Privacidade em risco: desafios na proteção do Cadastro de Pessoas Físicas - CPF

Vitor Felipe B. A. Carneiro[1], Felipe Fonteles Belo[1], Helio Carrara B. Junior[1], Bianca Cristina O. E. S. Silva[1], Nelcileno V. S. Araujo[1]

[1]Instituto de Computação - Programa Pós-Graduação em Computação Aplicada (PPGCOMP) - Universidade Federal de Mato Grosso (UFMT)
Av. Fernando Correia da Costa, nº 2367 Bairro Boa Esperança – CEP:78060-900 – Cuiabá - MT

vitorfelip@gmail.com, felipebelo@live.com, heliocarrara@gmail.com, bianca.ces81@gmail.com, nelcileno@ic.ufmt.br

Abstract. *This article examines the risks and challenges associated with the protection of the Brazilian individual taxpayer registry (CPF), a central yet highly vulnerable personal identifier. Based on a legal, technological, and social perspective, the study highlights recurring problems such as massive data breaches, weak authentication practices, and the widespread use of CPF in public and private services. The analysis emphasizes the importance of the General Data Protection Law (LGPD), the role of institutions, and the need for digital education among citizens. It concludes that effective CPF protection requires a combination of legislation, technology, and awareness to safeguard privacy and reduce identity fraud in Brazil.*

Resumo. *Este artigo analisa os riscos e desafios relacionados à proteção do Cadastro de Pessoa Física (CPF), dado essencial e altamente vulnerável no Brasil. A pesquisa destaca problemas recorrentes como vazamentos massivos, práticas frágeis de autenticação e uso indiscriminado do CPF em serviços públicos e privados. A análise aborda a importância da Lei Geral de Proteção de Dados (LGPD), o papel das instituições e a necessidade de educação digital para os cidadãos. Conclui-se que a proteção efetiva do CPF depende da integração entre legislação, tecnologia e conscientização, visando preservar a privacidade e reduzir fraudes de identidade no país.*

1. Introdução

A sociedade contemporânea está cada vez mais dependente da tecnologia digital, situação que amplia de forma exponencial o volume de dados pessoais coletados, processados e compartilhados diariamente. Nesse contexto, a privacidade tornou-se um dos bens mais valiosos e, ao mesmo tempo, um dos mais vulneráveis, uma vez que a utilização inadequada dessas informações pode resultar em danos irreparáveis aos cidadãos [Solove 2021].

No Brasil, o Cadastro de Pessoa Física (CPF) assume papel central na vida civil, social e econômica do indivíduo. Esse identificador único é solicitado em praticamente todas as esferas de interação, desde serviços públicos básicos até relações comerciais complexas, como a abertura de contas bancárias ou contratação de serviços digitais [Doneda 2019]. Essa centralidade, embora facilite processos burocráticos, também

transforma o CPF em alvo recorrente de criminosos cibernéticos, que exploram vulnerabilidades em sistemas e a falta de cuidados no manuseio desse dado.

Relatórios recentes demonstram que o Brasil figura entre os países com maior número de vazamentos de dados pessoais, frequentemente envolvendo milhões de CPFs expostos em bases ilegais disponíveis na internet. Esses incidentes não apenas comprometem a privacidade, mas também facilitam a prática de fraudes de identidade, golpes financeiros e engenharia social, ampliando o prejuízo econômico e moral para a população [CERT.br 2023].

Além disso, observa-se uma fragilidade histórica na utilização do CPF como chave primária de autenticação. Muitas instituições utilizam apenas o número de cadastro como critério de identificação, sem a adoção de medidas complementares de segurança. Essa prática amplia o risco de acesso indevido a serviços e amplia a vulnerabilidade das vítimas [CERT.br 2023].

Diante desse cenário, a proteção do CPF deve ser analisada não apenas sob a ótica tecnológica, mas também jurídica e social. A entrada em vigor da Lei Geral de Proteção de Dados (LGPD) estabeleceu um marco regulatório para o tratamento de dados pessoais no Brasil, reconhecendo o CPF como dado pessoal sujeito a salvaguardas específicas [Brasil 2018]. Contudo, a aplicação prática da legislação ainda enfrenta entraves relacionados à fiscalização, à conscientização dos cidadãos e à adequação das empresas aos padrões de segurança exigidos [Pellegrini 2021].

