem indevida, causar danos ou acessar informações de forma não autorizada. Essas Atividades ilegais causam bilhões em prejuízos anuais e afetam cidadãos comuns a grandes corporações. Com o avanço das tecnologias digitais e a crescente digitalização dos serviços públicos e privados, observa-se um aumento significativo dessas práticas ilícitas. Embora não haja uma definição única e expressa no ordenamento jurídico brasileiro, diversas normas tratam dessas condutas de forma específica. A Lei nº 12.737/2012 (Brasil, 2012), por exemplo, tipifica a invasão de dispositivos informáticos, enquanto o Código Penal Brasileiro (Brasil, 1940) prevê crimes como estelionato e fraude eletrônica, que podem ser praticados no ambiente digital.

De acordo com a Lei nº 12.737/2012 (Brasil, 2012), é crime a invasão de dispositivos informáticos alheios com o intuito de obter, adulterar ou destruir dados ou informações sem autorização do titular. Essa legislação representa um importante marco no combate aos crimes digitais no Brasil, especialmente no que se refere à proteção da intimidade e da vida privada no ambiente virtual.

Nesse contexto, os crimes digitais podem assumir diversas formas, como fraudes eletrônicas, phishing, disseminação de softwares maliciosos

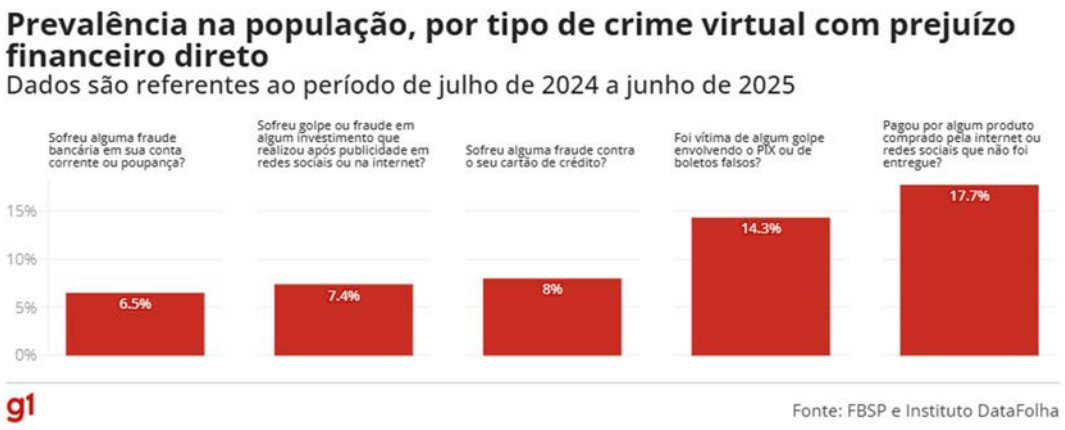
(malware), ataques de ransomware e vazamento de dados pessoais. Essas práticas atingem tanto indivíduos quanto instituições públicas e privadas, sendo especialmente preocupantes no âmbito da Administração Pública, que armazena grande volume de dados sensíveis.

Segundo Patrícia Peck Pinheiro (2021), o crescimento dos crimes cibernéticos está diretamente relacionado à expansão do uso da internet e à insuficiência de mecanismos de segurança da informação, o que torna as organizações mais vulneráveis a ataques.

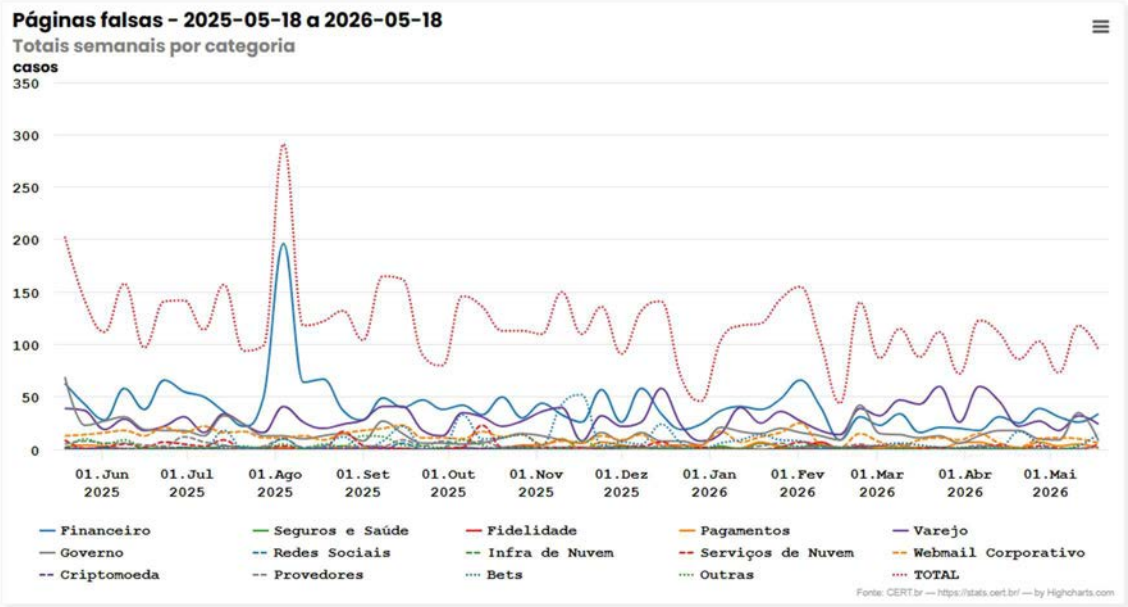
Os impactos decorrentes desses crimes são amplos e abrangem prejuízos financeiros, interrupção de serviços públicos, danos à imagem institucional e violação de direitos fundamentais, como a privacidade e a proteção de dados pessoais. Além disso, conforme destaca o Tribunal de Contas da União (2020), incidentes de segurança da informação no setor público podem comprometer a confiança da população nas instituições governamentais, afetando a credibilidade do Estado.

