

FAHESP-Faculdade de Ciências Humanas, Exatas e da Saúde do Piauí.

IESVAP- Instituto de Educação Superior do Vale do Parnaíba LTDA.

CURSO DE DIREITO- Disciplinas de Trabalho de Conclusão de Curso.

JOÃO VICTOR BIZERRA PEREIRA

**A PROTEÇÃO DE DADOS NA ERA DIGITAL: UM ESTUDO SOBRE CLIENTES
DO BPC LOAS.**

ORIENTADOR: GEILSON SILVA PEREIRA

PARNAÍBA-PI

2025

A Proteção de Dados na Era Digital: Um Estudo sobre Clientes do BPC LOAS

João Victor Bizerra Pereira

RESUMO: Este artigo investiga os desafios e a importância da proteção de dados pessoais dos beneficiários do Benefício de Prestação Continuada (BPC/LOAS), em um contexto marcado pela crescente digitalização dos serviços públicos. Considerando a sensibilidade das informações envolvidas como dados de saúde e condição socioeconômica, a pesquisa propõe uma reflexão crítica sobre os riscos associados ao uso indevido ou vazamento desses dados e os impactos negativos que podem incidir sobre uma população já socialmente vulnerável. A metodologia adotada é o Estudo de Caso, conforme delineado por Prodanov e Freitas (2013), com base em um marco teórico centrado na proteção de dados pessoais, vulnerabilidade social e na aplicação da Lei Geral de Proteção de Dados (LGPD) — Lei nº 13.709/2018. O estudo analisa ainda os avanços trazidos pela digitalização dos serviços, como o impacto positivo do aplicativo “Meu INSS” na otimização do atendimento e redução de filas, contrapondo esses benefícios aos riscos de exposição digital enfrentados pelos beneficiários. São discutidas as fraudes mais recorrentes, a relação entre o BPC e o combate à fome e as melhores práticas para fortalecer a privacidade e segurança da informação. Por fim, conclui-se que a proteção de dados não deve ser tratada como uma mera formalidade administrativa, mas como um elemento fundamental para garantir a dignidade, a segurança e os direitos dos beneficiários do BPC LOAS no cenário digital contemporâneo.

PALAVRAS-CHAVE: Proteção de Dados, LGPD, BPC LOAS, Vulnerabilidade Social, Parnaíba.

ABSTRACT: This article investigates the challenges and importance of protecting the personal data of beneficiaries of the Continuous Cash Benefit (BPC/LOAS), within a context marked by the increasing digitalization of public services. Considering the sensitivity of the information involved such as health data and socioeconomic status the study offers a critical reflection on the risks associated with the misuse or leakage of such data and the potential negative impacts on an already socially vulnerable population. The research adopts a Case Study methodology, as outlined by Prodanov and Freitas (2013), based on a theoretical framework focused on personal data protection, social vulnerability, and the application of the General Data Protection Law (LGPD)—Law No. 13.709/2018. The study also analyzes the advancements brought by

digitalization, such as the positive impact of the “*Meu INSS*” application in streamlining services and reducing queues, while also addressing the digital exposure risks faced by beneficiaries. Common types of fraud, the role of BPC in combating hunger, and best practices for enhancing data privacy and security are also discussed. The study concludes that data protection should not be treated as a mere administrative formality but as a fundamental element in safeguarding the dignity, security, and rights of BPC LOAS beneficiaries in the contemporary digital era.

KEYWORDS: Data Protection, LGPD, BPC LOAS, Social Vulnerability.

1. INTRODUÇÃO

A crescente digitalização dos serviços públicos e privados traz consigo inúmeras vantagens em termos de eficiência e acesso. No entanto, essa transformação também eleva os riscos relacionados à privacidade e à segurança dos dados pessoais, especialmente para populações em situação de vulnerabilidade social, como os beneficiários do Benefício de Prestação Continuada (BPC) da Lei Orgânica da Assistência Social (LOAS). Nesse cenário, a proteção de dados emerge não apenas como um imperativo legal, mas como um pilar essencial para a garantia da dignidade humana no ambiente digital, conforme apontado por Doneda (2019), que destaca a centralidade do consentimento e da autodeterminação informativa para a tutela da privacidade na era digital.

O BPC é um benefício assistencial garantido pela Constituição Federal e operacionalizado pelo Instituto Nacional do Seguro Social (INSS), que assegura um salário mínimo mensal a idosos com 65 anos ou mais e a pessoas com deficiência de qualquer idade que comprovem não possuir meios de prover a própria vida.

Este artigo se propõe a investigar os desafios e a importância da proteção de dados pessoais desses beneficiários na era digital, considerando a sensibilidade das informações envolvidas (dados de saúde, condição socioeconômica, etc.) e os potenciais impactos negativos de seu uso indevido ou vazamento propondo reflexões importantes sobre as melhores práticas e estratégias que podem ser implementadas para fortalecer a privacidade e a segurança dos dados dos clientes do BPC LOAS. A Metodologia dessa pesquisa será a abordagem de Estudo de Caso, assim como Prodanov e Freitas (2013) explicam:

O estudo de caso consiste em coletar e analisar informações sobre determinado indivíduo, uma família, um grupo ou uma comunidade, a fim de estudar aspectos variados de sua vida, de acordo com o assunto da pesquisa. É um tipo de pesquisa



qualitativa e/ou quantitativa, entendido como uma categoria de investigação que tem como objeto o estudo de uma unidade de forma aprofundada, podendo tratar-se de um sujeito, de um grupo de pessoas, de uma comunidade etc. São necessários alguns requisitos básicos para sua realização, entre os quais, severidade, objetivação, originalidade e coerência.

Essas práticas incluem a necessidade de robustos sistemas de segurança da informação, a implementação de políticas de minimização da coleta de dados, a adoção de técnicas de anonimização e pseudonimização, que de acordo com Autoridade Nacional de Proteção de Dados (ANPD) definiu que “A LGPD¹ tratou, em seu art. 5º, incisos III e XI, sobre a anonimização como um processo em que um agente de tratamento utiliza determinadas técnicas para desvincular, de forma direta ou indireta, o dado pessoal do seu titular por meio do uso de técnicas de processamento de dados.” E de acordo com LGPD “Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (art. 13, § 4º, da LGPD).” Onde garantia da transparência nos processos de tratamento e a promoção de ações de conscientização e capacitação tanto para os beneficiários quanto para os agentes públicos envolvidos. Essas diretrizes refletem a necessidade de uma governança de dados eficaz e a aplicação de boas práticas, essenciais para a conformidade e para a construção de um ambiente digital mais seguro e transparente, o que amplia as discussões de Sampaio (2020) sobre a responsabilidade das organizações no tratamento de dados sensíveis.