Nesse sentido, este artigo tem como objetivo analisar os riscos e desafios que envolvem a proteção do CPF, discutindo suas vulnerabilidades mais recorrentes, bem como apresentar as principais medidas de mitigação que podem contribuir para a preservação da privacidade e a redução de fraudes digitais no país.

2. Metodologia

Este estudo caracteriza-se como uma pesquisa exploratória e qualitativa, fundamentada em análise bibliográfica e documental. O objetivo central não foi a produção de dados empíricos inéditos, mas a interpretação crítica de informações já disponíveis em diferentes fontes.

Foram consideradas normativas legais nacionais e internacionais, em especial a Lei Geral de Proteção de Dados (LGPD) e o Regulamento Geral de Proteção de Dados da União Europeia (GDPR). Além disso, incorporaram-se relatórios técnicos e estatísticos publicados por instituições como o Comitê Gestor da Internet no Brasil (NIC.br), o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil (CERT.br) e a Autoridade Nacional de Proteção de Dados (ANPD).

Complementarmente, realizou-se uma revisão de literatura com base em obras de referência teórica na área de privacidade e proteção de dados, como os trabalhos de Solove (2021), Westin (1967), Doneda (2019) e Pellegrini (2021). Também foram examinados estudos de caso e notícias técnicas sobre megavazamentos de dados no Brasil e suas repercussões sociais e econômicas.

A análise foi organizada em três eixos principais:

1. Jurídico, examinando o papel da legislação e das instituições na salvaguarda do CPF;

2. Tecnológico, avaliando vulnerabilidades de sistemas e práticas de segurança da informação;
3. Social, abordando percepções de privacidade, cultura de compartilhamento de dados e impactos para os cidadãos.

Esse procedimento metodológico possibilitou compreender os riscos associados ao uso do CPF de forma integrada, articulando dimensões legais, técnicas e sociais, e oferecendo uma visão crítica sobre os desafios de proteção desse identificador no Brasil.

3. Privacidade e a Exposição do CPF

A privacidade, tradicionalmente concebida como o direito de estar só, evoluiu para um conceito mais abrangente que envolve o controle sobre a coleta, utilização e compartilhamento das informações pessoais. No contexto digital, esse direito está diretamente relacionado à proteção de dados, uma vez que o tratamento inadequado pode expor indivíduos a riscos de discriminação, fraude e violação de sua autonomia [Westin 1967], [Solove 2021].

Essa percepção sobre a importância da privacidade, no entanto, nem sempre se traduz em um entendimento claro sobre a proteção de dados no ambiente digital. A forma como os próprios cidadãos interpretam o que é privacidade revela uma visão mais abstrata do que prática. Uma pesquisa recente do Comitê Gestor da Internet no Brasil ilustra essa percepção:

Como demonstra o gráfico na Figura 1 do relatório do Comitê Gestor da Internet no Brasil, a maioria dos entrevistados associa a privacidade a conceitos amplos como "liberdade" e "individualidade", enquanto uma parcela menor a conecta diretamente à "proteção de dados" e ao "controle". Essa dissociação entre o valor abstrato da privacidade e as práticas concretas de proteção de dados ajuda a explicar por que um identificador tão crítico como o CPF é, muitas vezes, compartilhado sem a devida avaliação dos riscos, sendo tratado como um dado pessoal comum, embora sua natureza estratégica o torne especialmente sensível na realidade brasileira [NIC.br 2022].