1.4.1 Estelionato digital

De acordo com pesquisa realizada pelo Instituto Datafolha em parceria com o Fórum Brasileiro de Segurança Pública, divulgada em 2025, foram entrevistadas 2.007 pessoas com idade igual ou superior a 16 anos em 130 municípios brasileiros. O levantamento apontou que aproximadamente 24 milhões de brasileiros foram vítimas de golpes relacionados ao Pix ou boletos falsos, representando 14% dos entrevistados. Os dados demonstram que esse tipo de fraude virtual superou crimes como roubo ou furto de celular e circulação de dinheiro falso, evidenciando o crescimento dos crimes cibernéticos no país. Além disso, os prejuízos financeiros causados por essas práticas ultrapassaram R$ 29 bilhões, com média aproximada de R$ 1.198 perdidos por vítima (Data folha, 2025).

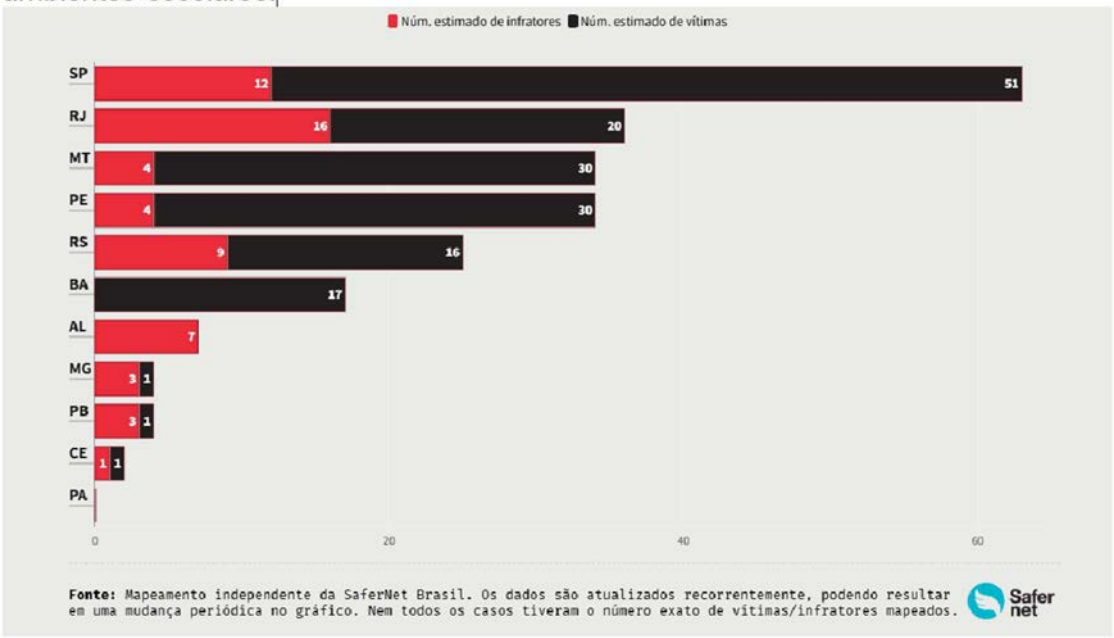


Phishing



Deepfakes

Estimativas da SaferNet para vítimas e autores em casos de deepfakes em ambientes escolares.



