REVISTA DE CIÊNCIAS SOCIAIS APLICADAS

Anonimização de Dados: as bases legais e implementação à luz da Lei Geral de Proteção de Dados

Data Anonymization: legal foundations and implementation under the General Data Protection Law

Osmam Brás Souto[1]
Felipe Andrade de Morais[2]

RESUMO

Este estudo pretende investigar como a anonimização de dados se insere no contexto da Lei Geral de Proteção de Dados, avaliando seus efeitos técnicos e sua implicação jurídica. Dentre os objetivos específicos, busca-se compreender os critérios técnicos necessários para que a anonimização seja considerada eficaz pela legislação, além de discutir as implicações jurídicas desta técnica no tratamento de dados pessoais. O estudo será conduzido com base no caráter qualitativo e exploratório, com análise bibliográfica e documental sobre a Lei Geral de Proteção de Dados, anonimização de dados e a legislação comparada, principalmente o GDPR da União Europeia. Além disso, serão analisados casos práticos e decisões judiciais relevantes sobre a aplicação da anonimização no contexto jurídico brasileiro. Espera-se que a pesquisa possa demonstrar que a anonimização de dados é uma ferramenta eficiente para garantir o compliance com a LGPD, desde que as técnicas aplicadas sejam eficazes e irreversíveis. Além disso, espera-se identificar as principais dificuldades e desafios das empresas e órgãos públicos na implementação da anonimização e sugerir melhorias para otimizar esse processo.

Palavras-chave: Lei Geral de Proteção de Dados; Anonimização; *Compliance*.

ABSTRACT

This study aims to investigate how data anonymization fits within the context of the General Data Protection Law, assessing its technical effects and legal implications. Among the specific objectives, it seeks to understand the technical criteria necessary for anonymization to be considered effective by legislation, as well as to discuss the legal implications of this technique in the processing of personal data. The study will be conducted based on a qualitative and exploratory approach, with bibliographic and documentary analysis on the General Data Protection Law, data anonymization, and comparative legislation, especially the GDPR of the European Union. Additionally, practical cases and relevant court decisions regarding the application of anonymization in the Brazilian legal context will be analyzed. It is expected that the research will demonstrate that data anonymization is an effective tool to ensure compliance with the LGPD, provided that the techniques applied are effective and irreversible. Furthermore, it is anticipated that the study will identify the main difficulties and challenges faced by companies and public bodies in implementing anonymization and suggest improvements to optimize this process.

Keywords: General Data Protection Law; Anonymization; Compliance.

[1]Doutor em Tecnologias Educacionais, Centro Universitário Uniceplac. E-mail: osmam.souto@uniceplac.edu.br
[2] Graduando em Direito, Centro Universitário Uniceplac. E-mail: felipe.morais@direito.uniceplac.edu.br

1 INTRODUÇÃO

O presente artigo nasce da inquietação acadêmica em investigar a aplicação concreta da técnica de anonimização de dados no contexto jurídico brasileiro, especialmente à luz das lacunas existentes na legislação nacional. A pesquisa, de natureza bibliográfica, procura aprofundar a discussão sobre os mecanismos e critérios que orientam o uso da anonimização como instrumento de proteção à privacidade dos indivíduos, considerando as exigências da Lei Geral de Proteção de Dados (LGPD) e os desafios que envolvem sua efetivação prática.

Diante disso, a investigação se debruça sobre a seguinte problemática: de que forma a anonimização pode ser implementada para atender aos requisitos da legislação vigente, assegurando a proteção da privacidade dos titulares de dados e respeitando os limites impostos pela norma?

O objetivo central deste trabalho é explorar a viabilidade e a forma adequada de aplicação da anonimização de dados à luz da LGPD, abordando tanto os aspectos normativos quanto os técnicos que permeiam o tema. Trata-se de um esforço para esclarecer, com base na literatura especializada, as possibilidades e os limites dessa prática no ordenamento jurídico brasileiro, promovendo uma análise crítica de sua eficácia como ferramenta de conformidade legal.

Dentre os objetivos específicos, destaca-se a intenção de estudar detalhadamente os conceitos fundamentais e os requisitos técnicos que definem a anonimização de dados. Também se pretende investigar como a LGPD interpreta e regula os dados anonimizados, além de discutir os ganhos e perdas associados ao uso dessa técnica no âmbito da proteção de dados pessoais. Por fim, será examinada a utilidade da anonimização como instrumento de compliance por parte das organizações que tratam informações sensíveis.

A hipótese que guia a presente pesquisa parte da premissa de que, quando implementada com critérios técnicos adequados e respaldo documental, a anonimização representa uma alternativa viável e segura para a conformidade com a LGPD. Essa prática poderia, inclusive, conferir maior previsibilidade jurídica aos agentes de tratamento de dados, permitindo uma gestão mais eficiente das informações coletadas, armazenadas e processadas.

A crescente preocupação global com a proteção dos dados pessoais encontra eco no Brasil, principalmente a partir da vigência da LGPD em 2020. A legislação impôs novos paradigmas à atuação das empresas e instituições públicas no que tange ao tratamento de dados, destacando-se, entre outras exigências, a necessidade de preservar a identidade dos titulares. A anonimização surge, nesse contexto, como uma ferramenta promissora para alcançar esse objetivo, embora sua execução prática ainda esteja cercada de desafios técnicos e jurídicos.

A pesquisa proposta busca oferecer subsídios para que os agentes de tratamento compreendam a relevância da anonimização como forma de atender aos preceitos legais sem comprometer a eficiência de suas operações.

2 DESENVOLVIMENTO

O crescimento contínuo do tráfego de informações por meio de canais digitais tem sido um dos fenômenos mais marcantes das últimas décadas, refletindo diretamente na forma como os dados circulam globalmente. Estimativas apontam que, apenas entre 2016 e 2020, houve um incremento de 30% no fluxo de dados mundial, com um salto significativo de 48%

no tráfego da internet internacional somente entre 2019 e 2020 (Brodsky, 2020). Esses números ilustram como o universo digital se consolidou como espaço central para o compartilhamento de informações, ao mesmo tempo em que amplia os riscos associados à exposição indevida de dados pessoais.

Diante dessa expansão acelerada, torna-se evidente a necessidade de normas e mecanismos que assegurem a proteção dos dados dos indivíduos. A digitalização de processos e a intensificação do uso de tecnologias de coleta e análise de dados exigem um controle rigoroso sobre a finalidade de uso dessas informações, que podem servir desde pesquisas acadêmicas até estratégias de marketing digital. A complexidade do tratamento de dados impõe um desafio contemporâneo: como garantir a segurança das informações sem limitar seu valor funcional e econômico?

Conforme observa Guilherme (2021, p. 11), o uso de dados transformou-se em uma atividade altamente lucrativa, na qual a privacidade passou a ser monetizada como parte de um modelo de negócios. Ao reconhecer o dado pessoal como um bem de valor, a legislação brasileira busca impedir abusos praticados por empresas e plataformas digitais.

A amplitude do uso de dados é notória. Eles são empregados para definir políticas públicas mais eficazes, criar soluções em saúde, educação e segurança, além de servirem como base para estratégias comerciais e financeiras. Essa pluralidade de finalidades reforça a importância da existência de normativas que regulem sua circulação, evitando abusos e garantindo a transparência no processo de tratamento de dados.