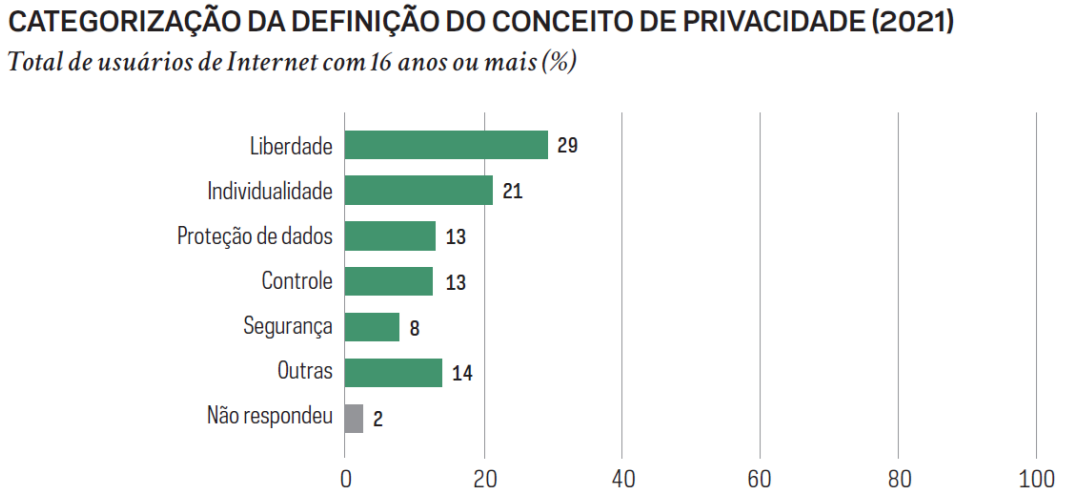

Figura 1. "Categorização da definição do conceito de privacidade (2021)"

No Brasil, a LGPD define dado pessoal como toda informação relacionada a uma pessoa natural identificada ou identificável. O CPF enquadra-se claramente nessa

definição, pois constitui um identificador único que permite a individualização do cidadão em diversas relações jurídicas e sociais [Brasil 2018]. Sua natureza estratégica faz com que seja considerado um dos dados mais sensíveis na realidade brasileira, ainda que a legislação o classifique apenas como dado pessoal comum.

O uso massivo do CPF em cadastros públicos e privados amplia a superfície de exposição e, consequentemente, o risco de vazamentos. Bancos de dados de e-commerces, aplicativos de delivery, planos de saúde, sistemas de crédito e até órgãos governamentais frequentemente solicitam esse número como requisito básico de identificação. Em muitos casos, não há critérios rigorosos de segurança, o que facilita o acesso indevido por terceiros mal-intencionados [Doneda 2019].

Casos recentes de grande vazamento de dados como a da Empresa Serasa, que envolveram a exposição de milhões de CPFs em fóruns clandestinos da internet, demonstram a fragilidade dos sistemas de proteção adotados por instituições públicas e privadas. Segundo a ANPD (2021), mais de 220 milhões de registros contendo CPFs já circularam ilegalmente em redes digitais, o que revela um cenário de risco permanente para toda a população brasileira.

Além dos vazamentos em larga escala, o CPF também é utilizado em práticas de engenharia social e fraudes de identidade. Criminosos exploram a confiança que empresas e órgãos depositam nesse número para obter crédito, realizar compras ou abrir contas bancárias em nome de terceiros. Esse tipo de golpe é especialmente prejudicial porque compromete não apenas a privacidade, mas também a reputação e a vida financeira das vítimas [CERT.br 2023].

Assim, o CPF representa um paradoxo: ao mesmo tempo em que é indispensável para a vida civil e econômica, também é uma das informações mais vulneráveis e cobiçadas no ecossistema digital brasileiro.

4. Desafios na Proteção

A proteção do CPF enfrenta desafios complexos que envolvem aspectos técnicos, jurídicos e culturais. Um dos principais problemas é a utilização desse dado como elemento central de autenticação em diversos serviços. Muitas instituições, públicas e privadas, utilizam apenas o CPF como critério de identificação, sem exigir mecanismos adicionais de segurança. Essa prática amplia a vulnerabilidade dos sistemas, pois o número pode ser facilmente obtido em cadastros, formulários ou em bases de dados expostas [Doneda 2019].

Outro obstáculo relevante é a fragilidade das bases de dados de órgãos governamentais e empresas privadas. Diversos relatórios apontam que sistemas de armazenamento de informações no Brasil apresentam falhas de segurança, ocasionando vazamentos em larga escala. O megavazamento revelado em 2021, que expôs informações de mais de 220 milhões de brasileiros, incluindo CPFs, demonstrou a gravidade do problema e a necessidade urgente de medidas de proteção mais robustas [DfndrLab 2021].