Obs: O primeiro caso identificado no mapeamento data de 2023 — período em que as tecnologias de criação de imagens evoluíram de forma acelerada ;

Dessa forma, verifica-se que os crimes digitais representam um dos principais desafios da sociedade contemporânea, exigindo políticas eficazes de prevenção, mecanismos de segurança e a aplicação rigorosa da legislação vigente, especialmente no âmbito da Administração Pública.

1.4.2 Categoria de crimes cibernéticos e suas modalidades

Com o avanço das tecnologias e da crescente utilização da internet para atividades pessoais, financeiras e profissionais os crimes cibernéticos representam uma das principais ameaças à segurança digital na sociedade contemporânea, tais práticas ilícitas podem ser classificadas em diferentes categorias Crimes próprios e os crimes cibernéticos impróprios.

Os crimes próprios correspondem às condutas que somente podem ser praticadas no ambiente virtual, os principais alvos são sistemas informáticos, redes de computadores ou dispositivos eletrônicos. Um exemplo claro são invasões de dispositivos e sistemas por hackers, a disseminação de softwares

maliciosos. Por outro lado, os crimes impróprios consistem em infrações já existentes no meio físico, mas que Infrações que já existiam no mundo físico e migraram para a internet, como estelionato, extorsão e difamação

Observa-se que as modalidades de crimes virtuais evoluem constantemente e exploram a engenharia social, ou seja, a manipulação psicológica da vítima com o objetivo de obter informações sigilosas ou vantagens ilícitas. As principais fraudes são:

a) Phishing e Fraudes Financeiras: Links falsos que simulam bancos ou órgãos do governo para roubar senhas e dados de cartão de crédito.

b) Estelionato Digital: Golpes do falso Pix, falsas ofertas de emprego ou a venda de produtos inexistentes em redes sociais.

c) Roubo de Identidade: Uso indevido de dados pessoais por terceiros para abertura de contas ou realização de compras em nome da vítima.

d) Crimes contra a Honra: Difamação, ameaças e cyberbullying utilizando perfis falsos nas redes sociais.

1.4. 2 Ocorrências de crimes cibernéticos recentes e emblemáticas

1.4.2.1 Ataque ao STJ – Superior Tribunal de Justiça (2020)

No dia 3 de novembro, o Superior Tribunal de Justiça (STJ) sofreu o pior ataque cibernético já empreendido contra uma instituição pública brasileira a ação criminosa comprometeu os sistemas internos do tribunal, causando a paralisação temporária de julgamentos, sessões virtuais e atividades administrativas. O ataque afetou diretamente o funcionamento da corte, evidenciando a vulnerabilidade das instituições públicas diante das ameaças digitais. De acordo com informações divulgadas na época, os criminosos utilizaram um software malicioso capaz de bloquear o acesso aos sistemas e arquivos do tribunal, dificultando o acesso às informações armazenadas (Brasil, 2020).

1.4.2.2 Ataque ao Ministério da Saúde e ConecteSUS (2021)

Na madrugada de sexta feira no dia 10 de dezembro o Ministério da Saúde foi alvo de um ataque cibernético que comprometeu diversos sistemas digitais do governo federal, incluindo a plataforma ConecteSUS, responsável pelo armazenamento e disponibilização de informações relacionadas à vacinação da população brasileira. O ataque causou instabilidade e indisponibilidade temporária dos serviços, impedindo o acesso de milhões de cidadãos aos certificados de vacinação contra a Covid-19.

A ação criminosa foi atribuída a hackers que invadiram os sistemas do ministério, comprometendo o funcionamento de plataformas essenciais utilizadas pela população e pela Administração Pública. Além da interrupção dos serviços, o episódio gerou preocupações relacionadas à segurança das informações pessoais armazenadas nos sistemas governamentais, especialmente diante da grande quantidade de dados sensíveis sob responsabilidade do Estado (G1a, 2021).

1.4.2.3 Megavazamento do Facebook no Brasil (2021)

Em setembro de 2023, a empresa Meta Platforms, responsável pela plataforma Facebook, foi condenada pela Justiça brasileira ao pagamento de indenização coletiva em decorrência do vazamento de dados pessoais de aproximadamente 8 milhões de usuários brasileiros em 2021. O incidente envolveu a exposição indevida de informações como nomes, números de telefone, e-mails e outros dados vinculados às contas da rede social (G1b, 2021).

2. CONSEQUÊNCIAS DO VAZAMENTO DE DADOS PESSOAIS

O vazamento de dados pessoais é uma das principais consequências da fragilidade dos sistemas de segurança da informação na sociedade atual. Com

o avanço da tecnologia e a digitalização crescente de serviços públicos e privados, o armazenamento de informações pessoais em bancos de dados digitais se tornou comum. Isso aumentou significativamente os riscos de acesso indevido, compartilhamento não autorizado e uso ilegal dessas informações.