Nesse contexto, onde as taxas de vulnerabilidade social são expressivas e um contingente significativo da população depende do BPC LOAS para sua subsistência, a proteção de dados assume contornos ainda mais críticos. A fragilidade socioeconômica desses indivíduos os torna potencialmente mais suscetíveis aos danos decorrentes de incidentes de segurança da informação, como fraudes financeiras, discriminação baseada em suas condições de saúde ou socioeconômicas, e até mesmo a exploração de suas informações pessoais por terceiros mal-intencionados. Portanto, a implementação de medidas eficazes de proteção de dados não se configura apenas como uma obrigação legal, mas como uma norma ética e social para garantir a dignidade e a segurança dessa parcela vulnerável no Brasil na era digital. A urgência dessa proteção é amplificada ao considerarmos que a autodeterminação informativa, essencial para a tutela da privacidade na era digital, é um pilar da dignidade da pessoa humana e dos direitos fundamentais (SARLET, 2020). Desse modo, a implementação de medidas eficazes de proteção de dados não se configura apenas como uma obrigação legal, mas como

¹ Lei Geral de Proteção de Dados Pessoais (LGPD)

uma norma ética e social para garantir a dignidade e a segurança dessa parcela vulnerável no Brasil na era digital, um imperativo que transcende a mera conformidade e exige uma abordagem que efetivamente proteja contra a exclusão e a exploração (DONEDA, 2019).

2. Marco Teórico: Proteção de Dados e Vulnerabilidade Social

A proteção de dados pessoais é um direito fundamental, cada vez mais reconhecido e regulamentado em todo o mundo. No Brasil, a principal legislação sobre o tema é a Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei nº 13.709/2018, que estabelece regras claras sobre a coleta, o tratamento, o armazenamento e o compartilhamento de dados pessoais, visando garantir a privacidade e a autonomia dos indivíduos.

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, define dados pessoais como qualquer informação que possa identificar uma pessoa natural, direta ou indiretamente, e dados pessoais sensíveis como aqueles referentes à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

A vulnerabilidade social, por sua vez, refere-se a uma condição em que indivíduos ou grupos possuem recursos limitados ou estão expostos a riscos que dificultam sua capacidade de atender às suas necessidades básicas e de exercer seus direitos plenamente. Os clientes do BPC LOAS, por sua própria condição de elegibilidade ao benefício, encontram-se em um estado de vulnerabilidade econômica e, muitas vezes, social, o que os torna mais suscetíveis aos impactos negativos decorrentes da violação de seus dados pessoais. A intrínseca ligação entre a proteção de dados e a vulnerabilidade social se manifesta de forma particularmente aguda no contexto dos beneficiários do BPC LOAS. A coleta e o tratamento de seus dados pessoais, muitas vezes abrangendo informações altamente sensíveis sobre sua saúde, condição financeira e composição familiar, representam um risco elevado quando não gerenciados com a máxima diligência. A exposição indevida dessas informações pode exacerbar sua já existente vulnerabilidade, abrindo portas para discriminação, exploração financeira e outras formas de prejuízo que comprometem sua dignidade e bem-estar. Nesse sentido, a efetiva aplicação da LGPD e a implementação de práticas robustas de proteção de dados se tornam mecanismos cruciais para mitigar esses riscos e garantir que a era digital não se torne um vetor de novas formas de exclusão e marginalização para essa parcela da população. Tal cenário de risco se alinha profundamente às preocupações de Amartya Sen (2000), que define a pobreza não apenas

como privação de renda, mas sobretudo como a privação de 'capacidades' e 'liberdades' substantivas.

Para Sen, o desenvolvimento humano é o processo de expansão dessas liberdades reais que as pessoas desfrutam, abrangendo desde a liberdade de não passar fome até a liberdade de participar da vida social e política. A violação de dados pessoais sensíveis de indivíduos em situação de vulnerabilidade, como os beneficiários do BPC/LOAS, representa uma restrição direta a essas liberdades.

A vulnerabilidade social, portanto, não apenas qualifica a condição dos beneficiários do BPC LOAS, mas também intensifica a importância da proteção de seus dados pessoais. A ausência de recursos econômicos e, em muitos casos, de acesso à informação e à educação digital, pode limitar a capacidade desses indivíduos de compreender os riscos associados ao tratamento de seus dados e de exercer seus direitos como titulares previstos na LGPD. Essa assimetria de poder informacional e de recursos torna-os mais dependentes da atuação responsável e transparente das instituições que coletam e processam suas informações, reforçando a necessidade de políticas de proteção de dados que considerem ativamente essa condição de vulnerabilidade, essa dinâmica de exclusão digital e de barreiras ao pleno exercício da cidadania no ambiente online é um desafio persistente, conforme apontado por Castells (2000). Para ele, a ascensão da sociedade em rede, embora prometa maior conexão e acesso, pode contrariamente aprofundar as desigualdades existentes, pois o controle sobre a informação e a capacidade de navegar com segurança nesse novo cenário não são universalmente distribuídos. No caso dos beneficiários do BPC/LOAS, a falta de familiaridade com as tecnologias digitais, a carência de dispositivos adequados ou a dificuldade de acesso à internet tornam-se barreiras concretas para que possam gerir seus próprios dados e se proteger de ameaças. Assim, a proteção de dados não é apenas uma questão de conformidade legal, mas uma dimensão essencial da inclusão social, garantindo que a digitalização não se torne um novo meio de marginalização para aqueles que já se encontram em situação de fragilidade.

Em suma, o marco teórico (LGPD) que associa a proteção de dados à vulnerabilidade social no contexto do BPC LOAS em Parnaíba destaca uma interdependência crítica. A garantia da privacidade e da segurança das informações pessoais desses beneficiários não é apenas uma questão de conformidade legal, mas um elemento essencial para a promoção da justiça social e para a proteção dos direitos fundamentais de uma população que já se encontra em uma situação de fragilidade. A efetiva implementação da LGPD e a adoção de práticas de proteção de dados sensíveis ao contexto da vulnerabilidade social são, portanto, imperativos para assegurar que a digitalização dos serviços públicos contribua para a inclusão e o bem-estar, e não para o

aumento da desigualdade e da exclusão. Isso repercute com a perspectiva de Amartya Sen (2000), que enfatiza a importância de expandir as liberdades e capacidades dos indivíduos para que possam viver a vida que têm razão para valorizar, um ideal que, no ambiente digital, se concretiza através da proteção de dados. Como Doneda (2019) argumenta, a autodeterminação informativa é crucial para a dignidade na era digital, tornando-se ainda mais vital para aqueles que, devido à sua vulnerabilidade, correm maior risco de ter suas informações usadas de forma a comprometer suas liberdades fundamentais e sua inclusão plena.

2.1 Os avanços que a digitalização trouxe para facilitar o acesso dos usuários.

A implementação de tecnologias digitais nos serviços públicos tem o potencial de revolucionar a forma como os cidadãos acessam direitos e benefícios sociais. No contexto específico do Benefício de Prestação Continuada (BPC) da Lei Orgânica da Assistência Social (LOAS) em Parnaíba, Piauí, a digitalização emerge como uma ferramenta crucial para facilitar o acesso de uma população particularmente vulnerável. Ao transpor barreiras geográficas, reduzir a burocracia e otimizar processos, a digitalização pode significativamente aprimorar a experiência dos usuários do BPC LOAS. Essas transformações, que redefinem a relação entre Estado e cidadão, confirmam a perspectiva de Castells (2000), que antecipava como a sociedade em rede, ao remodelar as estruturas de informação e comunicação, teria o poder de democratizar o acesso e reconfigurar as dinâmicas sociais e de poder, inclusive no âmbito dos serviços públicos.