Esses incidentes de segurança e a exposição contínua de informações alimentam uma crescente desconfiança por parte da população. O receio em fornecer dados pessoais, especialmente aqueles considerados sensíveis, é um reflexo direto dessa vulnerabilidade, como aponta o gráfico da figura 2 seguir:

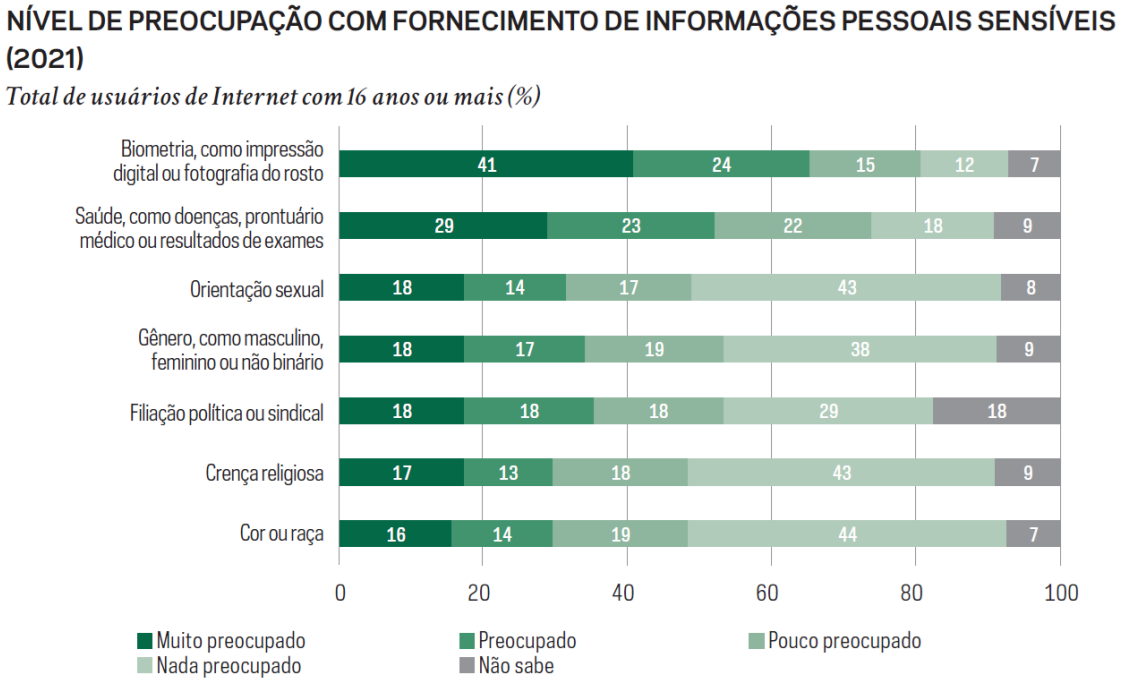

Figura 2. "Nível de preocupação com fornecimento de informações pessoais sensíveis (2021)"

Observa-se que as porcentagens apresentadas na Figura 2 reproduzem os valores originais do relatório oficial do Comitê Gestor da Internet no Brasil (NIC.br, 2022). As somas não totalizam exatamente 100% porque cada categoria de resposta foi considerada de forma independente, conforme metodologia da pesquisa Painel TIC 2021 descrita no relatório. Esse formato reflete arredondamentos e a possibilidade de respostas múltiplas, sem comprometer a interpretação dos resultados.

Os dados Apresentados na Figura acima revelam um elevado nível de preocupação dos usuários ao compartilhar informações como dados de saúde, financeiros e de geolocalização. Ironicamente, apesar dessa apreensão, o CPF, que frequentemente serve como chave de acesso a muitos desses dados, continua sendo solicitado e fornecido de forma massiva em múltiplos serviços. Essa prática contradiz diretamente os princípios de minimização de dados estabelecidos pela LGPD e reforça a cultura de exposição generalizada [NIC.br 2022].