Esses Vazamentos podem ocorrer por diversos motivos, como ataques cibernéticos, falhas de segurança, descuidos pessoais, descuidos no tratamento das informações, uso de softwares maliciosos e até mesmo ações internas de pessoas autorizadas. Quando essas informações são expostas de forma inconveniente, os danos afetam não apenas os titulares, mas também empresas, instituições públicas e a sociedade como um todo. Entre as principais consequências estão os prejuízos financeiros, o roubo de identidade, fraudes bancárias, estelionato digital, extorsões e invasões de contas pessoais. Os criminosos podem usar dados vazados, como CPF, senhas, números de telefone e informações bancárias, para aplicar golpes virtuais, fazer compras indevidas, acessar serviços em nome da vítima. Além dos danos financeiros.

O vazamento de dados pode causar sérios danos à privacidade, à honra e à segurança das pessoas, especialmente quando envolvem informações confidenciais, como laudos médicos, biométricos etc. Em muitos casos, a exposição dessas informações pode gerar constrangimentos, discriminação e danos psicológicos às vítimas. Na Administração Pública, os riscos são ainda mais preocupantes, pois os órgãos governamentais guardam uma grande quantidade de informações sensíveis da população. Vazamentos que envolvem instituições públicas podem minar a confiança da sociedade no Estado e facilitar práticas criminosas contra cidadãos e serviços governamentais.

3. O USO DA INTELIGÊNCIA ARTIFICIAL E SEUS RISCOS À PROTEÇÃO DE DADOS

A Inteligência Artificial (IA) é usada cada vez mais no dia a dia. Ela está presente em redes sociais, aplicativos, assistentes virtuais, sistemas bancários, plataformas digitais e em órgãos públicos. Essa tecnologia analisa grandes

quantidades de dados permitindo que os sistemas aprendam padrões, realizem tarefas automáticas e ofereçam respostas rápidas e eficientes. Existem diferentes tipos de Inteligência Artificial, cada um destinado às funções específicas. Exemplos: Inteligência Artificial (IA) de reconhecimento facial utilizadas em segurança e identificação; IAs generativas que podem criar textos, imagens, vídeos e áudios. Também tem-se os algoritmos de recomendação, presentes em redes sociais e plataformas digitais, que sugerem conteúdos aos usuários com base em seu comportamento na internet.

Apesar dos benefícios essas tecnologias, a Inteligência Artificial pode ser usada para fins criminosos para criar vídeos, imagens e vozes falsas que parecem reais. Isso pode ser utilizado para espalhar notícias falsas, cometer fraudes financeiras, falsificar identidades e manipular informações e criar mensagens fraudulentas mais convincentes, páginas falsas de phishing e sistemas automáticos que aplicam golpes em grande escala. Muitas vezes, essas práticas utilizam dados pessoais de vazamentos de informações na internet.

4. A IMPORTÂNCIA DA LGPD NO COMBATE AOS CRIMES DIGITAIS

A Lei Geral de Proteção de Dados (LGPD), instituída pela Lei nº 13.709/2018 (Brasil, 2018), representa um importante avanço na proteção dos dados pessoais e no fortalecimento da segurança das informações no ambiente digital. Sua criação ocorreu em razão do crescente avanço das tecnologias digitais e da necessidade de estabelecer mecanismos capazes de garantir maior privacidade, transparência e segurança no tratamento de dados pessoais. Ela é fundamental no combate aos crimes digitais, pois obriga empresas a adotarem medidas rigorosas de segurança e privacidade. Ao reduzir as vulnerabilidades e exigir o controle sobre os dados dos usuários, a lei dificulta a ação de cibercriminosos, como roubos de identidade, fraudes e vazamentos.

4.1 EFETIVIDADE DA LGPD

A efetividade da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) representa um importante avanço na cultura de privacidade e proteção de dados no Brasil, especialmente diante do crescimento das tecnologias digitais e dos crimes cibernéticos. A legislação contribuiu para ampliar os direitos dos cidadãos em relação aos seus dados pessoais, permitindo maior controle sobre informações armazenadas por empresas e instituições públicas.

Nesse contexto, a LGPD (Brasil, 2018) fortaleceu o direito dos titulares de solicitar acesso, correção e exclusão de dados pessoais, além de exigir maior transparência quanto à forma de tratamento dessas informações. Além disso, a legislação impulsionou mudanças na cultura organizacional de empresas e instituições, incentivando investimentos em segurança da informação, políticas de privacidade e mecanismos de prevenção contra vazamentos de dados.

Cabe destacar o fortalecimento do entendimento jurídico relacionado à proteção de dados pessoais. Os tribunais brasileiros passaram a consolidar posicionamentos voltados à responsabilização de instituições envolvidas em falhas de segurança e vazamentos de informações, contribuindo para maior efetividade da legislação.