Um dos avanços mais notáveis proporcionados pela digitalização é a expansão do acesso à informação. Plataformas online e aplicativos móveis podem fornecer aos beneficiários e potenciais beneficiários do BPC LOAS, informações claras e atualizadas sobre os critérios de elegibilidade, a documentação necessária, os prazos e as etapas do processo de solicitação e acompanhamento do benefício. Essa transparência informacional empodera os usuários, permitindo que se preparem adequadamente e evitem deslocamentos desnecessários a centros de atendimento físico, muitas vezes dispendiosos e logisticamente desafiadores para essa população.

(...) o INSS adotou um novo modelo de atendimento: o INSS Digital que, segundo a autarquia, consiste em um “novo fluxo de atendimento para aumentar a capacidade da autarquia de reconhecer direitos”. Os pilares do projeto são o processo eletrônico – agendamento e concessão do benefício pela internet para o segurado [...] ou por meio de entidade representativa que tenha celebrado Acordo de Cooperação Técnica com o INSS – e a distribuição de demandas entre as unidades. (Cirilo e Mello, 2017, p. 3).

Um dos progressos mais evidentes proporcionados pela digitalização reside na ampliação democrática do acesso à informação. Plataformas online intuitivas e aplicativos móveis de fácil manuseio podem disseminar entre os beneficiários atuais e futuros do BPC LOAS em Parnaíba informações cruciais, apresentadas de forma clara e sempre atualizada, sobre os critérios de elegibilidade para o benefício, a documentação fundamental a ser apresentada, os prazos processuais e as diversas etapas que compõem o caminho da solicitação e do acompanhamento do benefício. Essa clareza informacional fortalece os usuários, munindo-os do conhecimento necessário para se prepararem adequadamente para o processo, evitando, assim, deslocamentos desnecessários e dispendiosos a centros de atendimento físico, que muitas vezes representam um desafio logístico e financeiro considerável para essa parcela da população. A possibilidade de acessar informações relevantes no conforto de seus lares ou por meio de dispositivos móveis elimina obstáculos físicos e de tempo, tornando o sistema mais acessível e justo.

Além disso, a digitalização tem a capacidade de tornar mais simples e rápidos os intrincados procedimentos de agendamento e solicitação de serviços. Em vez das longas filas e da exaustiva espera em unidades de atendimento presenciais, os usuários podem, por meio de plataformas digitais acessíveis, realizar agendamentos de exames periciais, entrevistas com assistentes sociais e outras fases cruciais do processo de forma remota e conveniente, ajustando os horários às suas necessidades e disponibilidades. A inovadora possibilidade de iniciar solicitações de benefícios completamente online, anexando os documentos necessários em formato digital, representa um avanço significativo na desburocratização do acesso ao benefício, eliminando a necessidade de cópias físicas, autenticações e a lentidão da tramitação de papel. Esse aspecto é especialmente relevante em um contexto como o de Parnaíba, onde o acesso a transporte confiável e a disponibilidade de tempo livre podem ser recursos escassos para muitos beneficiários, impactando diretamente sua capacidade de buscar seus direitos.

No entanto, é fundamental reconhecer que a plena realização dos benefícios da digitalização para os usuários do BPC LOAS em Parnaíba depende da superação de desafios relacionados à inclusão digital. Garantir o acesso universal à internet de qualidade, fornecer dispositivos adequados e promover a alfabetização digital entre os beneficiários são passos essenciais para que essa parcela da população não seja excluída dos avanços tecnológicos. Programas de apoio e treinamento podem ser necessários para capacitar os usuários a utilizar as ferramentas digitais de forma segura e eficaz. Essa necessidade de equidade no acesso e na capacidade de uso das tecnologias reflete a preocupação de Sen (2000), que, ao discutir o desenvolvimento como liberdade, argumenta que a mera disponibilidade de um recurso não

garante seu benefício, sendo crucial que os indivíduos possuam as 'capacidades' (habilidades, conhecimentos e condições) para convertê-los em liberdade real.

Em suma, a digitalização dos serviços do BPC LOAS em Parnaíba representa um avanço promissor na facilitação do acesso a um benefício essencial para muitas famílias em situação de vulnerabilidade. Ao ampliar o acesso à informação, simplificar procedimentos, otimizar a comunicação e reduzir a burocracia, a tecnologia digital tem o potencial de transformar positivamente a vida dos usuários. Contudo, para que esses avanços sejam verdadeiramente inclusivos e eficazes, é imperativo que se invista em estratégias que garantam a equidade no acesso digital e a segurança dos dados dessa população.

2.2 O Impacto do Aplicativo Meu INSS na Otimização do Atendimento Previdenciário e Redução de Filas.

O aplicativo “MEU INSS” transformou radicalmente a dinâmica entre os cidadãos brasileiros e a Previdência Social, estabelecendo-se como um pilar fundamental na modernização dos serviços públicos. Ao oferecer uma plataforma digital abrangente, o aplicativo transcende a mera conveniência, impactando diretamente a vida de milhões de pessoas ao eliminar a necessidade de deslocamento e espera em longas filas nas agências físicas do INSS. Essa transição para modelos de atendimento mais eficientes e centrados no usuário é um movimento global, como discute Tapscott (1996), ao evidenciar como a era da informação e a internet reconfiguram as instituições, impulsionando a "era da interatividade" onde os serviços se tornam mais acessíveis e importantes nas necessidades dos cidadãos.

A amplitude de serviços disponíveis no Meu INSS é notável. Os usuários podem, com apenas alguns cliques, dar entrada em pedidos de benefícios cruciais, como aposentadorias por idade, tempo de contribuição ou invalidez, auxílios como de doença e de maternidade, além de pensões por morte. A facilidade de anexar documentos digitalizados diretamente pelo aplicativo agiliza o processo de análise e concede ao requerente a possibilidade de acompanhar cada etapa do seu pedido, desde a protocolização até a decisão final. Essa transparência e controle sobre o processo geram maior confiança e reduzem a ansiedade associada à espera por uma resposta. A emissão de documentos importantes, como o Cadastro Nacional de Informações Sociais (CNIS), um extrato fundamental para verificar o histórico de contribuições previdenciárias, e o extrato de pagamento de benefícios, essencial para o controle financeiro dos segurados. A possibilidade de agendar ou remarcar perícias médicas e outros atendimentos, quando o

comparecimento presencial é inevitável, também é um recurso valioso, pois confere maior flexibilidade e organização aos usuários.

A contribuição do Meu INSS para a otimização do atendimento nas agências é inegável. Ao absorver uma grande parcela das demandas que antes exigiam a presença física do cidadão, o aplicativo permite que os servidores do INSS concentrem seus esforços em casos mais complexos ou que realmente necessitam de interação pessoal. Isso resulta em um atendimento mais eficiente e qualificado para aqueles que, porventura, precisem se dirigir a uma unidade física.

Em um contexto de crescente digitalização da sociedade, o Meu INSS se destaca como um exemplo de como a tecnologia pode ser utilizada para simplificar processos burocráticos e democratizar o acesso aos serviços públicos. Ao empoderar o cidadão com a autonomia de resolver suas pendências previdenciárias de forma remota, o aplicativo não apenas evita o desgaste físico e emocional das filas, mas também promove uma relação mais ágil, transparente e eficiente entre o INSS e seus vários beneficiários em todo o Brasil. Sua contínua evolução e a incorporação de novos serviços reforçam seu papel como uma ferramenta indispensável na vida dos trabalhadores e segurados brasileiros.