Além dos incidentes massivos, a reutilização do CPF em diferentes cadastros amplia a superfície de ataque. O mesmo número é solicitado em lojas virtuais, planos de telefonia, sistemas bancários e até em simples cadastros de fidelidade. A ausência de políticas de minimização de dados contraria os princípios estabelecidos pela LGPD e reforça a ideia de que a exposição do CPF é generalizada [Brasil 2018].

O cenário torna-se ainda mais crítico quando se considera a atuação de criminosos que utilizam CPFs obtidos ilegalmente para práticas de engenharia social. Ao combinar o número de cadastro com outras informações facilmente disponíveis na internet, como nome completo ou endereço, fraudadores conseguem aplicar golpes sofisticados de identidade, abrindo contas bancárias ou solicitando crédito em nome das vítimas [CERT.br 2023].

Outro desafio relevante diz respeito à atuação das instituições responsáveis pela fiscalização do uso do CPF e pela garantia da aplicação da LGPD. Apesar de a criação da Autoridade Nacional de Proteção de Dados (ANPD) ter representado um avanço regulatório importante, sua estrutura ainda é limitada em termos de orçamento e pessoal, o que dificulta o monitoramento efetivo de práticas abusivas e o acompanhamento de incidentes em larga escala. Além disso, órgãos como Ministério Público, Procon e entidades de defesa do consumidor enfrentam obstáculos para responsabilizar empresas que utilizam o CPF de forma indiscriminada, seja pela ausência de mecanismos ágeis de investigação, seja pela sobrecarga de demandas. Essa fragilidade institucional contribui para a perpetuação de um ambiente em que o CPF é explorado com pouca ou nenhuma restrição, ampliando a vulnerabilidade da população.

Por fim, destaca-se a falta de conscientização da população. Muitos cidadãos compartilham o CPF indiscriminadamente, sem avaliar os riscos associados. Esse comportamento, aliado à ausência de políticas de segurança efetivas nas instituições, potencializa o ciclo de vulnerabilidade e compromete a privacidade em escala nacional [Solove 2021].

5. Medidas de Proteção

A proteção do CPF exige uma abordagem multidimensional que combine legislação, tecnologia e conscientização social. Do ponto de vista jurídico, a LGPD estabeleceu princípios fundamentais para o tratamento adequado das informações pessoais, como finalidade, necessidade e segurança [Brasil 2018]. A atuação da Autoridade Nacional de Proteção de Dados (ANPD) é essencial para fiscalizar o cumprimento da norma, aplicar sanções e orientar boas práticas de governança. No entanto, a efetividade dessas medidas depende de investimentos institucionais e da consolidação de uma cultura de proteção de dados no país [Pellegrini 2021].

No campo tecnológico, a adoção de mecanismos de segurança robustos é indispensável para mitigar os riscos de vazamento e uso indevido do CPF. Práticas como a criptografia de bases de dados, a anonimização em situações nas quais não seja necessária a identificação direta do indivíduo e a utilização de autenticação multifator são estratégias eficazes para dificultar o acesso de criminosos a informações sensíveis [Kaspersky 2023]. Além disso, a segmentação de cadastros e a aplicação de políticas de minimização de dados reduzem a exposição ao limitar a coleta apenas ao que for estritamente necessário [Solove 2021].

Experiências internacionais demonstram que a proteção de identificadores pessoais pode ser fortalecida por meio de boas práticas já consolidadas em outras jurisdições. Na União Europeia, por exemplo, a GDPR impõe a adoção obrigatória do princípio da minimização de dados, restringindo a coleta de identificadores como o NIF apenas quando estritamente necessário [GDPR 2016]. Nos Estados Unidos, embora não exista uma legislação geral, diferentes setores aplicam estratégias de diversificação de identificadores, de modo que um único número não concentre todo o risco de autenticação e identificação [HIPAA 1996]. Tais medidas poderiam inspirar a realidade brasileira, reduzindo a centralidade do CPF e estimulando o desenvolvimento de mecanismos alternativos de autenticação mais seguros.