Apesar dos avanços alcançados pela Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018), sua eficácia ainda enfrenta vários desafios no Brasil. O aumento constante dos crimes cibernéticos, dos vazamentos de dados e das fraudes digitais mostra que muitas instituições ainda apresentam falhas em seus sistemas de segurança. Isso dificulta a proteção das informações pessoais dos cidadãos. Além disso, a rápida evolução das tecnologias digitais e das táticas usadas por crimes virtuais leva ao surgimento de novas formas de ataques cibernéticos, que muitas vezes conseguem superar os métodos tradicionais de segurança.

Nesse cenário, várias organizações ainda lutam com questões relacionadas à adoção de novas tecnologias, ao investimento em cibersegurança e ao cumprimento integral das exigências da legislação. No

setor público, os desafios são ainda mais graves, devido à grande quantidade de dados sensíveis que os órgãos governamentais armazenam. Os ataques cibernéticos registrados nos últimos anos mostram a necessidade de reforçar as políticas de segurança da informação e implementar medidas preventivas mais eficazes para proteger os dados da população. Outro ponto importante é que muitas pessoas não conhecem os direitos garantidos pela LGPD (Brasil, 2018). Isso dificulta a identificação de irregularidades no uso indevido de informações pessoais e reduz a eficácia da proteção que a legislação oferece.

Portanto, a eficácia da LGPD (Brasil, 2018) não depende apenas da existência da norma, mas também de uma fiscalização adequada, da conscientização da população e do investimento constante em segurança da informação e em mecanismos de proteção de dados pessoais.

4.2 RESPONSABILIDADE DA ADMINISTRAÇÃO PÚBLICA

A responsabilidade da Administração Pública consiste no dever que o Estado possui de reparar danos causados aos cidadãos em decorrência da atuação de seus agentes e na falha na prestação dos serviços públicos. No ordenamento jurídico brasileiro, essa responsabilidade encontra fundamento no artigo 37, § 6º da Constituição Federal (Brasil, 1988), que estabelece a responsabilização do poder público pelos danos causados por seus agentes a terceiros.

Nesse cenário, a responsabilidade da Administração Pública torna-se ainda mais relevante, considerando que órgãos governamentais armazenam grande quantidade de informações sensíveis da população. Dados pessoais como CPF, endereço, informações bancárias, registros médicos e documentos oficiais exigem elevado nível de segurança e proteção por parte do Estado.

Em regra, a responsabilidade do Estado é considerada objetiva, ou seja, não há necessidade de comprovação de dolo ou culpa do agente público. Para que exista o dever de indenizar, basta a comprovação do dano sofrido, da conduta administrativa e do nexo causal entre ambos. Dessa forma, caso um

cidadão seja prejudicado em razão de falhas relacionadas à proteção de dados pessoais, o poder público poderá ser responsabilizado pelos prejuízos causados (Carvalho Filho, 2019).

Além disso, quando ocorre omissão da Administração Pública diante do dever de proteção e segurança das informações, a responsabilidade poderá ocorrer em razão da falha na prestação do serviço público. Nesses casos, ataques cibernéticos, vazamentos de dados e falhas de segurança podem gerar consequências jurídicas para o Estado, especialmente quando ficar demonstrada a ausência de medidas preventivas adequadas.

Ataques sofridos por órgãos públicos brasileiros nos últimos anos, como os casos envolvendo o Superior Tribunal de Justiça (STJ) e o sistema ConecteSUS, demonstram a importância da adoção de políticas eficazes de segurança da informação e investimentos em cibersegurança na Administração Pública (G1, 2021).

Dessa forma, observa-se que a responsabilidade da Administração Pública na proteção dos dados pessoais não se limita apenas ao armazenamento das informações, envolvendo também o dever de garantir segurança, prevenção e tratamento adequado dos dados dos cidadãos, conforme previsto na Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) e na Constituição Federal (Brasil, 1988).

4.3 PENALIDADES PREVISTAS NA LGPD

A Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) estabelece uma série de penalidades aplicáveis às instituições e organizações que realizarem tratamento inadequado de dados pessoais ou descumprirem as normas previstas na legislação. Essas sanções possuem o objetivo de garantir maior segurança no tratamento das informações pessoais, incentivar a adoção de medidas preventivas e responsabilizar agentes que atuem de forma negligente na proteção de dados.

Além das penalidades administrativas previstas na LGPD (Brasil, 2018), determinadas condutas relacionadas aos crimes digitais também encontram previsão no Código Penal Brasileiro (Brasil,l 1940) e em legislações específicas, especialmente em situações envolvendo invasão de dispositivos, fraudes eletrônicas, vazamentos de informações e ataques cibernéticos.