À medida que cresce o volume de dados trafegando pelas redes, amplia-se também o debate sobre os limites da utilização dessas informações. Muitos países, atentos à necessidade de proteger os indivíduos, passaram a elaborar legislações específicas voltadas à regulação do tratamento de dados pessoais. Essa tendência regulatória internacional reflete a preocupação com o equilíbrio entre inovação tecnológica e proteção de direitos.

Exemplos disso podem ser encontrados na União Europeia, com o Regulamento Geral sobre a Proteção de Dados (GDPR); na Argentina, com a Lei nº 25.326 de 2000; e no Japão, com a Act on the Protection of Personal Information (APPI), de 2015. Tais normativas representam importantes marcos legais na defesa da privacidade e têm influenciado positivamente outros países, inclusive o Brasil, na formulação de suas próprias legislações.

A LGPD, promulgada em 2018 e vigente desde 2020, foi o passo fundamental do Brasil para alinhar-se ao cenário internacional de proteção de dados. Sua principal missão é estabelecer diretrizes claras para o tratamento responsável de informações pessoais, fortalecendo os direitos dos cidadãos e impondo obrigações às empresas e instituições públicas que atuam como agentes de tratamento.

A norma brasileira adota como pilares a proteção da privacidade, a segurança da informação e o respeito à liberdade informacional dos indivíduos. Ao colocar em destaque os direitos à personalidade e ao controle dos próprios dados, a LGPD busca reequilibrar as relações entre os titulares e os agentes de tratamento, estabelecendo deveres, obrigações e sanções administrativas para quem desrespeitar suas disposições.

Entre os princípios que regem a LGPD, destaca-se o da finalidade, que determina que os dados devem ser utilizados com propósitos legítimos, específicos e informados. Essa exigência reforça o compromisso com a transparência e impede o uso desvirtuado das informações pessoais, exigindo clareza na comunicação entre os controladores e os titulares.

É nesse cenário que se insere a anonimização, um dos mecanismos sugeridos pela LGPD para o tratamento adequado de dados. Trata-se de um processo técnico que busca eliminar qualquer possibilidade de associação direta ou indireta entre o dado e seu titular, sendo fundamental para minimizar os riscos de exposição e vazamento de informações.

2.1 Lei Geral de Proteção de Dados (LGPD)

A LGPD tem o intuito de preservar o dado pessoal tendo em vista o titular e a sua personalidade, estabelecendo diretrizes sobre quanto o controle que o titular pode ofertar sobre seus dados, desse modo, a Lei Geral de Proteção de Dados, em suas disposições inaugurais, estabelece o direcionamento que deverá ser dado no tratamento de dados pessoais, seja esse tratamento feito por pessoa física ou pessoa jurídica, de direito público ou privado.

Com base nesse entendimento, observa-se que a Lei Geral de Proteção de Dados Pessoais (LGPD) tem como finalidade central a proteção dos dados pessoais dos indivíduos, reconhecendo tais informações como elementos essenciais à dignidade e à autodeterminação informativa. A legislação adota uma conceituação abrangente de dado pessoal, definindo-o como toda informação relacionada a pessoa natural identificada ou identificável, conforme dispõe o art. 5º, inciso I. Nesse contexto, a LGPD também estabelece uma distinção relevante entre dado pessoal comum e dado pessoal sensível. Este último engloba informações de natureza mais íntima e potencialmente discriminatória, como aqueles referentes à origem racial ou étnica, convicções religiosas, opiniões políticas, filiação a sindicatos ou organizações religiosas, filosóficas ou políticas, bem como dados relativos à saúde, vida sexual, informações genéticas ou biométricas, desde que associadas a uma pessoa natural, nos termos do art. 5º, inciso II.

No que tange ao tratamento de dados, a LGPD também se encarrega de delimitar com precisão o alcance desse conceito, a fim de garantir a clareza sobre as atividades que envolvem o uso de dados pessoais. Conforme previsto no art. 5º, inciso X, tratamento é definido como toda operação realizada com dados pessoais, independentemente do meio utilizado, incluindo a coleta, produção, recepção, entre outras ações. Tal definição evidencia o amplo espectro de ações abarcadas pela legislação, reforçando a necessidade de observância rigorosa aos princípios e deveres nela contidos por parte dos agentes de tratamento.

A Lei Geral de Proteção de Dados ainda prevê a definição de agente de tratamento (art. 5, IX da LGPD) sendo o controlador e o operador, os quais competem as deliberações quanto a realização de tratamento de dados, bem como a competência decisória quando as medidas a serem adotadas.

Por fim, a Lei Geral de Proteção de Dados prevê as hipóteses e requisitos que deverão ser preenchidos para que o tratamento de dados pessoais seja aplicado em seu art. 7, caput.

A proteção de dados pessoais nada mais é do que a junção de uma sequência de processos de segurança aplicados em operações de tratamento de dados, além disso, a LGPD de modo principiológico estabelece disposições gerais capazes de direcionar os preceitos basilares da proteção de dados. Em seu art. 2º, a LGPD dispões sobre os fundamentos aplicados à proteção de dados, bem como:

> Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
> I – o respeito à privacidade;
> II – a autodeterminação informativa;
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
> IV – a inviolabilidade da intimidade, da honra e da imagem;
> V – o desenvolvimento econômico e tecnológico e a inovação;
> VI – a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (Brasil, 2018).

Conforme destaca Guilherme (2021, p. 11), nota-se de maneira clara a intenção do legislador em resguardar os direitos da personalidade, em consonância com os dispositivos do Código Civil brasileiro, especialmente entre os artigos 11 e 21. Assim, a proteção conferida aos dados pessoais não se restringe a uma dimensão técnica ou burocrática, mas se fundamenta no reconhecimento da dignidade humana como núcleo fundamental do ordenamento jurídico.

Ainda com base na interpretação de Guilherme (2021, p. 18), a LGPD conceitua de forma ampla e inclusiva o termo "tratamento de dados", compreendendo como tal qualquer operação realizada com dados pessoais, o que abarca desde a coleta até o armazenamento, passando pelo uso, compartilhamento e eliminação dessas informações. Para que a proteção de dados se materialize de forma eficaz, é imprescindível compreender que ela depende da integração de três camadas estruturantes: a governança de dados, a política de privacidade e a política de segurança da informação, conforme delineado pela norma técnica ISO/IEC 27001 (2019).

A governança de dados, por sua vez, refere-se ao conjunto de diretrizes, processos e padrões internos adotados por uma organização com o propósito de estruturar e controlar o fluxo de informações pessoais sob sua responsabilidade. Trata-se de uma estratégia de gestão que busca estabelecer os fundamentos e valores que orientarão o tratamento dos dados, cabendo aos controladores e operadores a responsabilidade de definir e aplicar as regras específicas que regerão esse processo, conforme previsto no art. 50 da LGPD. Embora a legislação conceda aos agentes de tratamento certa autonomia para desenvolverem políticas internas de governança, essa liberdade está condicionada à observância dos princípios da proteção de dados e ao cumprimento das boas práticas. Nesse sentido, o Manual da Associação Brasileira de Advogados (ABA) para a adequação à LGPD orienta que as organizações adotem um sistema de governança robusto, com mecanismos que assegurem a responsabilização, a transparência, o monitoramento contínuo e a revisão periódica das medidas implementadas, promovendo uma cultura organizacional voltada à conformidade e à ética no tratamento de dados pessoais.