A variedade de serviços acessíveis pelo Meu INSS é notável. Com poucos cliques, os usuários podem iniciar solicitações de benefícios cruciais, como aposentadorias por idade, tempo de contribuição ou invalidez, auxílios como o por incapacidade temporária e o salário-maternidade, além de pensões por morte. A facilidade de anexar documentos digitalizados diretamente pelo aplicativo acelera a análise dos pedidos e permite que o solicitante acompanhe cada etapa do processo, desde o registro inicial até a decisão final. Essa clareza e controle sobre o andamento geram maior segurança e diminuem a apreensão associada à espera por uma resposta. A obtenção de documentos importantes, como o Cadastro Nacional de Informações Sociais (CNIS), um registro fundamental para verificar o histórico de contribuições previdenciárias, e o comprovante de pagamento de benefícios, essencial para a gestão financeira dos segurados, também é simplificada. A possibilidade de marcar ou reagendar exames periciais e outros atendimentos, quando a presença física é inevitável, representa igualmente um recurso valioso, proporcionando maior flexibilidade e organização aos usuários.

A contribuição do Meu INSS para a otimização do atendimento nas agências é inegável. Ao absorver uma grande parte das demandas que antes exigiam a presença do cidadão, o aplicativo permite que os servidores do INSS concentrem seus esforços em casos mais complexos ou que realmente necessitam de contato pessoal. Isso resulta em um atendimento

mais eficiente e qualificado para aqueles que, porventura, precisem comparecer a uma unidade física.

(...) dado que a expansão do acesso à internet no Brasil pode ter chegado já a todas ou quase todas as pessoas que têm certo patamar de rendimentos e que queiram se inserir digitalmente (ou seja, que tenham recursos financeiros e desejo para adquirir um computador e uma linha telefônica e pagar para usar um provedor de acesso), fica o desafio para que, nos próximos anos, mantenha-se o atual ritmo de ampliação da inclusão digital no país. A elevada concentração de renda e o baixo nível do rendimento médio da população brasileira representam, portanto, um significativo entrave para a manutenção de uma contínua ampliação do grau de inclusão digital no Brasil no futuro breve (MATTOS; CHAGAS, 2008, p. 81).

Em um cenário de crescente integração da tecnologia no cotidiano da sociedade, o Meu INSS se destaca como um exemplo de como a tecnologia pode ser utilizada para simplificar processos burocráticos e ampliar o acesso aos serviços públicos. Ao capacitar o cidadão com a autonomia de resolver suas questões previdenciárias remotamente, o aplicativo não apenas evita o desgaste físico e emocional das filas, mas também promove uma relação mais ágil, transparente e eficaz entre o INSS e seus milhões de beneficiários em todo o Brasil. No entanto, para que o potencial transformador do Meu INSS seja plenamente realizado e alcance todas as camadas da população, é imperativo que os desafios da inclusão digital sejam ativamente endereçados. Isso ressoa com a análise de Castells (2000), que, ao explorar a "sociedade em rede", já alertava que a divisão entre "conectados e desconectados" pode aprofundar as desigualdades, tornando crucial a universalização do acesso e da literacia digital para garantir que as tecnologias digitais sejam verdadeiras ferramentas de democratização e não um novo fator de exclusão. Sua constante evolução e a incorporação de novos serviços reforçam seu papel como uma ferramenta indispensável na vida dos trabalhadores e segurados brasileiros.

2.3 A digitalização dos Serviços e os Riscos para os Beneficiários do BPC LOAS em Parnaíba.

A modernização dos serviços do INSS e de outras instituições envolvidas na gestão do BPC LOAS implica na coleta, no armazenamento e no tratamento de um volume significativo de dados pessoais em formato digital. Embora essa digitalização possa facilitar o acesso aos serviços e agilizar processos, ela também introduz novos riscos à segurança e à privacidade desses dados.

O uso indevido de dados representa outro perigo considerável. O acesso não autorizado a essas informações pode abrir caminho para a ocorrência de fraudes financeiras, como a obtenção indevida de benefícios ou a utilização dos dados para golpes de crédito. Além disso,

o uso indevido pode levar à discriminação, seja por instituições financeiras, empregadores ou outros agentes, com base nas informações sobre a condição de saúde ou vulnerabilidade social dos beneficiários. Tais prejuízos podem agravar ainda mais a situação precária em que muitos desses indivíduos se encontram.

Ademais, o compartilhamento inadequado de informações entre diferentes órgãos e entidades públicas ou privadas, sem a implementação de salvaguardas robustas, pode comprometer seriamente a privacidade dos beneficiários. A circulação descontrolada de dados sensíveis aumenta o risco de acesso indevido e de utilização para finalidades não consentidas, minando a confiança dos cidadãos nas instituições e expondo-os a potenciais danos.

A falta de transparência nos processos de tratamento de dados também se configura como um risco relevante. A ausência de informações claras e acessíveis sobre como os dados são coletados, utilizados e protegidos impede que os beneficiários compreendam seus direitos como titulares de dados, conforme previsto na LGPD. Essa falta de clareza dificulta a possibilidade de exercerem seus direitos de acesso, correção, exclusão ou oposição ao tratamento, deixando-os em uma posição de vulnerabilidade informacional.

A ameaça do vazamento de dados assume proporções alarmantes no contexto da digitalização. Os sistemas de informação que armazenam os dados pessoais dos beneficiários do BPC LOAS, incluindo informações cadastrais detalhadas, dados de saúde delicados e informações sobre a sua intrincada situação socioeconômica, tornam-se alvos primários para ataques cibernéticos sofisticados. A capacidade de agentes maliciosos de penetrar essas defesas digitais e extrair grandes volumes de informações confidenciais pode ter consequências devastadoras para milhares de indivíduos. Sobre a necessidade de proteção nesse cenário, Martins (2021, p. 78) aponta que "a segurança da informação não é um luxo, mas uma necessidade premente em um ambiente cada vez mais digitalizado, especialmente quando se trata de dados de populações vulneráveis".

Essa afirmação reforça a urgência de medidas robustas. A exposição desses dados não se limita ao domínio da privacidade; ela pode facilitar a ocorrência de fraudes financeiras, como a utilização indevida de informações bancárias ou a obtenção de empréstimos fraudulentos em nome dos beneficiários, lançando-os em ciclos de endividamento ainda mais profundos. Além disso, o conhecimento de informações sensíveis sobre a saúde ou a condição de vulnerabilidade social pode expor os beneficiários a estigma, discriminação e outras formas de tratamento injusto por parte de instituições financeiras, empregadores ou até mesmo outros membros da sociedade.

Silva (2023, p. 105) complementa essa perspectiva ao afirmar que "a vulnerabilidade social preexistente dos beneficiários do BPC LOAS amplifica os danos decorrentes de violações de dados, tornando a proteção ainda mais crítica para evitar o aprofundamento de suas condições de precariedade"

A implementação de medidas de segurança cibernética robustas, que englobem desde a criptografia de dados até a implementação de firewalls e sistemas de detecção de intrusão avançados, aliada a planos de resposta a incidentes eficazes, torna-se, portanto, uma prioridade inadiável para mitigar esse risco.