Constam do artigo 53 da LGPD (Brasil, 2018) as seguintes penalidades administrativas:

> I – Advertência: aplicada com indicação de prazo para adoção de medidas corretivas;
> II – Multa simples: multa de até 2% do faturamento da pessoa jurídica de direito privado, limitada ao valor máximo de R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
> III- Multa diária: aplicada enquanto permanecer a infração, observados os limites previstos na legislação.
> IV- Publicização da infração: divulgação pública da infração após devidamente apurada e confirmada sua ocorrência;
> V- Bloqueio dos dados pessoais: suspensão temporária do uso dos dados pessoais relacionados à infração até a regularização da situação;
> VI- Eliminação de dados pessoais: exclusão definitiva dos dados pessoais relacionados à infração.

De sua vez o Código Penal (Brasil, 1940) traz:

> Invasão de dispositivo informático
> Artigo 154-A do Código Penal
> Detenção de 1 a 4 anos e multa.
>
> Fraude eletrônica / Estelionato digital
> Artigo 171, §2º-A do Código Penal
> Reclusão de 4 a 8 anos e multa.
>
> Interrupção ou perturbação de serviço telemático ou informático
> Artigo 266 do Código Penal
> Reclusão de 1 a 3 anos e multa.

Importa salientar que o deepfake, que é uma técnica de inteligência artificial que cria vídeos, áudios ou imagens falsos, mas extremamente realistas, manipulando rosto vozes e movimentos humanos (Barbieri, 2026), não possui tipificação específica no Código Penal brasileiro (CP) (Brasil, 1940) até o momento. Entretanto, sua utilização pode enquadrar-se em crimes já previstos na legislação penal, tais como estelionato eletrônico, artigo 171 do CP; falsidade ideológica, artigo 299 do CP e os crimes contra a honra, previstos nos artigos 138 a 140 do CP.

5. MEDIDAS PREVENTIVAS E MECANISMOS DE COMBATE AOS CRIMES CIBERNÉTICOS

O crescimento dos crimes cibernéticos e dos vazamentos de dados pessoais demonstra a necessidade da adoção de medidas preventivas capazes de fortalecer a segurança das informações no ambiente digital. Com o avanço das tecnologias e a crescente digitalização dos serviços públicos e privados, torna-se essencial a implementação de mecanismos voltados à prevenção de ataques cibernéticos, fraudes eletrônicas e acessos não autorizados aos sistemas informáticos.

Entre as principais práticas preventivas destacam-se a utilização de autenticação em dois fatores, criação de senhas fortes, atualização constante de softwares e sistemas operacionais, além do uso de antivírus e ferramentas de proteção digital (Brasil, 2026). Além disso, recomenda-se que usuários e instituições adotem práticas de navegação segura, evitando acessar links suspeitos, realizar downloads de arquivos desconhecidos ou fornecer dados pessoais sem a verificação da autenticidade das plataformas utilizadas. A utilização de cartões virtuais em compras online e a restrição do acesso a serviços bancários em redes Wi-Fi públicas também representam importantes mecanismos de proteção contra fraudes eletrônicas e roubos de dados.

No âmbito corporativo e da Administração Pública, torna-se essencial o investimento contínuo em segurança da informação, incluindo sistemas de monitoramento, controle de acesso, criptografia de dados e capacitação dos usuários e servidores públicos quanto aos riscos relacionados aos crimes digitais.

Em relação aos mecanismos de combate aos crimes cibernéticos, o ordenamento jurídico brasileiro possui legislações específicas voltadas à repressão dessas práticas ilícitas. Entre elas destaca-se a Lei nº 12.737/2012 (Brasil, 2012), conhecida como Lei Carolina Dieckmann, responsável por criminalizar a invasão de dispositivos informáticos e o furto de dados. Além disso, a Lei nº 14.155/2021 (Brasil, 2021) promoveu o aumento das penas relacionadas aos crimes de estelionato eletrônico e fraudes digitais.

Outro ponto importante, refere-se à atuação conjunta entre órgãos públicos e instituições privadas no combate aos crimes cibernéticos. A cooperação entre entidades como a Polícia Federal, delegacias especializadas em crimes digitais e instituições financeiras possibilita maior eficiência na investigação e repressão de fraudes eletrônicas, ataques cibernéticos e demais delitos praticados no ambiente virtual. Além disso, campanhas de conscientização e educação digital possuem papel fundamental na prevenção dos crimes cibernéticos, contribuindo para informar a população acerca dos riscos existentes na internet e das medidas de proteção relacionadas à segurança das informações pessoais.