A política de privacidade é um elemento que decorre da governança, mais especificamente da sua aplicação, uma vez que o implemento da governança visa o compliance com a legislação atrelado a boas práticas, deste modo, uma vez estabelecido o compliance por meio da governança, a política de segurança da informação busca se ocupar do tratamento efetivo destes dados, bem como a sua manutenção e a sua operação. Podemos ter uma melhor compreensão quanto a política de privacidade analisando o regramento da legislação a respeito da segurança e do sigilo de dados, dispostas no Capítulo VII, da Lei Geral de Proteção de Dados, vejamos,

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
>
> § 1º A autoridade nacional poderá dispor sobre padrões técnicos mínimos para tornar aplicável o disposto no caput deste artigo, considerados a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis, assim como os princípios previstos no caput do art. 6º desta Lei.
>
> § 2º As medidas de que trata o caput deste artigo deverão ser observadas

desde a fase de concepção do produto ou do serviço até a sua execução.

No âmbito das normas internacionais, a política de segurança da informação ganha respaldo em instrumentos técnicos consolidados, como as normas ISO/IEC 27701 e ISO/IEC 27001. A primeira, voltada à gestão da privacidade da informação, define requisitos e boas práticas voltadas à construção, manutenção e aprimoramento de sistemas de gestão da informação, assegurando que os dados pessoais sejam tratados de forma responsável e alinhada às expectativas legais e éticas. Já a ISO/IEC 27001 estabelece parâmetros para a estruturação de sistemas de segurança da informação, abrangendo processos de planejamento, implementação, monitoramento e melhoria contínua, com ênfase na proteção de ativos informacionais e na resposta eficiente a incidentes de segurança.

A convergência entre a LGPD e essas normas internacionais reforça a necessidade de integração entre a legislação e a governança organizacional. A eficácia da proteção de dados se potencializa quando as organizações adotam políticas internas compatíveis com os modelos de gestão padronizados, promovendo uma cultura de conformidade e controle. Assim, a LGPD não apenas impõe obrigações legais, mas também estimula a adoção de boas práticas que já são amplamente reconhecidas em escala global, como parte de uma abordagem estruturada e estratégica de proteção da privacidade.

Ao se tratar da operacionalização do tratamento de dados, é fundamental compreender as etapas que compõem o chamado “ciclo de vida” dos dados pessoais. Segundo documento técnico elaborado pelo Comitê de Privacidade da Secretaria de Estado da Fazenda de Minas Gerais, o tratamento de dados deve ser compreendido como um processo dividido em cinco fases distintas: coleta, retenção, processamento, compartilhamento e, por fim, eliminação. Cada uma dessas etapas demanda cuidados específicos e o cumprimento de requisitos legais e técnicos que assegurem a proteção dos dados ao longo de todo seu percurso dentro da organização.

Na fase da coleta, é essencial garantir que os dados sejam obtidos mediante consentimento claro e informado, ou com base em hipóteses legais previstas na LGPD. A retenção, por sua vez, deve ocorrer por prazo necessário ao cumprimento da finalidade que justificou o tratamento, evitando o armazenamento excessivo e desnecessário. Já o processamento abrange todas as ações realizadas sobre os dados, o que inclui análise, cruzamento, categorização e outras atividades que exijam controle técnico rigoroso. O compartilhamento, quando necessário, exige transparência e critérios normativos objetivos para que terceiros também se comprometam com a proteção das informações compartilhadas.

A etapa da eliminação representa um dos pontos mais críticos da gestão de dados, pois envolve não apenas a exclusão segura das informações dos sistemas, mas também o dever de comprovar que o dado foi efetivamente descartado, não restando qualquer possibilidade de recuperação indevida. Compreender e respeitar esse ciclo é condição indispensável para garantir a conformidade com a LGPD, a confiança do titular dos dados e a integridade do ambiente digital. Assim, é por meio da harmonização entre normas legais e técnicas, como as normas ISO, e a gestão consciente de cada fase do ciclo de vida dos dados, que se constrói um modelo de proteção sólido e eficaz.

2.2 Aspectos legais da anonimização na LGPD

A exploração descontrolada e muitas vezes predatória de dados pessoais por organizações públicas e privadas passou a ser vista como uma estratégia de mercado, transformando-se em um modelo de negócio baseado no acúmulo indiscriminado de informações. Essa prática gerou um fenômeno conhecido como *data swamp*, caracterizado pela formação de grandes volumes de dados sem qualquer governança ou estruturação adequada, conforme exposto por Barbieri (2020). A ausência de critérios técnicos e jurídicos

para o tratamento desses dados resultou em um ambiente caótico e vulnerável, incompatível com os princípios da finalidade específica e da transparência, que foram estabelecidos pela Lei Geral de Proteção de Dados (LGPD) como fundamentais à proteção da privacidade e da integridade dos titulares.

Antes de aprofundar a análise sobre os contornos legais da anonimização e sua aplicação prática, é essencial esclarecer o seu conceito jurídico e técnico. A anonimização é descrita como um conjunto de procedimentos que visam suprimir qualquer dado que permita a identificação direta ou indireta de um indivíduo. Luiz Fernando Guilherme (2021) define a anonimização como um "procedimento segundo o qual se desvincula certo dado a uma pessoa", o que implica na despersonalização das informações. Nesse sentido, a LGPD, em seu artigo 5º, inciso III, estabelece que o dado anonimizado é aquele que, considerando os meios técnicos razoáveis e disponíveis no momento do tratamento, não permite a identificação do seu titular. Assim, entende-se que a anonimização rompe com o vínculo entre a informação e o sujeito a quem se refere.

De acordo com o artigo 12 da LGPD, os dados anonimizados não são considerados dados pessoais para os fins da legislação, exceto nos casos em que o processo de anonimização seja reversível mediante o uso de esforços razoáveis e meios próprios. Guilherme (2021) destaca que, “quando houver a possibilidade de reidentificação do titular por meio de tecnologias razoavelmente acessíveis, o dado deverá voltar a ser tratado sob os rigores da LGPD.” A legislação, portanto, admite uma zona de exceção, na qual a anonimização, se não for tecnicamente sólida, pode perder seu efeito protetivo.

O parágrafo 1º do mesmo artigo estabelece parâmetros objetivos para o que se considera "esforço razoável", incluindo o tempo e o custo envolvidos na tentativa de reverter o processo de anonimização, à luz das tecnologias disponíveis. Essa cláusula representa uma importante salvaguarda legal, pois delimita até que ponto um dado pode ser tratado como efetivamente anonimizado. Barbieri (2020) acrescenta que a anonimização deve ser compreendida como uma estratégia de *privacy by design*, isto é, como uma abordagem preventiva que incorpora a proteção de dados desde a concepção do sistema. Com isso, não apenas a confidencialidade é assegurada, mas também se amplia a disponibilidade dos dados, visto que eles não estão sujeitos às mesmas restrições impostas aos dados pessoais.