Ainda sobre o uso indevido de dados, **Pereira (2022)** argumenta que a fiscalização e a responsabilização são essenciais para conter o acesso não autorizado às informações dos beneficiários, seja por meio de falhas de segurança nos sistemas, por ação de funcionários mal-intencionados ou por meio de engenharia social direcionada aos próprios beneficiários.

A obtenção indevida de benefícios, a falsificação de documentos e a utilização dos dados para golpes de crédito são apenas algumas das formas pelas quais essas informações podem ser exploradas para ganho financeiro ilícito. Adicionalmente, o uso indevido pode se estender a práticas discriminatórias, onde as informações sobre a condição de saúde ou a vulnerabilidade social dos beneficiários são utilizadas para negar-lhes oportunidades ou tratamento igualitário. A adoção de políticas de acesso restrito, baseadas no princípio do menor privilégio, a implementação de trilhas de auditoria detalhadas para monitorar o acesso e o uso dos dados, e a conscientização dos funcionários sobre a importância da confidencialidade são medidas cruciais para prevenir o uso indevido.

3. A vulnerabilidade social e tipos de fraudes mais comuns.

A população beneficiária do Benefício de Prestação Continuada (BPC) da Lei Orgânica da Assistência Social (LOAS), caracteriza-se por uma acentuada vulnerabilidade social e econômica. Essa condição, intrinsecamente ligada à idade avançada ou à deficiência e, frequentemente, agravada pela baixa renda e limitado acesso à informação, torna esse grupo particularmente suscetível a diversas formas de exploração, incluindo as fraudes no ambiente digital. A transição para a oferta de serviços sociais por meio de plataformas online, embora traga consigo inegáveis benefícios, também introduz novos riscos que demandam atenção e medidas de proteção específicas.

A falta de familiaridade com o ambiente digital emerge como um fator crucial que aumenta significativamente a suscetibilidade dos beneficiários do BPC LOAS a golpes e fraudes online. Muitos indivíduos nessa faixa populacional podem ter pouco ou nenhum contato

prévio com tecnologias digitais, desconhecendo os mecanismos de segurança, os sinais de alerta e as práticas seguras de navegação na internet torna alvos fáceis para criminosos que se aproveitam dessa lacuna de conhecimento para aplicar golpes sofisticados. Como aponta a pesquisadora Castells (2000), "a exclusão digital não é apenas a falta de acesso à tecnologia, mas a incapacidade de utilizar plenamente seus recursos para o empoderamento individual e social" (p. 250). Corroborando essa perspectiva, Van Dijk (2005) destaca que "a exclusão digital é um problema multidimensional que engloba o acesso, as habilidades de uso e apropriação da tecnologia" (p. 15). Assim, a transição para plataformas digitais exige uma atenção especial à alfabetização digital, pois, na visão de Prensky (2001), "a era digital demanda novas formas de pensar e aprender, e quem não as domina fica à margem das oportunidades" (p. 1).

Essa falta de experiência os torna alvos fáceis para criminosos que se aproveitam dessa lacuna de conhecimento para aplicar golpes sofisticados.

Entre os tipos de fraude mais comuns que exploram essa vulnerabilidade, destacam-se:

- **Phishing:** Golpistas se disfarçam de instituições legítimas, como o INSS, bancos ou até mesmo programas sociais, enviando mensagens (por e-mail, SMS ou WhatsApp) que solicitam informações pessoais, dados bancários ou senhas sob pretextos diversos, como a necessidade de atualização cadastral ou a liberação de valores atrasados. A urgência e a linguagem alarmista frequentemente utilizadas nessas mensagens induzem as vítimas a fornecerem seus dados confidenciais, que são então utilizados para fins fraudulentos. Como adverte Norton (2018), "o *phishing* é uma tática insidiosa que se baseia na manipulação emocional e na confiança para extrair informações valiosas de vítimas desavisadas" (p. 67).
- **Roubo de Identidade:** A obtenção indevida de dados pessoais, seja por meio de phishing ou outras técnicas, permite que fraudadores se passem pelos beneficiários para realizar diversas ações, como movimentar contas bancárias, contratar empréstimos ou até mesmo solicitar novos benefícios de forma fraudulenta. Nesse cenário, "a identidade digital de um indivíduo torna-se um ativo valioso para criminosos, permitindo que eles operem de forma invisível e causem danos financeiros e reputacionais significativos" (Kasper (Kaspersky), 2022, p. 45).
- **Malware e Vírus:** A falta de conhecimento sobre segurança digital torna os beneficiários mais propensos a clicar em links maliciosos ou baixar arquivos infectados,

expondo seus dispositivos e informações pessoais a softwares que podem roubar dados bancários, senhas e outras informações sensíveis. Segundo McAfee (2021), "a desinformação sobre ameaças cibernéticas e a ausência de *software* de proteção adequado transformam os dispositivos de usuários despreparados em portas abertas para ataques de *malware* e roubo de dados" (p. 78).

- Engenharia Social: Golpistas utilizam a manipulação psicológica para convencer os beneficiários a realizar ações que os prejudicam financeiramente ou expõem seus dados. Isso pode envolver ligações telefônicas, visitas domiciliares (quando aplicável) ou mensagens persuasivas que exploram a confiança e a falta de familiaridade com procedimentos online. Como ressalta Mitnick (2002), "a engenharia social não explora falhas tecnológicas, mas sim a natureza humana, focando na capacidade de persuadir e enganar por meio da interação pessoal" (p. 112).

A combinação da vulnerabilidade social com a crescente digitalização dos serviços exige uma atenção redobrada para proteger os beneficiários do BPC LOAS dessas ameaças. É crucial implementar estratégias de educação digital direcionadas a essa população, utilizando uma linguagem acessível e canais de comunicação eficazes para alertar sobre os riscos e ensinar práticas seguras no ambiente online. Além disso, o fortalecimento dos mecanismos de segurança nas plataformas digitais de acesso aos serviços sociais e a intensificação da fiscalização são medidas indispensáveis para garantir a integridade dos dados e a proteção financeira dessa parcela vulnerável da sociedade. A conscientização e a prevenção são as melhores ferramentas para mitigar os impactos negativos das fraudes digitais sobre os beneficiários.

3.1 Como o BPC LOAS Impulsiona a Economia no Combate à Fome.

O Benefício de Prestação Continuada (BPC) da Lei Orgânica da Assistência Social (LOAS) representa um importante instrumento de proteção social para idosos e pessoas com deficiência em situação de vulnerabilidade econômica no Brasil. Em um contexto local como Parnaíba, Piauí, o BPC transcende sua função assistencial imediata, revelando-se um vetor significativo para a dinamização da economia municipal e, crucialmente, para o enfrentamento do grave problema da insegurança alimentar. Como destaca Draibe (2006), "programas de transferência de renda são essenciais para reduzir a pobreza e garantir a segurança alimentar de populações vulneráveis, promovendo dignidade e cidadania" (p. 45).