Dessa forma, observa-se que o combate aos crimes cibernéticos depende não apenas da existência de mecanismos tecnológicos de proteção, mas também da conscientização da sociedade, da atuação das autoridades competentes e da aplicação efetiva das legislações voltadas à proteção de dados e à segurança digital.

6. DESAFIOS FUTUROS

O avanço das tecnologias digitais e o crescimento dos crimes cibernéticos representam desafios cada vez maiores para a proteção de dados pessoais. A evolução da Inteligência Artificial, especialmente com o uso de deepfakes e golpes virtuais automatizados a crescente digitalização dos serviços públicos, torna os ataques digitais mais sofisticados e difíceis de identificar. Devido a isso exigem-se maiores investimentos em cibersegurança, atualização dos sistemas e capacitação de servidores públicos para prevenção de vazamentos e ataques cibernéticos, necessidade de atualização constante das legislações relacionadas aos crimes digitais, uma vez que as novas práticas criminosas evoluem rapidamente no ambiente virtual. A conscientização da população sobre segurança digital também se torna essencial para redução de fraudes e utilização indevida de dados pessoais.

Dessa forma, observa-se que a proteção de dados e o combate aos crimes cibernéticos dependem do fortalecimento das políticas de segurança da

informação, da evolução das legislações e da conscientização da sociedade diante dos riscos presentes no ambiente digital.

CONCLUSÃO

O presente trabalho teve como objetivo analisar a importância da proteção de dados pessoais diante do crescimento dos crimes cibernéticos, especialmente no âmbito da Administração Pública, destacando o papel da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018) como instrumento fundamental na garantia da privacidade, segurança da informação e proteção dos direitos fundamentais dos cidadãos.

Ao longo da pesquisa, verificou-se que o avanço das tecnologias digitais e a crescente digitalização dos serviços públicos contribuíram significativamente para o aumento dos riscos relacionados aos vazamentos de dados, fraudes eletrônicas e demais crimes praticados no ambiente virtual. Observou-se ainda que órgãos públicos e instituições privadas passaram a lidar diariamente com grande volume de informações pessoais, tornando essencial a adoção de medidas eficazes de segurança da informação e cibersegurança.

Cabe destacar ainda que a LGPD (Brasil, 2018) representa importante mecanismo jurídico de proteção dos dados pessoais, estabelecendo princípios, direitos, deveres e penalidades voltadas à responsabilização de instituições que realizem tratamento inadequado das informações dos usuários. Entretanto, apesar dos avanços proporcionados pela legislação, ainda existem desafios relacionados à efetividade da norma, à fiscalização, à adaptação tecnológica e ao combate às constantes evoluções dos crimes cibernéticos.

Também foi possível observar que a utilização inadequada de tecnologias como a Inteligência Artificial pode potencializar riscos relacionados à privacidade e à segurança digital, especialmente diante do crescimento de práticas como deepfakes, golpes virtuais e manipulação de informações no ambiente digital.

Dessa forma, conclui-se que a proteção de dados pessoais deve ser tratada como elemento essencial para garantia da privacidade, segurança e confiança da sociedade no ambiente digital. Assim, torna-se indispensável o fortalecimento das políticas públicas de segurança da informação, a conscientização da população acerca dos riscos cibernéticos e a aplicação efetiva da legislação vigente, visando reduzir vulnerabilidades e promover maior proteção aos dados pessoais no contexto da Administração Pública e da sociedade contemporânea.

REFERÊNCIAS

BARBIERI, Maurício. Deepfake: o que é, como funciona e implicações jurídicas. 26/03/2026. Disponível em: https://www.barbieriadvogados.com/deepfake-o-que-e-como-funciona-brasil/ Acesso em: 25 mai. 2026.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). Segurança da informação e proteção de dados pessoais. Brasília: ANPD, 2024.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988.

BRASIL. Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal. Diário Oficial da União: Brasília, DF, 1940.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Código Civil. Diário Oficial da União: Brasília, DF, 2002.

BRASIL. Lei nº 12.737, de 30 de novembro de 2012. Lei Carolina Dieckmann. Diário Oficial da União: Brasília, DF, 2012.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União: Brasília, DF, 2018.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Lei do Governo Digital. Diário Oficial da União: Brasília, DF, 2021.

BRASIL. [Lei Geral de Proteção de Dados (2018)]. Lei Geral de Proteção de Dados Pessoais : Lei no 13.709/2018. – Brasília, DF : Senado Federal, Coordenação de Edições Técnicas, 2024.

BRASIL. Polícia Federal. Combate a crimes cibernéticos. Disponível em: https://www.gov.br/pf/pt-br/assuntos/combate-a-crimes-ciberneticos. Acesso em 25 mai.2026.