A implementação de mecanismos eficazes de anonimização exige uma avaliação contextual que considere o grau de identificabilidade presente na base de dados analisada Bioni (2021). Como consequência da perda da característica de dado pessoal, o consentimento do titular torna-se dispensável para a manutenção desses dados pelo controlador. A LGPD, inclusive, autoriza a anonimização como alternativa à eliminação de dados ao término do tratamento, nos termos do art. 16, inciso IV, quando o uso exclusivo do controlador não for incompatível com os direitos do titular.

No que se refere às técnicas de anonimização, há diversas metodologias reconhecidas no âmbito técnico. Brasher (2018) identificou algumas das principais estratégias utilizadas para garantir a descaracterização dos dados pessoais, entre as quais destacam-se: supressão, generalização, agregação, adição de ruído e substituição. Essas técnicas têm aplicação variada a depender da natureza da base de dados e da sensibilidade das informações envolvidas. Cada uma apresenta graus distintos de segurança e de perda de precisão informacional, sendo necessário ponderar entre a proteção da privacidade e a utilidade dos dados tratados.

Complementarmente, o Parecer 05/2014, emitido pelo Grupo de Trabalho do Artigo 29 da União Europeia, traz uma abordagem crítica e técnica sobre as práticas de anonimização. O documento destaca que, independentemente da técnica adotada, sempre existirão riscos residuais que devem ser constantemente monitorados. A anonimização não deve ser considerada uma medida pontual, mas parte de um processo contínuo de avaliação, em que

os riscos de reidentificação são reexaminados periodicamente com base nos avanços tecnológicos e contextuais. Apesar de admitir tais riscos, a LGPD reconhece a anonimização como o método mais seguro e juridicamente adequado para o tratamento de dados sensíveis, conforme disposto no artigo 7º, inciso IV.

Paralelamente à anonimização, a LGPD também contempla outras técnicas de proteção de dados, como a pseudonimização. Essa técnica é mencionada no §4º do art. 13 da LGPD e é definida como o processo pelo qual um dado perde a possibilidade de associação direta ou indireta a uma pessoa, exceto mediante o uso de informações adicionais que devem ser mantidas separadamente em ambiente seguro e controlado. Embora seja uma forma de proteção relevante, ela não exclui a possibilidade de reidentificação, o que a diferencia substancialmente da anonimização.

A pseudonimização, portanto, deve ser compreendida como uma técnica auxiliar e não como uma solução definitiva de proteção de dados. Ao contrário da anonimização, ela não rompe completamente o vínculo entre os dados e seus titulares, pois admite a reversão da de-identificação mediante acesso a elementos adicionais. Essa possibilidade impõe restrições quanto ao seu uso em contextos que exijam maior grau de confidencialidade, como no tratamento de dados sensíveis ou em pesquisas científicas com sigilo garantido.

Com base nas definições legais e técnicas, conclui-se que a anonimização constitui uma das principais estratégias de conformidade com a LGPD. Seu uso possibilita o processamento de dados sem infringir os direitos fundamentais do titular, promovendo a confidencialidade e a segurança das informações tratadas. O dado anonimizado, conforme estabelece a legislação brasileira, não é considerado dado pessoal, salvo nos casos em que seja possível reverter o processo com esforços razoáveis, conforme os critérios definidos em lei. Assim, a anonimização deve ser compreendida não apenas como um recurso técnico, mas como uma exigência ética e jurídica voltada à proteção da dignidade informacional do indivíduo.

3 PRINCIPAIS TÉCNICAS DE ANONIMIZAÇÃO

O processo de anonimização visa atuação sobre os identificadores de um dado de modo a garantir a irreversibilidade e a impossibilidade de identificação do titular, como já discorrido, no entanto o processo de aplicação está fundado na pertinência dada ao caso concreto. Esta situação se deve ao fato de que a LGPD não estabeleceu regra específica na utilização das técnicas de anonimização de forma expressa, não há, portanto, metodologia universal aplicável.

Preliminarmente é importante compreender os conceitos de *Personally Identifiable Information* (PII), que representam as informações pessoalmente identificáveis que ligam o dado ao seu titular (Brasher, 2018). Portanto a aplicação da anonimização enquanto técnica incidirá sob as informações de identificação pessoal ou PII.

Ao retomar a atenção para a aplicação de técnicas de anonimização enquanto instrumento que garante a adequação na proteção de dados pessoais, é possível notar um amplo conjunto de metodologias. Respectivamente cada uma dessas metodologias ou técnicas possuem funcionamento e requisitos próprios, sendo assim, para promover o amplo entendimento quanto a aplicação da anonimização é necessária antes compreender em que circunstâncias deverão ser utilizadas cada técnica, bem como o seu funcionamento:

A supressão é o processo que remove as informações de identificação pessoal (PII) em sua integridade de uma base de dados ou garante a substituição de informações por valores fixos pré-definidos (Brasher, 2018), oferecendo uma ampla proteção, efetividade e segurança ao titular dos dados. Na prática são suprimidos os dados dos titulares como seus CPF, RG, e seu número, por exemplo.

Ao imaginar uma situação real de aplicação da supressão, é possível imaginar o seguinte: Um administrador de dados de um hospital que acompanha prescrições médicas deverá suprimir os nomes dos pacientes antes de compartilhar os seus dados (Ohm, 2009). Com base no apresentado, segue um demonstrativo da aplicação da supressão, conforme Tabela 1.

Tabela 1 – Demonstração da aplicação da supressão

Dado Original	Dado anonimizado
CPF: “123.456.789-12”	“xxx.xxx.xxx-xx”
RG: “1.234.567”	“REMOVIDO”

Fonte: os autores (2025)

O dilema em torno do uso da supressão está ligado ao distanciamento da realidade do dado que esse processo promove, uma vez que esta técnica proporciona um fator acentuado de perda da integralidade do dado pessoal. Esta questão se deve ao fato de que a supressão é uma técnica considerada agressiva, promovendo uma redução significativa na utilidade dos registros anonimizados (Brasher, 2018). Desse modo, entende-se que a sua utilização de forma isolada pode promover a inutilização de para fins posteriores que precisam ser dados a esses dados suprimidos.

A Generalização de atributos é o processo que embaralha as informações de identificação pessoal de modo que confunde a sua real vinculação, sem excluir qualquer informação do conjunto original, porém confundindo a sua real vinculação. De acordo com Paul Ohm, a generalização consegue alcançar um equilíbrio mais adequado com relação à privacidade e a utilidade do dado, bem como a integridade da informação (Ohm, 2009). Com base no apresentado, segue o demonstrativo da aplicação da generalização (Tabela 2).

Tabela 2 – Exemplo de estrutura de banco de dados original

Nome Completo	Cidade de Nascimento	Idade
Fernando Silva	Porto Alegre	54
Maria Santos	Uberlândia	75
José Pereira	João Pessoa	38

Fonte: os autores (2025)

A Tabela 3 em questão apresenta como seria a estrutura de um banco de dados, onde foram coletados dados capazes de identificar o seu titular. Em consonância com o modelo de aplicação da generalização, segue a tabela dos dados anonimizados por meio da generalização.