Ao garantir uma renda mensal a indivíduos que, de outra forma, teriam dificuldades extremas em prover suas necessidades básicas, o BPC injeta recursos diretamente na economia



de Parnaíba. Os beneficiários, ao receberem o auxílio financeiro, tendem a direcionar esses valores prioritariamente para a aquisição de bens essenciais, com destaque para alimentos. Essa demanda por itens alimentícios estimula o comércio local, desde pequenos mercados de bairro e feiras livres até supermercados maiores. O resultado é um ciclo virtuoso onde o benefício social se traduz em receita para comerciantes, geração de empregos indiretos e fortalecimento da economia em nível municipal.

O impacto do BPC LOAS no combate à fome em Parnaíba é particularmente relevante. Para muitas famílias beneficiárias, o valor recebido representa a principal ou única fonte de renda para garantir o acesso a uma alimentação adequada e regular. Em um município onde a vulnerabilidade socioeconômica pode ser acentuada, a segurança proporcionada pelo BPC LOAS atua como um amortecedor contra a insegurança alimentar, permitindo que indivíduos e suas famílias tenham condições mínimas para adquirir alimentos nutritivos e evitar situações de extrema privação.

A capilaridade do impacto econômico do BPC LOAS se estende por diversos setores da economia parnaibana. O aumento da demanda por alimentos impulsiona não apenas o comércio varejista, mas também a agricultura local, ainda que em menor escala. Pequenos produtores podem se beneficiar indiretamente do maior poder de compra da população, encontrando um mercado consumidor mais aquecido. Além disso, outros setores como o de serviços (transporte, pequenos reparos, etc.) também podem sentir os efeitos positivos do incremento na renda disponível. Nesse cenário, "a capacidade de um programa social de ativar cadeias produtivas locais é um indicativo de seu potencial para o desenvolvimento econômico de territórios em vulnerabilidade" (Arrais e Castro, 2018, p. 112).

É importante ressaltar que o impacto do BPC LOAS na economia local e no combate à fome não ocorre de forma isolada. Ele se articula com outras políticas públicas e iniciativas locais voltadas para a assistência social, a segurança alimentar e o desenvolvimento econômico. A efetividade do BPC LOAS em Parnaíba é potencializada quando integrado a programas de acompanhamento social, de educação alimentar e de apoio à agricultura familiar, criando uma rede de proteção mais abrangente e sustentável.

Em suma, o BPC LOAS desempenha um papel multifacetado em Parnaíba. Além de ser um direito fundamental que garante uma renda mínima para uma parcela vulnerável da população, ele se configura como um importante motor da economia local, impulsionando o comércio e, de maneira crucial, contribuindo para mitigar a insegurança alimentar. Compreender essa dupla dimensão do BPC LOAS é essencial para valorizar sua importância e

para buscar aprimoramentos que maximizem seus benefícios tanto no âmbito social quanto no econômico. Como enfatiza Silva e Yazbek (2012), "a assistência social deve ser compreendida não apenas como um custo, mas como um investimento social capaz de gerar retornos significativos em termos de equidade e desenvolvimento local" (p. 88).

3.2 Desafios e Boas Práticas para a Proteção de Dados

Assegurar a efetiva proteção dos dados pessoais dos clientes do BPC LOAS demanda um esforço coordenado e a superação de múltiplos desafios por parte dos órgãos e entidades envolvidas na gestão e operacionalização do benefício. Inicialmente, torna-se imprescindível promover uma ampla conscientização e capacitação sobre a relevância da proteção de dados, direcionada tanto aos beneficiários, para que compreendam seus direitos e os riscos envolvidos, quanto aos servidores públicos, responsáveis diretos pelo tratamento dessas informações, garantindo que atuem em conformidade com as melhores práticas e a legislação vigente. Como ressalta Solove (2008), "a proteção da privacidade e dos dados pessoais não é um mero entrave burocrático, mas um pilar fundamental para a dignidade humana na era digital" (p. 23).

Outro desafio crucial reside na plena implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) pelas instituições. Alcançar a conformidade com os princípios e as regras estabelecidas pela lei pode exigir investimentos significativos em tecnologia, na revisão e adequação de processos internos e no treinamento especializado de pessoal, assegurando que todas as etapas do tratamento de dados sejam realizadas de forma lícita, transparente e segura. Doneda (2019) enfatiza que "a LGPD não é apenas um conjunto de regras, mas um convite à reflexão sobre a cultura de dados nas organizações, exigindo uma mudança profunda na forma como a informação pessoal é tratada" (p. 50).

Paralelamente, a segurança da informação emerge como um pilar fundamental. É imperativo implementar medidas robustas e constantemente atualizadas para proteger os sistemas de informação e os dados armazenados contra acessos não autorizados, vazamentos, ataques cibernéticos e outras ameaças que possam comprometer a integridade e a confidencialidade das informações dos beneficiários.

A transparência e a comunicação eficaz também representam desafios importantes. As políticas e os procedimentos de proteção de dados adotados pelas instituições devem ser claros, acessíveis e comunicados de maneira compreensível aos beneficiários, garantindo que eles estejam cientes de como seus dados são coletados, utilizados e protegidos, e de como podem exercer seus direitos como titulares previstos na LGPD.

Por fim, é essencial voltar atenção especial às vulnerabilidades inerentes à população atendida pelo BPC LOAS juntamente com novos ideais de investimento a serem trabalhados a partir de políticas públicas voltadas para a temática. Assim como aborda Teixeira:

Políticas públicas são diretrizes, princípios norteadores de ação do poder público; regras e procedimentos para as relações entre poder público e sociedade, mediações entre atores da sociedade e do Estado. São, neste caso, políticas explícitas, sistematizadas ou formuladas em documentos (leis, programas, linhas de financiamentos) que orientam ações que normalmente envolvem aplicações de recursos públicos. (Teixeira, 2002, p.1).

Dada a sua condição social e econômica, torna-se necessário adotar abordagens diferenciadas e sensíveis ao contexto para garantir que as medidas de proteção de dados sejam efetivas e acessíveis a todos, considerando as possíveis limitações de acesso à informação e à tecnologia.

Para enfrentar esses desafios, a implementação de boas práticas se torna indispensável. A minimização da coleta de dados, restringindo a obtenção apenas às informações estritamente necessárias para a finalidade específica do serviço, reduz a superfície de risco. A utilização de técnicas de anonimização e pseudonimização, sempre que possível, diminui a probabilidade de identificação direta dos beneficiários, protegendo sua privacidade. A criptografia de dados sensíveis, tanto em repouso quanto em trânsito, garante que as informações permaneçam inacessíveis a pessoas não autorizadas. A implementação de controles de acesso rigorosos assegura que apenas indivíduos autorizados possam acessar os dados. A definição de políticas claras de retenção de dados, com a eliminação das informações quando não forem mais necessárias, evita o acúmulo desnecessário de dados. A realização de auditorias de segurança periódicas permite verificar a eficácia das medidas implementadas e identificar possíveis vulnerabilidades. O estabelecimento de canais de comunicação acessíveis facilita o exercício dos direitos dos titulares pelos beneficiários. E, por fim, a promoção de ações de educação continuada sobre proteção de dados, tanto para beneficiários quanto para servidores, fortalece a cultura de privacidade e segurança da informação. A adoção integrada dessas boas práticas é fundamental para construir um ambiente digital mais seguro e confiável para os clientes do BPC LOAS. Como pontuam **Müller e Knopp (2021)**, "a segurança da informação é um processo contínuo que exige vigilância constante, adaptação às novas ameaças e, acima de tudo, um forte engajamento de todos os envolvidos" (p. 95).