BRASIL. São Paulo. Tribunal de Justiça do Estado de São Paulo. Secretaria de Governança de Sistemas. Infoeproc. Edição n. 07. Autenticação em Dois Fatores (2FA) no eproc. Disponível em: https://www.tjsp.jus.br/Download/EPROC/InfoEproc/Infoeproc7.pdf Acesso em 25 de mai. 2026.

BRASIL. SUPERIOR TRIBUNAL DE JUSTIÇA - STJ. Comunicado oficial sobre ataque hacker. 19/11/2020 Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/19112020-Comunicado-da-Presidencia-do-STJ.aspx Acesso em 25 mai. 2026.

CÂMARA, Vitor. A Importância da Proteção de Dados Pessoais na Era Digital. 27/05/2024. Jus Brasil. Disponível em: https://www.jusbrasil.com.br/artigos/a-importancia-da-protecao-de-dados-pessoais-na-era-digital/2517769819. Acesso em 25 mai.2026.

CAPANEMA, Walter Aranha. A responsabilidade civil na Lei Geral de Proteção de Dados. Cadernos Jurídicos, São Paulo, v. 21, n. 53, p. 163–170, 2020.

CARVALHO FILHO, José dos Santos. Manual de Direito Administrativo. 33ª ed. São Paulo: Atlas, 2019.

CERT.br. Estatísticas de phishing. Disponível em: https://stats.cert.br/phishing/ Acesso em 25 mai.2026.

DI PIETRO, Maria Sylvia Zanella. Direito Administrativo. 36. ed. Rio de Janeiro: Forense, 2023.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. 2. ed. São Paulo: Thomson Reuters, 2020.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. Revista de Direito Brasileira, v. 23, n. 9, 2020.

G1a. Ataque ao ConecteSUS. Jornal Nacional. 10/12/2021. Disponível em: https://g1.globo.com/jornal-nacional/noticia/2021/12/10/ataque-hacker-ao-site-do-ministerio-da-saude-tira-do-ar-o-conectesus.ghtml Acesso em 25 mai. 2026.

G1b. Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber. Número é maior do que a população do país, estimada em 212 milhões, porque inclui dados de falecidos. Informações expostas incluem CPF, nome, sexo e data de nascimento, além de uma tabela com dados de veículos e uma lista com CNPJs. Origem dos dados ainda é desconhecida. 28/01/2021. Disponível em: Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber | G1 Acesso em 25 mai.2026.

GARCIA, Lara Rocha et. al. Lei Geral de Proteção de Dados (LGPD): Guia de implantação. Google Books. Editora Blucher, 24 de jul. de 2020. Disponível em: Lei Geral de Proteção de Dados (LGPD): Guia de implantação - Lara Rocha Garcia, Edson Aguilera-Fernandes, Rafael Augusto Moreno Gonçalves, Marcos Ribeiro Pereira-Barretto - Google Livros. Acesso em 25 de mai.2026.

KASPERSKY. O que é cibercrime. Disponível em: https://www.kaspersky.com.br/resource-center/threats/what-is-cybercrime Acesso em 25 mai. 2026.

KATTEL, R.; MERGEL, I. Estonia's digital transformation. UCL Working Paper, 2018.

KOGA, Matheus. Golpe do Pix como funciona e como se proteger. Especialistas explicam como criminosos agem e orientam como evitar fraudes. 25/05/2026. Disponível em: https://www.bandab.com.br/seguranca/golpe-do-pix-como-funciona-como-se-proteger/ Acesso em: 25 mai.2026.

LIMA RAPÔSO, C. F. Et. al. LGPD e tecnologia da informação. Uberlândia: RACE 2019.

MENDES, Laura Schertel. Privacidade, proteção de dados e defesa do consumidor. São Paulo: Saraiva, 2014.

MEIRELLES, Hely Lopes. Direito Administrativo Brasileiro. 49. ed. São Paulo: Malheiros, 2023.

ORGANIZAÇÃO PARA A COOPERAÇÃO E DESENVOLVIMENTO ECONÔMICO (OECD). OECD Economic Surveys: Estonia 2019. Paris: OECD Publishing, 2019.

PINHEIRO, Patrícia Peck. Direito Digital. 7. ed. São Paulo: Saraiva, 2021.

SAFERNET BRASIL. Crimes na Web. Mapeamento da SaferNet identifica deepfakes sexuais em escolas em 10 dos 27 estados brasileiros. Imagens de Abuso e Exploração Sexual Infantil. Disponível em: https://new.safernet.org.br/content/mapeamento-da-safernet-identifica-deepfakes-sexuais-em-escolas-em-10-dos-27-estados Acesso em 25 mai. 2026.

TRIBUNAL DE CONTAS DA UNIÃO (TCU). Referencial básico de governança. Brasília: TCU, 2020.