Outra medida fundamental consiste na capacitação de equipes técnicas e jurídicas para lidar com incidentes de segurança. Empresas e órgãos públicos devem

possuir planos de resposta a incidentes que contemplem desde a identificação rápida do vazamento até a comunicação imediata às vítimas e às autoridades competentes. A transparência nesses processos é indispensável para restaurar a confiança dos cidadãos e minimizar os impactos sociais e econômicos dos ataques [CERT.br 2023].

Além das medidas institucionais e tecnológicas, é fundamental observar como a percepção de risco já influencia o comportamento dos próprios usuários no ambiente digital. A preocupação com a privacidade tem levado muitos a reconsiderar suas ações online, evitando situações que poderiam comprometer seus dados, o que demonstra uma mudança de postura.

A Figura 03 ilustra dados apresentados no relatório do Comitê Gestor da Internet no Brasil evidenciando que uma parcela significativa dos usuários já adota uma postura mais cautelosa, deixando de instalar aplicativos ou de preencher cadastros por receio quanto ao uso de suas informações. Essa mudança de comportamento, embora muitas vezes reativa, sinaliza uma oportunidade: a população está se tornando mais atenta. Isso reforça a urgência e a potencial eficácia de campanhas de educação digital para capacitar os cidadãos a protegerem ativamente seus dados, como o CPF, um ponto crucial para a construção de uma cultura de segurança digital no país [NIC.br 2022].

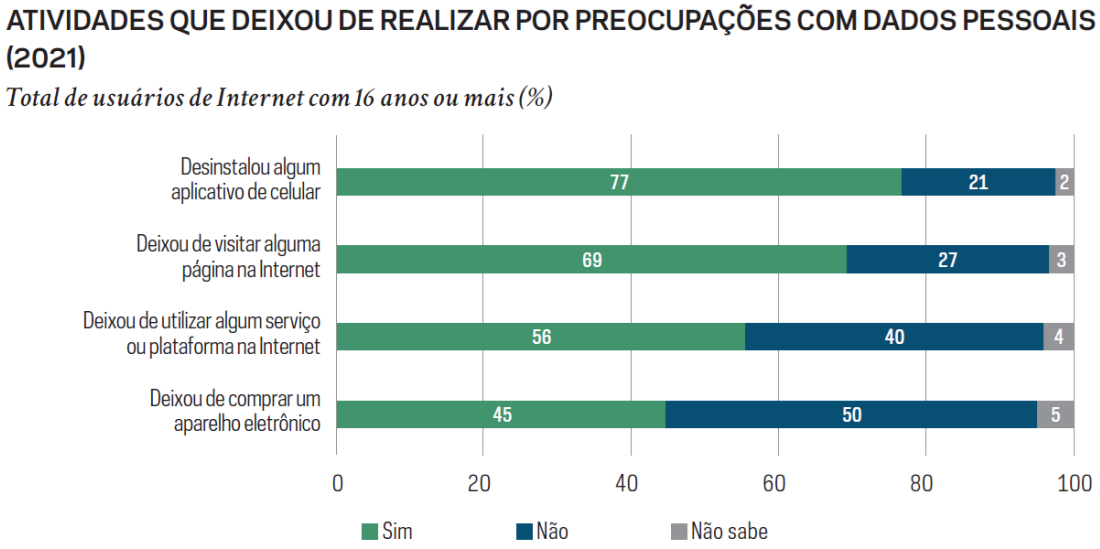

Figura 3. "Atividades que deixou de realizar por preocupações com dados pessoais (2021)"

Por fim, destaca-se a necessidade de educação digital da população. Muitos usuários compartilham o CPF de forma indiscriminada, sem compreender os riscos envolvidos. Pesquisas recentes reforçam a percepção de que a população brasileira ainda carece de conscientização em relação à proteção de dados pessoais. Segundo levantamento do Comitê Gestor da Internet no Brasil, em 2023, 67% dos usuários de internet afirmaram ler as políticas de privacidade, mas, ao mesmo tempo, 51% concordam com os termos sem ler o que dizem [NIC.br 2024]. Essa contradição evidencia uma falta de engajamento e compreensão sobre como seus dados são tratados, o que amplia a vulnerabilidade do CPF, já que cidadãos continuam a fornecê-lo em cadastros de procedência duvidosa, sem avaliar os riscos envolvidos. Campanhas de conscientização podem orientar cidadãos sobre práticas seguras, como evitar fornecer o