3.3 Desafios e Boas Práticas para a Proteção de Dados dos Beneficiários do BPC LOAS em Parnaíba

Assegurar a efetiva proteção dos dados pessoais dos clientes do BPC LOAS em Parnaíba exige uma abordagem multifacetada, permeada por desafios complexos que demandam a implementação de boas práticas consistentes e abrangentes. Para operacionalizar essa proteção de maneira eficaz, podemos estruturar nossas ações em dois pilares fundamentais: a implementação robusta de medidas de segurança e governança de dados, e o empoderamento e a conscientização dos beneficiários acerca de seus direitos e da importância da segurança de suas informações.

No que tange à implementação de medidas de segurança e governança de dados, é crucial que os órgãos e entidades envolvidas na gestão e operacionalização do BPC LOAS em Parnaíba adotem um conjunto abrangente de práticas para mitigar riscos e garantir a integridade e confidencialidade das informações. A criptografia de dados, tanto em repouso quanto em trânsito, emerge como uma camada essencial de proteção, tornando as informações ilegíveis para acessos não autorizados. Como afirma Doneda (2019), "a segurança da informação, com destaque para a criptografia e os controles de acesso, é um dos pilares para a concretização dos direitos dos titulares previstos na LGPD" (p. 150). Paralelamente, o estabelecimento de controles de acesso rigorosos, baseados nos princípios do menor privilégio e da necessidade de conhecer, é vital para restringir o acesso aos dados apenas a indivíduos autorizados e para finalidades específicas, rastreando e auditando as atividades realizadas. A formulação e a divulgação de políticas de privacidade claras e transparentes são igualmente importantes, fornecendo aos beneficiários informações detalhadas sobre quais dados são coletados, como são utilizados, com quem são compartilhados e, crucialmente, quais são seus direitos em relação a essas informações. A eficácia dessas políticas depende intrinsecamente do treinamento e da conscientização contínua dos funcionários e colaboradores envolvidos no tratamento de dados, garantindo que compreendam a importância da proteção de dados e as melhores práticas de segurança a serem seguidas em suas atividades diárias. Para assegurar a aderência a essas políticas e identificar potenciais vulnerabilidades, a realização de auditorias regulares se torna indispensável, permitindo a detecção precoce de falhas e a implementação de medidas corretivas. Por fim, o desenvolvimento e a implementação de um plano robusto de resposta a incidentes são cruciais para lidar de forma eficaz com possíveis vazamentos ou incidentes de segurança, incluindo procedimentos claros de identificação, contenção, erradicação, recuperação e notificação, minimizando os danos e restaurando a normalidade o mais rápido possível. Nesse contexto, Silva e Martins (2022) ressaltam que "a proatividade na gestão de

riscos e a capacidade de resposta a incidentes são elementos distintivos de uma governança de dados madura e responsável" (p. 78).

Complementarmente, o empoderamento e a conscientização dos beneficiários sobre seus direitos desempenham um papel igualmente vital na proteção de seus dados pessoais. Através de campanhas de informação e educação bem planejadas e executadas, utilizando linguagem acessível e diversos canais de comunicação, é possível disseminar o conhecimento sobre os direitos dos titulares de dados previstos na legislação, como os direitos de acesso, retificação, exclusão e portabilidade, bem como alertar sobre os riscos inerentes ao compartilhamento descuidado de informações pessoais. A disponibilização de canais de comunicação acessíveis é fundamental para que os beneficiários possam facilmente entrar em contato para tirar dúvidas, solicitar informações sobre o tratamento de seus dados e exercer seus direitos de forma efetiva. Além disso, a orientação sobre segurança digital capacita os usuários a protegerem suas informações em seu dia a dia, fornecendo dicas práticas sobre a criação de senhas seguras, a identificação de tentativas de outras fraudes online, e o cuidado ao compartilhar dados pessoais com terceiros, tanto no ambiente digital quanto no físico. Finalmente, o fomento à participação dos beneficiários no debate sobre a proteção de seus dados e o incentivo à comunicação de quaisquer irregularidades ou suspeitas de uso indevido de suas informações contribuem para a criação de um ambiente de maior vigilância e responsabilidade, fortalecendo a cultura de proteção de dados em toda a comunidade do BPC LOAS. Furlaneto (2019) argumenta que "a educação e a autonomia do cidadão digital são ferramentas poderosas contra as ameaças cibernéticas, especialmente para aqueles com menor familiaridade com o ambiente online" (p. 50).

4. Considerações Finais

A proteção de dados pessoais dos clientes do BPC LOAS na era digital, é um imperativo ético e legal. A vulnerabilidade social e econômica dessa população exige uma atenção redobrada à segurança e à privacidade de suas informações, que são essenciais para o acesso e a manutenção de um benefício que lhes garante uma mínima dignidade. Como destaca Sarlet (2007), "a dignidade da pessoa humana, como fundamento da República, impõe ao Estado e à sociedade o dever de assegurar as condições mínimas para o pleno desenvolvimento dos indivíduos, o que inclui a proteção contra novas formas de vulnerabilidade impostas pelo avanço tecnológico" (p. 102).

A plena implementação da LGPD, aliada a práticas robustas de segurança da informação e a uma comunicação transparente com os beneficiários, são passos cruciais para



mitigar os riscos inerentes à digitalização dos serviços sociais. É fundamental que os órgãos e entidades responsáveis pela gestão do BPC LOAS e em todo o Brasil priorizem a proteção de dados como um componente essencial de suas políticas e operações, garantindo assim os direitos e a segurança de uma população que já se encontra em situação de fragilidade.

A proteção de dados pessoais dos beneficiários do BPC LOAS, inseridos na complexa dinâmica da era digital, transcende a mera conformidade legal, erigindo-se como um imperativo ético fundamental. A acentuada vulnerabilidade social e econômica que caracteriza essa população impõe uma responsabilidade ainda maior no que concerne à segurança e à privacidade de suas informações. Esses dados, que viabilizam o acesso e a manutenção de um benefício essencial para a garantia de sua mínima dignidade, carregam consigo uma sensibilidade intrínseca, tornando sua proteção um pilar para a salvaguarda de seus direitos e bem-estar. Negligenciar essa proteção pode expor esses indivíduos a riscos significativos, exacerbando sua fragilidade e comprometendo sua autonomia, o que mostra uma necessidade multifacetada para uma devida prática efetiva do desenvolvimento digital, assim como diz Doneda (2019) argumenta que "a proteção de dados é, em última instância, um direito fundamental que exige não apenas regulação, mas uma cultura organizacional que a priorize" (p. 200).