Tabela 3 – Dados anonimizados por meio da generalização

Nome Completo	Estado de Nascimento	Faixa Etária
FS	Rio Grande do Sul	50-60
MS	Minas Gerais	70-80
JP	Paraíba	30-40

Fonte: os autores (2025)

A principal crítica ao modelo de anonimização por generalização de atributos é a constatação de que o revestimento de proteção neste caso seria mais frágil que o dado anonimizado pela supressão, em contrapartida, a informação ainda se apresenta íntegra.

A Agregação é o processo de anonimização que reduz a especificidade do dado mantendo suas propriedades, podendo unir informações auxiliares para apresentar um panorama geral. Trata-se de espécie de anonimização muito utilizada em médias ou distribuições estatísticas, pois, para Brasher (2018, p. 7). “fornece estatísticas resumidas ao agrupar titulares que compartilham algum dado pessoal”. A Adição de Ruído consiste no processo que adiciona informações externas de dados improdutivos, com o intuito de confundir a vinculação entre PII e o seu titular. A Substituição é a técnica que mistura os valores de dados em si, substituindo os identificadores por um outro parâmetro de dados.

Para (Basher, 2018, p. 7), a Agregação, a Adição de Ruído e a Substituição “reduzem substancialmente a capacidade de vincular os dados anonimizados aos seus titulares, ao impedir o acesso aos dados brutos”.

Dentre as modalidades de anonimização apresentadas, a Supressão se mostra como a mais agressiva entre elas, uma vez que descarta completamente os PII durante o tratamento. Em contrapartida as demais técnicas tem a capacidade de tornar imprecisas as informações apresentadas, o que dificulta a vinculação direta com o titular.

Cabe ainda ressaltar que a ANPD já se manifestou pelo entendimento que (Nota Técnica nº 46/2022/CGF/ANPD, p. 7) “a anonimização não é uma medida de segurança impositiva, que deve ser adotada em todo e qualquer tratamento de dados pessoais”, visto que a adoção dessas medidas deve seguir de uma análise à luz dos princípios da finalidade e necessidade (Art. 6, I e III) na situação concreta.

3.1 Desafios na implementação prática: análise dos limites éticos atinentes à privacidade

A anonimização de dados pessoais, embora tecnicamente consolidada como uma das estratégias mais promissoras para garantir a privacidade no tratamento informacional, enfrenta diversos desafios quando transposta para o plano ético e jurídico. Conforme aponta Brasher (2018), apesar de sua adoção crescente, a anonimização tem falhado em garantir uma proteção efetiva e irreversível à identidade dos titulares, principalmente em razão da evolução das técnicas de reidentificação. Nesse cenário, a discussão ultrapassa os limites da

segurança da informação e alcança o campo dos direitos fundamentais, sobretudo o direito à privacidade, o qual se apresenta cada vez mais vulnerável em contextos de hiperdigitalização.

A dificuldade em delimitar o próprio conceito de privacidade é um dos principais entraves éticos na aplicação da anonimização. Tradicionalmente concebida como o "direito de ser deixado em paz" (*right to be let alone*), a privacidade evoluiu e hoje assume contornos mais complexos, especialmente no contexto da sociedade da informação. Para Doneda (2021), a privacidade deve ser compreendida como um direito dinâmico, em constante mutação, que requer releitura à luz das novas formas de processamento de dados. Na era digital, os limites da privacidade não estão apenas ligados à não exposição, mas à capacidade de controle que o titular exerce sobre suas informações pessoais.

A LGPD incorpora esse novo entendimento ao propor o princípio da autodeterminação informacional como base para o tratamento de dados, conferindo ao titular maior controle sobre o uso de suas informações (Guilherme, 2021). Contudo, mesmo com o respaldo legal, a aplicação prática da anonimização revela limitações técnicas e jurídicas que impedem a efetivação plena desse direito. Ferreira (2023) destaca que os riscos residuais de reidentificação, mesmo após procedimentos de anonimização, colocam em xeque a eficácia das medidas implementadas, especialmente diante do avanço de tecnologias de big data e inteligência artificial.

O Parecer 05/2014 do Grupo de Trabalho do Artigo 29 da União Europeia já alertava para a necessidade de revisão contínua das técnicas de anonimização, recomendando a avaliação periódica dos riscos e a adoção de salvaguardas proporcionais. Essa preocupação é corroborada por Ohm (2009), que argumenta que a anonimização muitas vezes cria uma falsa sensação de segurança, pois ignora os potenciais de reidentificação que emergem da combinação de dados aparentemente inócuos.

Em sua pesquisa, Carvalho (2021) adverte que a anonimização não deve ser vista como solução absoluta, mas como uma camada de proteção adicional dentro de um ecossistema de segurança mais amplo. O desafio, segundo a autora, está na necessidade de reconhecer os limites dessa técnica e no dever de não negligenciar os impactos éticos associados ao uso indevido de dados anonimizados, sobretudo quando o tratamento desses dados é conduzido de maneira opaca ou sem finalidades legítimas. A ausência de governança sólida e transparência institucional pode comprometer significativamente a integridade do processo.

Narayanan e Shmatikov (2010) alertam que a reidentificação pode ocorrer mesmo sem o uso direto de dados sensíveis, a partir da correlação de padrões e perfis, desafiando o pressuposto de que a anonimização torna os dados inofensivos. Isso implica em uma revisão crítica da neutralidade atribuída aos dados anonimizados.

Além disso, a LGPD, ao definir no artigo 12 que os dados anonimizados não serão considerados dados pessoais, exceto quando sujeitos à reversão por meios razoáveis, introduz um conceito vago e passível de interpretações diversas sobre o que seria "esforço razoável". Mendes *et al*. (2023) afirmam que esse critério deve ser compreendido à luz da proporcionalidade, ponderando-se tempo, custo, complexidade técnica e o estado atual das tecnologias disponíveis. No entanto, essa indeterminação abre margem para controvérsias jurídicas e decisões contraditórias no âmbito judicial.

Do ponto de vista da ética, a manipulação de dados anonimizados sem o consentimento do titular, ainda que tecnicamente permitida pela legislação, pode violar os princípios fundamentais de transparência e finalidade. Lima *et al*. (2022) observam que a anonimização, quando realizada de forma descontextualizada e sem critérios claros de necessidade, pode configurar uma afronta à confiança depositada pelos indivíduos nas instituições que processam seus dados. Portanto, é indispensável que a anonimização esteja

inserida em um sistema de governança ético, transparente e comprometido com o respeito aos direitos fundamentais.

Ferreira *et al*. (2022) contribuem ao propor que a anonimização seja acompanhada de políticas robustas de mitigação de riscos, com auditorias regulares, protocolos de resposta a incidentes e mecanismos de accountability. Isso está em consonância com a abordagem de *privacy by design*, defendida pela ISO/IEC 27701 (2019), que determina que a proteção da privacidade deve ser incorporada desde o início do ciclo de vida dos dados. A implementação dessas diretrizes ainda é um desafio, sobretudo em ambientes com pouca maturidade digital ou baixa compreensão dos impactos jurídicos do tratamento de dados.