número em cadastros de procedência duvidosa, monitorar movimentações financeiras e utilizar ferramentas de verificação de crédito para identificar possíveis usos indevidos [Doneda 2019]. Nesse sentido, a soma de políticas públicas, responsabilidade institucional e participação ativa da sociedade representa o caminho mais promissor para garantir maior proteção ao CPF e, consequentemente, à privacidade no Brasil.

6. Conclusão

O CPF constitui um elemento central da vida civil e econômica no Brasil, porém sua ampla utilização e exposição o tornam um dos dados pessoais mais vulneráveis do país. A análise desenvolvida neste artigo evidenciou que os riscos associados a esse identificador decorrem tanto da fragilidade estrutural de sistemas públicos e privados quanto do uso indiscriminado em cadastros e serviços digitais, o que o transforma em alvo constante de fraudes e vazamentos.

Os megavazamentos recentes demonstram que a proteção do CPF não pode ser encarada apenas como responsabilidade individual do cidadão, mas sim como um desafio coletivo que envolve Estado, empresas e sociedade. O número crescente de fraudes de identidade e golpes associados ao uso indevido do CPF reforça a urgência de políticas de segurança mais eficazes, acompanhadas da adoção de tecnologias capazes de reduzir a superfície de ataque.

Este estudo, de natureza exploratória e qualitativa, baseado em pesquisa bibliográfica e documental, contribuiu ao integrar as dimensões jurídica, tecnológica e social da proteção do CPF. Ao reunir legislações, relatórios técnicos e literatura especializada, buscou-se oferecer uma visão crítica e abrangente dos principais desafios enfrentados atualmente no Brasil.

A LGPD representou um avanço significativo ao reconhecer o CPF como dado pessoal e estabelecer regras para seu tratamento. Entretanto, sua efetividade depende da capacidade de fiscalização da ANPD, da adequação das instituições e da consolidação de uma cultura de privacidade que envolva toda a sociedade. Nesse cenário, a conjugação entre medidas jurídicas, soluções tecnológicas e conscientização cidadã surge como o caminho mais promissor para mitigar riscos.

Conclui-se que a proteção do CPF exige um esforço integrado em que legislação, tecnologia e educação se complementem para garantir maior segurança e preservar o direito fundamental à privacidade. Futuras pesquisas podem aprofundar a análise de alternativas ao uso exclusivo do CPF como identificador, bem como investigar mecanismos inovadores de autenticação e estratégias de fiscalização mais eficientes para a realidade brasileira.

Referencias

ANPD. (2021). ANPD está apurando no caso do vazamento de dados de mais de 220 milhões de pessoas. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-esta-apurando-no-caso-do-vazamento-de-dados-de-mais-de-220-milhoes-de-pessoas.

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

CERT.br. (2023). Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação no Brasil – TIC Domicílios 2022. Comitê Gestor da Internet no Brasil.

DfndrLab. (2021). Megavazamento de dados de 223 milhões de brasileiros. PSafe Blog.

Doneda, D. (2019). Da Privacidade à Proteção de Dados Pessoais. Editora RT.

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Union.

Kaspersky. (2023). O que é criptografia de dados?. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption.

NIC.br. (2022). Privacidade e Proteção de Dados Pessoais: Perspectivas de indivíduos, empresas e organizações públicas no Brasil. Comitê Gestor da Internet no Brasil.

NIC.br. (2024). Privacidade e Proteção de Dados Pessoais 2023: Perspectivas de indivíduos, empresas e organizações públicas no Brasil. Comitê Gestor da Internet no Brasil.

Pellegrini, G. (2021). A Efetividade da Lei Geral de Proteção de Dados. Editora Foco.

Solove, D. J. (2021). Understanding Privacy. Harvard University Press.

U.S. Department of Health and Human Services. (1996). Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Westin, A. F. (1967). Privacy and Freedom. Atheneum.