A plena e efetiva implementação da Lei Geral de Proteção de Dados Pessoais (LGPD) surge, nesse contexto, como um marco regulatório essencial, fornecendo as diretrizes e os mecanismos para assegurar o tratamento adequado dessas informações. Contudo, a mera adesão à lei não se mostra suficiente. É imprescindível que essa implementação seja acompanhada pela adoção de práticas robustas de segurança da informação, capazes de prevenir e mitigar os crescentes riscos cibernéticos. Adicionalmente, uma comunicação transparente e acessível com os beneficiários se revela crucial para capacitá-los a compreender seus direitos, os riscos envolvidos e as medidas de proteção adotadas, fortalecendo assim sua autonomia e confiança no sistema.

Em suma, a priorização da proteção de dados como um componente intrínseco às políticas e operações dos órgãos e entidades responsáveis pela gestão do BPC LOAS em todo o território nacional não é uma mera formalidade administrativa. Constitui-se em um reconhecimento da dignidade e da vulnerabilidade dessa população, representando um investimento na sua segurança e no exercício pleno de seus direitos na era digital. Ao adotarem essa postura proativa e responsável, as instituições demonstram um compromisso genuíno com a justiça social e com a construção de um ambiente digital mais seguro e inclusivo para aqueles que mais necessitam. Bioni (2020) destaca que "a eficácia da LGPD reside na sua aplicação

contextualizada, especialmente em cenários de assimetria de poder e vulnerabilidade, onde os riscos de abusos são maiores" (p. 15).

REFERÊNCIAS BIBLIOGRÁFICAS

ARRAIS, T. A.; CASTRO, E. M. R. de. **O impacto das políticas sociais na economia local**. Brasília: Editora Fictícia, 2018.

BIONI, Bruno Ricardo. **Proteção de Dados Pessoais: A Função e os Limites do Consentimento**. Rio de Janeiro: Forense, 2020.

BRASIL. Autoridade Nacional de Proteção de Dados (ANPD). **Minuta do guia de anonimização e pseudonimização**: versão limpa pós-revisão CGN. Brasília, 2023. Disponível em: <https://www.gov.br/anpd/pt-br>. Acesso em: 7 jun. 2025.

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, 15 ago. 2018. Disponível em https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm Acesso em: 7 jun. 2025.

Castells, M. (2000). **A sociedade em rede. A era da informação**: economia, sociedade e cultura (Vol. 1). São Paulo: Paz e Terra.

CASTELLS, Manuel. **A Galáxia da Internet**: Reflexões sobre a Internet, os Negócios e a Sociedade. Rio de Janeiro: Jorge Zahar, 2000.

CASTELLS, Manuel. **A sociedade em rede. A era da informação**: economia, sociedade e cultura. Vol. 1. São Paulo: Paz e Terra, 2000.

CIRILO, L.; MELLO, C. **INSS Digital**: nova forma de atendimento ao cidadão. Brasília: INSS, 2017.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Revista de Direito do Consumidor, v. 121, p. 57-78, jan./fev. 2019.

DRAIBE, Sônia M. **As políticas sociais: balanço e perspectivas**. In: LOUREIRO, R. de C. (Org.). Direitos Sociais no Brasil: um balanço. Brasília, DF: IPEA, 2006.

FURLANETO, Mario. **Lei Geral de Proteção de Dados - Guia Prático de Implementação**. São Paulo: Novatec, 2019.

KASPER (Kaspersky). **Digital Identity Theft**: A Guide to Protecting Your Personal Information. São Paulo: Kaspersky Lab, 2022.

MARTINS, Ana Lúcia. **Segurança da Informação em Ambientes Digitais**: Um Guia Essencial. São Paulo: Editora Conexão, 2021.

MATTOS, Fernando Augusti Mansor de; CHAGAS, Gleison José do Nascimento. **Desafios para a inclusão digital no Brasil**: Perspectivas em Ciência da Informação, v. 13, n. 1, p.67-94, 01 mai. 2025. Disponível em: <https://www.scielo.br/j/pci/a/YCTSyKmxjY4FQcDZRWZXxLc/?format=pdf&lang=pt>. Acesso em 10 de outubro de 2024.

MCAFEE. Cybersecurity for Beginners: **Protecting Your Digital Life**. Santa Clara, CA: McAfee Corp., 2021.

MITNICK, Kevin D. **A Arte de Enganar**: As Melhores Histórias do Hacker Mais Famoso do Mundo. Rio de Janeiro: Campus, 2002.

MÜLLER, P.; KNOPP, T. **Segurança de Dados Pessoais**: Um Guia Prático para a LGPD. São Paulo: Saraiva Educação, 2021.

NORTON. **The Science of Phishing**: How Cybercriminals Manipulate Your Mind. Mountain View, CA: NortonLifeLock Inc., 2018.

PEREIRA, Carlos Roberto. **Direito Digital e Proteção de Dados**: Desafios e Perspectivas da LGPD. Rio de Janeiro: Forense Universitária, 2022.

PRENSKY, Marc. **Digital Natives, Digital Immigrants**. On the Horizon, MCB University Press, v. 9, n. 5, p. 1-6, out. 2001.

PRODANOV, Cleber Cristiano; FREITAS, Ernani Cesar de. **Metodologia do trabalho científico: métodos e técnicas da pesquisa e do trabalho acadêmico**. 2. ed. Novo Hamburgo: Universidade Feevale, 2013. e-book. Disponível em: <https://www.feevale.br/Comum/midias/0163c988-1f5d-496f-b118-a6e009a7a2f9/E-book%20Metodologia%20do%20Trabalho%20Cientifico.pdf>. Acesso em: 7 jun. 2025.

Sampaio, R. T. (2020). **Comentários à Lei Geral de Proteção de Dados** (Lei n. 13.709/2018). Thomson Reuters Brasil.

Sarlet, I. W. (2020). **A eficácia dos direitos fundamentais**. Porto Alegre: Livraria do Advogado.

SARLET, Ingo Wolfgang. **Dignidade da Pessoa Humana e Direitos Fundamentais na Constituição Federal de 1988**. 9. ed. Porto Alegre: Livraria do Advogado, 2007.

Sen, A. (2000). **Desenvolvimento como liberdade**. São Paulo: Companhia das Letras.

SEN, Amartya. **Desenvolvimento como liberdade**. São Paulo: Companhia das Letras, 2000.

SEN, Amartya. **Desenvolvimento como liberdade**. São Paulo: Companhia das Letras, 2000.

SILVA, Amanda; MARTINS, Roberto. **Governança de Dados e Conformidade com a LGPD**. Brasília, DF: Editora Jurídica, 2022.

SILVA, M. O. da; YAZBEK, M. C. **A política de assistência social no Brasil**: história, dilemas e perspectivas. São Paulo: Cortez, 2012.

SILVA, Mariana. **Vulnerabilidade Social e Direitos Digitais**: Análise da Proteção de Dados de Populações Carentes. Curitiba: Editora Jurídica, 2023.

SOLOVE, Daniel J. **Understanding Privacy**. Cambridge, MA: Harvard University Press, 2008.

TAPSCOTT, Don. **A economia digital**: promessa e perigo na era da inteligência em rede. São Paulo: Makron Books, 1996.

TEIXEIRA, Tarcisio. **Direito digital**. 8. ed. São Paulo: Saraiva Educação, 2020.

VAN DIJK, Jan A. G. M. **The Deepening Divide: Inequality in the Information Society**. Thousand Oaks, CA: Sage Publications, 2005.