Outro ponto crítico é o impacto da anonimização em contextos de exclusão social e discriminação algorítmica. Segundo Neves (2023), a aplicação de algoritmos de anonimização em ambientes de internet das coisas (IoT) pode reproduzir vieses existentes nos dados originais, mesmo que desidentificados. Isso demonstra que a anonimização, por si só, não é suficiente para eliminar os efeitos nocivos da coleta massiva de dados. Assim, é necessário pensar a técnica dentro de uma perspectiva interseccional, considerando os impactos sobre populações vulneráveis.

Na perspectiva do direito administrativo, o Decreto nº 45.771/2024 do Distrito Federal estabelece diretrizes para a implementação da LGPD nos órgãos públicos, reforçando a necessidade de anonimização nos processos que envolvam dados sensíveis. No entanto, Sales e Spósito (2023) demonstram que a efetividade dessas diretrizes ainda é limitada pela escassez de ferramentas tecnológicas compatíveis com a realidade da administração pública e pela ausência de capacitação técnica adequada entre os servidores responsáveis pelo tratamento de dados.

Diante do exposto, verifica-se então que os limites éticos da anonimização se manifestam na tensão entre a eficácia técnica e a proteção integral da dignidade da pessoa humana. A anonimização não pode ser vista como um fim em si mesma, mas como parte de uma política mais ampla de proteção de dados, que envolva ética, transparência, governança e responsabilidade social. Conforme advertido por Pinheiro (2020), o respeito à privacidade deve ser construído a partir de uma compreensão sistêmica, que vá além da mera conformidade normativa e alcance o compromisso genuíno com os direitos fundamentais no ambiente digital.

3.2 Anonimização como mecanismo de conformidade

A anonimização, quando utilizada como um mecanismo de conformidade com a Lei Geral de Proteção de Dados (LGPD), deve ser avaliada sob critérios técnicos, jurídicos e contextuais. A pertinência de sua aplicação está diretamente relacionada à natureza da base de dados, à finalidade do tratamento e ao ambiente técnico em que os dados serão operados. Ainda que seja uma importante ferramenta para mitigar riscos à privacidade e cumprir obrigações legais, é consenso entre estudiosos que ela não elimina totalmente a possibilidade de reidentificação dos dados.

Esse risco de reidentificação ocorre justamente porque os algoritmos de mineração de dados e inteligência artificial têm se sofisticado ao ponto de cruzar múltiplas fontes informacionais, permitindo inferências altamente precisas. A técnica de reidentificação não requer, necessariamente, a presença de dados sensíveis, mas sim a combinação de dados aparentemente neutros que, reunidos, permitem a criação de perfis únicos (Narayanan; Shmatikov, 2010). Portanto, conforme defendem Ferreira *et al*. (2022), a anonimização deve ser encarada como uma prática baseada em risco, exigindo a constante revisão das técnicas utilizadas e das condições contextuais da base tratada.

A própria LGPD, ao tratar da anonimização no art. 12, prevê a possibilidade de

reversão do processo, estabelecendo a noção de “esforço razoável” como critério para a distinção entre dado anonimizado e dado pessoal. Essa cláusula, embora juridicamente necessária para evitar abusos, traz um desafio hermenêutico substancial, pois “esforço razoável” é um conceito jurídico indeterminado. Como afirmam Mendes *et al*. (2023), sua interpretação dependerá de parâmetros objetivos que levem em conta tempo, custo e viabilidade técnica, conforme expressamente previsto no §1º do artigo. No entanto, esses critérios ainda carecem de jurisprudência consolidada, o que pode gerar insegurança jurídica no momento de sua aplicação.

Em complemento, o conceito de “meios próprios” também carece de melhor definição normativa, mas pode ser compreendido, à luz de Bioni (2020), como os recursos materiais, técnicos, tecnológicos e operacionais efetivamente disponíveis ao controlador no momento da anonimização. Dessa forma, a conformidade legal não deve se apoiar unicamente na técnica aplicada, mas no exame concreto da relação entre o agente, os dados e o risco.

Para lidar com essas incertezas, alguns autores propõem a adoção de modelos de gestão baseados em risco, com políticas contínuas de avaliação e mitigação. Segundo Lima *et al*. (2022), a conformidade com a LGPD exige não apenas a adoção formal de técnicas de anonimização, mas a institucionalização de práticas de governança e segurança da informação que promovam a responsabilidade demonstrável (*accountability*) diante da Autoridade Nacional de Proteção de Dados (ANPD).

A anonimização, dentro desse modelo de conformidade, não é um evento único e estanque, mas um processo cíclico, que deve ser revisto constantemente à medida que novas ameaças e tecnologias surgem. Brasher (2018) destaca que a eficácia de qualquer técnica de desidentificação depende do contexto e da atualização constante dos métodos, sob pena de se tornar obsoleta e, portanto, ineficaz. A conformidade, portanto, exige vigilância contínua, capacitação das equipes técnicas e investimentos permanentes em tecnologia e auditoria.

Ferreira (2023) reforça que a conformidade com a LGPD deve ser sustentada por evidências técnicas de que as práticas adotadas são suficientes para minimizar os riscos de exposição indevida dos dados. Isso inclui a elaboração de relatórios de impacto à proteção de dados, a documentação dos processos de anonimização e a existência de planos de contingência.

Carvalho (2021) argumenta que, além do respaldo técnico, a anonimização como mecanismo de conformidade precisa estar inserida em um arcabouço ético, em que o respeito à autodeterminação informacional do titular seja prioridade. Isso significa que mesmo dados anonimizados devem ser tratados com cautela, especialmente quando utilizados para fins que extrapolem a expectativa legítima do titular no momento da coleta. A conformidade, nesse sentido, não se limita ao cumprimento literal da lei, mas envolve o alinhamento com os princípios gerais da proteção de dados.

Além disso, como apontam Ferreira *et al*. (2022), a utilização de dados anonimizados para fins de pesquisa e desenvolvimento deve ser cercada de controles adicionais, incluindo a análise de risco de reidentificação e o estabelecimento de critérios técnicos para acesso e uso. A anonimização, nesse contexto, deve ser integrada a uma política institucional de proteção de dados, acompanhada de revisões periódicas e avaliações independentes sobre a eficácia das técnicas aplicadas.

Por fim, Neves (2023) sustenta que, em ambientes de Internet das Coisas (IoT), a complexidade da coleta e transmissão de dados exige abordagens dinâmicas para a anonimização, baseadas em algoritmos adaptativos e modelos inteligentes. A conformidade nesses casos deve estar associada à capacidade dos sistemas de se autoconfigurarem diante de novos cenários de risco, o que demanda um avanço significativo no desenvolvimento de tecnologias reguladas e auditáveis.

A adoção da anonimização deve ser acompanhada por uma cultura de responsabilidade, de transparência e de revisão constante dos riscos, para que a proteção de dados se mantenha alinhada aos princípios da dignidade da pessoa humana e da confiança no ambiente digital.

4 CONSIDERAÇÕES FINAIS

Considerando o cenário globalizado de constante fluxo e compartilhamento de dados pessoais, torna-se imperativa a adoção de mecanismos eficazes de regulação que assegurem a proteção da privacidade dos titulares. Nesse contexto, a anonimização desponta como uma ferramenta técnica e jurídica relevante, capaz de viabilizar o tratamento de dados de forma segura e conforme aos princípios estabelecidos pela Lei Geral de Proteção de Dados (LGPD). A sua utilização permite ao controlador realizar operações sobre conjuntos de dados sem incorrer em violação direta aos direitos fundamentais dos indivíduos, desde que observadas as bases legais apropriadas, especialmente os princípios da necessidade e da finalidade. A análise do caso concreto, portanto, deve nortear a decisão pela aplicação dessa técnica, evitando generalizações ou automatismos que comprometam a eficácia da proteção.

A efetividade da anonimização, contudo, depende de sua correta implementação, que deve considerar não apenas os aspectos técnicos, mas também o valor informacional dos dados processados. Assim, a adoção de técnicas de anonimização deve encontrar um equilíbrio entre a proteção da identidade do titular e a manutenção da funcionalidade dos dados. O uso indiscriminado de procedimentos que eliminem completamente o conteúdo informacional pode gerar resultados ineficazes do ponto de vista analítico e administrativo, contrariando o próprio princípio da proporcionalidade.

Ao delimitar os contornos da aplicação da anonimização, é necessário reconhecer a existência de limitações técnicas, como a possibilidade de reidentificação dos dados, especialmente diante do avanço das tecnologias de cruzamento e mineração de informações. Essas limitações não devem ser ignoradas, uma vez que implicam riscos concretos à privacidade e à segurança dos dados tratados. Adicionalmente, é fundamental considerar os limites éticos envolvidos, que dizem respeito à proteção da dignidade do titular e ao respeito à autodeterminação informacional. A anonimização, portanto, deve ser compreendida não como uma garantia absoluta, mas como um instrumento que, embora relevante, exige contínuo aprimoramento e vigilância.

Diante disso, é prudente afirmar que a anonimização se configura como um mecanismo promissor de conformidade com a LGPD, contribuindo para a redução de riscos e para o fortalecimento da confiança nas relações jurídicas e tecnológicas envolvendo o tratamento de dados pessoais. Entretanto, a ausência de normativas específicas que padronizem sua aplicação técnica e operacional dificulta sua consolidação como prática unificada.

Outro ponto que merece atenção é a urgência de fomentar debates e iniciativas institucionais voltadas à regulamentação mais detalhada da anonimização, incluindo a definição de diretrizes claras para avaliação de risco de reidentificação, critérios objetivos sobre o conceito de "esforço razoável" e orientações sobre “meios próprios” conforme a LGPD. A elaboração de padrões técnicos e metodológicos, compatíveis com a realidade nacional, pode auxiliar na uniformização de condutas e na qualificação dos processos internos de proteção de dados. Essa normatização contribuiria para minimizar ambiguidades interpretativas e elevaria o nível de maturidade das organizações quanto ao tratamento seguro de informações.

Assim sendo, a anonimização deve ser compreendida como parte de uma estratégia maior de governança e proteção de dados, integrada a políticas de segurança da informação, boas práticas e uma cultura institucional voltada à responsabilidade no uso de informações

pessoais. Embora apresente limitações técnicas e éticas, sua utilização, quando planejada, contextualizada e auditada, pode representar um importante aliado para o cumprimento dos preceitos da LGPD. Assim, mais do que uma técnica isolada, a anonimização deve ser encarada como expressão do compromisso com os direitos fundamentais e com o respeito à privacidade em uma sociedade digital em constante transformação.

REFERÊNCIAS

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Guia sobre tratamento de dados pessoais para fins acadêmicos**. Brasília: ANPD, 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/web-guia-anpd-tratamento-de-dados-para-fins-academicos.pdf. Acesso em: 27 ago. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Nota Técnica nº 46/2022/CGF/ANPD**. Disponível em: https://www.gov.br/anpd/pt-br/documentos-epublicacoes/sei_00261-000730_2022_53-nt-46.pdf. Acesso em: 27 ago. 2024.

AMERICAN BAR ASSOCIATION (ABA). **Manual ABA para a adequação da LGPD**. [S.l.], 2020. Disponível em: https://aba.com.br/wp-content/uploads/2020/07/Manual_LGPD_04_junho.pdf. Acesso em: 27 ago. 2024.

BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. **Cadernos Jurídicos – Direito Digital e Proteção de Dados Pessoais**, São Paulo, ano 21, n. 53, p. 179–190, jan./mar. 2020. Disponível em: https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_9_anonimizacao_e_dado.pdf. Acesso em: 12 abril 2025.

BARBIERI, Carlos. **Governança de dados**. Rio de Janeiro: Editora Alta Books, 2020. E-book. ISBN 9788550815435. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788550815435/. Acesso em: 11 mar. 2025.

BARRETO, Fabíola Gonçalvez; HENRIQUE, Fabricio Gustavo. Lei Geral de Proteção de Dados e a aplicabilidade na anonimização. *In*: **WORKTEC: revista científica**. 2. ed. Ribeirão Preto: Faculdade de Tecnologia de Ribeirão Preto, 2021. Disponível em: http://www.fatecrp.edu.br/WorkTec/edicoes/2021-2/trabalhos/IV-Worktec-LEI_GERAL_DE_PROTEC%C3%87%C3%83O_DE_DADOS_E_A_APLICABILIDADE_NA_ANONI7MIZAC%C3%83O.pdf. Acesso em: 2 ago. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília: Presidência da República, 1988. Disponível em: https://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 27 ago. 2024.

BRODSKY, Paul. **Internet Traffic and Capacity in Covid- Adjusted Terms**. Blog Telegeography. 27 de agosto de 2020. Disponível em: https://blog.telegeography.com/internet traffic-and-capacity-in-covid-adjusted-terms. Acesso em: 09 mar. 2025.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 maio 2025.

BRASHER, E. A. Addressing the failure of anonymization: guidance from the European Union's General Data Protection Regulation. **Columbia Business Law Review**, v. 1, n. 1, p. 8–23, 2018. Disponível em:

https://journals.library.columbia.edu/index.php/CBLR/article/view/1217/289. Acesso em: 28 dez. 2024.

CARVALHO, Fernanda Potiguara. **O ser atrás do dado:** limites e desafios da anonimização e seus reflexos nos requisitos estabelecidos pela LGPD. 2021. [156] f., il. Dissertação (Mestrado em Direito) — Universidade de Brasília, Brasília, 2021. http://repositorio.unb.br/handle/10482/48043 . Acesso em: 27 ago. 2024.

DONEDA, Danilo. Panorama Histórico da Proteção de Dados Pessoais. *In*: DONEDA, Danilo; SARLET, Ingo Wolfgang; MENDES, Laura Schertel Mendes; RODRIGUES JÚNIOR, Otávio Luiz; BIONI, Bruno Ricardo. **Tratado de proteção de dados pessoais**. Rio de Janeiro: Ed. Forense [Book], 2021. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9788530994105. Acesso em: 11 mar. 2025.

FERREIRA, J. R. **Aplicação da Lei Geral de Proteção de Dados com Utilização de Modelos de Anonimização de Dados em Ambiente de Nuvem Pública**. Dissertação de Mestrado Profissional, Departamento de Engenharia Elétrica, Universidade de Brasília, Brasília, DF, 44 p. Disponível em: http://repositorio2.unb.br/jspui/handle/10482/47940. Acesso em: 27 ago. 2024.

FERREIRA, Juliano Rodrigues *et al*. **Mitigação dos Riscos à Privacidade através da Anonimização de Dados**. 2022. Brasília, RISTI, N.º E49, 04/2022 p. 573-585, 2022. Disponível em: https://ppee.unb.br/wp-content/uploads/2023/07/Mitigacao_dos_Riscos_a_Privaci.pdf. Acesso em: 27 ago. 2024.

FERREIRA, Juliano Rodrigues. **Aplicação da Lei Geral de Proteção de Dados com utilização de modelos de anonimização de dados em ambiente de nuvem pública**. 2023. x, 44 f., il. Dissertação (Mestrado Profissional em Engenharia Elétrica) — Universidade de Brasília, Brasília, 2023. Disponível em: https://www.ppee.unb.br/wp-content/uploads/2023/05/PPEE___Dissertacao_Juliano_Ferreira-v3-1.pdf. Acesso em: 27 ago. 2024.

GOVERNO DO DISTRITO FEDERAL. **Decreto nº 45.771, de 2024**. Sistema Integrado de Normas Jurídicas do Distrito Federal, 2024. Disponível em: https://www.sinj.df.gov.br/sinj/Norma/2d779a53407041f7b899c348124f2cdb/exec_dec_45771_+2024.html#capVI_art29. Acesso em: 27 ago. 2024.

GRUPO DE TRABALHO DE PROTEÇÃO DE DADOS DO ARTIGO 29. **Parecer 05/2014 sobre técnicas de anonimização Bruxelas**: [s. n.], 2014. Disponível em: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_pt.pdf. Acesso em: 8 maio 2025.

GUILHERME, Luiz Fernando Do Vale De **A. Manual de proteção de dados**. São Paulo: Edições 70, 2021. E-book. pág.11. ISBN 9786556272054. Disponível em: https://integrada.minhabiblioteca.com.br/reader/books/9786556272054/. Acesso em: 09 mar. 2025.

ISO Central Secretary. **Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines**. Geneva, CH, 2019. Disponível em: https://www.iso.org/standard/71670.html. Acesso 5 out. 2025.

LIMA, Adriano Carlos *et al*. **LGPD - Lei Geral de Proteção de Dados Pessoais:** Manual de Implementação. São Paulo: Thomson Reuters Revista dos Tribunais, 2022. Disponível em: https://next-proview.thomsonreuters.com/title. Acesso em: 09 mar. 2025.

LIMA, Cíntia Rosa Pereira de. **Comentários à Lei Geral de Proteção de Dados**. São Paulo: Grupo Almedina, 2020. E-book. ISBN 9788584935796. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 27 ago. 2024.

MENDES, Laura Schertel *et al*. **Anuário do Observatório da LGPD da Universidade de Brasília:** análise comparada entre elementos da LGPD e do GDPR. Brasília: Universidade de Brasília, Faculdade de Direito, 2023. v. 1. DOI: https://doi.org/10.26512/9786500923988. Disponível em: https://livros.unb.br/index.php/portal/catalog/book/540. Acesso em: 27 ago. 2024.

MORAES, Felipe Sousa. **Anonimização de Dados dos Boletins de Ocorrência**. 2023. Trabalho de conclusão de Curso (Graduação em Sistemas de Informação) – Universidade Federal Rural da Amazônia, Belém, 2023. Disponível em: https://bdta.ufra.edu.br/jspui/bitstream/123456789/3110/1/Anonimiza%c3%a7%c3%a3o%20de%20dados%20dos%20boletins%20de%20ocorr%c3%aancia.pdf. Acesso em: 27 ago. 2024.

MINAS GERAIS. Secretaria de Estado de Fazenda. **LGPD-SEF:** ciclo de vida dos dados pessoais – Introdução. [S.l.]: SEF/MG, [2022]. Disponível em: https://www.fazenda.mg.gov.br/transparencia/lgpd/LGPD-SEF-Ciclo-de-Vida-Introducao.pdf. Acesso em: 3 mar. 2025.

NEVES, Flávio da Silva. **SMART ANONYMITY:** Um Mecanismo para Recomendação de Algoritmos de Anonimização de Dados Baseado no Perfil dos Dados para Ambientes IoT. 2023. Dissertação (Doutorado em Engenharia de Software e Linguagens de Programação) – Universidade Federal de Pernambuco, Pernambuco, 2023. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/53688/1/TESE%20Fl%c3%a1vio%20da%20Silva%20Neves.pdf. Acesso em: 27 ago. 2024.

NEVES, Flávio da Silva. **Smart anonymity:** um mecanismo para recomendação de algoritmos de anonimização de dados baseado no perfil dos dados para ambientes IoT. 2023. Tese (Doutorado em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2023. Disponível em: https://repositorio.ufpe.br/handle/123456789/53688. Acesso em: 27 ago. 2024.

NARAYANAN, A.; SHMATIKOV, V. Myths and fallacies of “personally identifiable information". **In Communications of the ACM**, v. 53, n. 6, p. 24, 1 jun. 2010. Disponível em: https://dl.acm.org/doi/10.1145/1743546.1743558. Acesso em 27 ago 2024.

OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. **UCLA Law Review**, v. 57, n. 6, p. 1701–1777, 2009. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006. Acesso em: 15 nov. 2024.

PINHEIRO, Patrícia P. **Segurança Digital - Proteção de Dados nas Empresas**. Rio de Janeiro: Grupo GEN, 2020. E-book. ISBN 9788597026405. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026405/. Acesso em: 27 ago. 2024.

SALES, Raylan da Silva; SPÓSITO, Stefano Luppi. **Uma biblioteca para anonimização de dados pessoais brasileiros em textos**. 2023. Monografia (Trabalho de conclusão de Curso em Ciência da Computação) – Universidade de Brasília, Brasília, 2023. Disponível em: https://bdm.unb.br/bitstream/10483/37607/1/2023_RaylanSales_StefanoSposito_tcc.pdf. Acesso em: 27 ago. 2024.

SANTOS, E. E. dos; SOARES, T. M. M. K. R. Riscos, ameaças e vulnerabilidades: O impacto da segurança da informação nas organizações. **Revista Tecnológica da Fatec Americana**, v. 7, n. 02, p. 43–51, 2019. Disponível em:

https://www.fatec.edu.br/revista/index.php/RTecFatecAM/article/view/188/193. Acesso em: 10 abril. 2025.

SÃO PAULO (Estado). **Decreto nº 65.347, de 9 de dezembro de 2020**. Assembleia Legislativa do Estado de São Paulo, São Paulo, 2020. Disponível em: https://www.al.sp.gov.br/repositorio/legislacao/decreto/2020/decreto-65347-09.12.2020.html. Acesso em: 27 ago. 2024.

TEIXEIRA, Tarcísio; GUERREIRO, Ruth M. **Lei Geral de Proteção de Dados Pessoais (LGPD):** Comentada Artigo por Artigo. Rio de Janeiro: Grupo GEN, 2022. E-book. ISBN 9786555599015. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555599015/. Acesso em: 27 ago. 2024.