

Aplicação da Lei Geral de Proteção de Dados Pessoais para agentes de tratamento de pequeno porte: análise em clínicas odontológicas

Application of the General Data Protection Law for small-scale data processing agents: an analysis in dental clinics

Giovanna Silva Camelo Paiva
<https://orcid.org/0009-0002-3801-4187>
Bacharel em Administração. Bacharel em Direito. Universidade de Brasília (UnB), Faculdade de Economia, Administração, Contabilidade, e Gestão de Políticas Públicas, Departamento de Administração. Brasília - Brasil.
giovannascp01@gmail.com

Edvan Gomes da Silva
<https://orcid.org/0009-0005-5271-5328>
Especialização em Cibersegurança. Universidade de Brasília (UNB), Faculdade de Tecnologia, Departamento de Engenharia Elétrica, Brasília - Brasil.
edvan402@gmail.com

Carlos André de Melo Alves
<https://orcid.org/0000-0001-9566-2514>
Doutor em Administração (USP). Professor da Universidade de Brasília (UNB), Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, Departamento de Administração, Brasília - Brasil. carlosandre@unb.br

Rafael Rabelo Nunes
<https://orcid.org/0000-0002-1538-4276>
Doutor em Engenharia Elétrica. Professor da Universidade de Brasília, Brasília-DF e do Centro Universitário UniAtenas, Paracatu-MG, - Brasil.
rafaelrabelo@unb.br

RESUMO

Com o avanço das tecnologias e a crescente importância das informações na sociedade contemporânea, tornou-se necessário o gerenciamento seguro e responsável de dados. Em resposta a essa necessidade, legislaturas em todo o mundo elaboraram normas de proteção de dados pessoais para salvaguardar o direito à privacidade. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709, de 14 de agosto de 2018, regulamenta esse assunto. Agentes de tratamento de pequeno porte, como controladores e operadores de dados pessoais, podem enfrentar desafios em conformidade com a LGPD devido ao seu tamanho, requerendo intervenção da Autoridade Nacional de Proteção de Dados (ANPD) para efetuar ajustes normativos. Empresas de saúde, em especial, devem priorizar a conformidade com a LGPD, dada a natureza sensível dos dados de saúde que manipulam continuamente. Este estudo visa avaliar a aplicação da LGPD em clínicas odontológicas do Distrito Federal e da Bahia. Trata-se de pesquisa descritiva com abordagem qualitativa. A coleta dos dados empregou entrevistas com 10 cirurgiões-dentistas. Identificaram-se categorias de adequação, incluindo conhecimento da LGPD, políticas de segurança da informação, conscientização e treinamento interno, controle de acesso, segurança e armazenamento de dados pessoais, e especificidades do cotidiano em clínicas odontológicas. As análises revelaram que, apesar da natureza da área, há um conhecimento limitado sobre a LGPD entre os profissionais, destacando a falta de familiaridade com essa legislação. Os resultados têm relevância tanto para os profissionais odontológicos quanto para as autoridades encarregadas da aplicação da lei no país.

Palavras-chave: lei geral de proteção de dados pessoais; privacidade de dados pessoais; agentes de tratamento de dados; clínicas odontológicas.

ABSTRACT

With the advancement in technologies and the increasing importance of information in contemporary society, secure and responsible data management has become necessary. In response to this need, legislatures worldwide have enacted regulations to protect personal data and safeguard the right to privacy. In Brazil, the General Data Protection Law (LGPD), Law No. 13,709 of August 14, 2018, regulates this matter. Small-scale data processing agents, such as data controllers and personal data processors, may face compliance challenges with the LGPD due to their size, requiring intervention from the National Data Protection Authority (ANPD) to make regulatory adjustments. Healthcare companies, in particular, should prioritize compliance with the LGPD due to the sensitive nature of the health data they continuously handle. This study aims to evaluate the implementation of the LGPD in dental clinics in the Federal District and Bahia, Brazil. It is a descriptive research with a qualitative approach. Data collection involved interviews with 10 dentists. Categories of adequacy were identified, including knowledge of the LGPD, information security policies, internal awareness and training, access control, security and storage of personal data, and specificities of daily routines in dental clinics. The analysis revealed that, despite the nature of the field, there is limited knowledge about the LGPD among professionals, highlighting unfamiliarity with this legislation. The results are relevant for both dental professionals and the authorities responsible for enforcing the law in the country.

Keywords: General Data Protection Law; Personal Data Privacy; Data Processing Agents; Dental Clinics.

Recebido em 15/02/2024. Aprovado em 18/06/2024. Avaliado pelo sistema *double blind peer review*. Publicado conforme normas da ABNT.
<https://doi.org/10.22279/navus.v14.1869>

1 INTRODUÇÃO

Atualmente, a sociedade está imersa na era da Transformação Digital, marcada pelo avanço das Tecnologias da Informação e Comunicação (TIC), impulsionando a Era dos Dados e da Informação. Esse contexto, permeado pelo crescente uso de plataformas digitais, eleva a relevância das informações, refletindo no progresso tecnológico, crescimento de bancos de dados e no aprimoramento da qualidade, produtividade e redução de custos, contribuindo para a economia e o cotidiano da sociedade contemporânea (de Souza; Alvares; Nunes, 2022).

Nesse cenário, o correto gerenciamento dos dados torna-se relevante para a segurança e responsabilidade no tratamento das informações. As inovações em TIC têm agilizado o processamento e armazenamento dos dados, demandando das empresas a busca por melhores alternativas para viabilizar essa gestão (Juarez; Alves; Nunes; de Oliveira, 2022).

A Segurança da Informação emerge como um atributo na proteção dos dados pessoais, englobando medidas para defender as informações processadas em sistemas (eletrônicos ou físicos) contra acessos não autorizados, manipulações, interrupções ou destruições. O modelo mais difundido para orientar a gestão da segurança da informação é a tríade CID: confidencialidade, integridade e disponibilidade da informação (União Européia, 2016).

Com o aumento dos fluxos de informação resultantes do avanço tecnológico, surgem novos desafios quanto ao armazenamento, uso e manipulação de dados pessoais, impactando diretamente no direito à privacidade. O uso indevido desses dados implica riscos à privacidade e à personalidade dos indivíduos na sociedade da informação (Finelstein; Finkelstein, 2019).

No Brasil o direito à privacidade, com previsão constitucional e respaldado pelo Código Civil, assegura a inviolabilidade da intimidade, vida privada, honra e imagem das pessoas. Esse direito ganha relevância em face da proteção dos dados pessoais, sendo a Lei Geral de Proteção de Dados (LGPD) no Brasil um marco para tutelar a personalidade do indivíduo frente aos riscos do tratamento de dados (Brasil, 2023).

Segundo Mendes (2014), a proteção de dados pessoais emerge na sociedade da informação para salvaguardar a personalidade do indivíduo frente aos potenciais riscos do tratamento desses dados. O objetivo dessa legislação é garantir que o indivíduo saiba quem detém seus dados, quais informações estão em posse e como estão sendo utilizadas, preservando sua privacidade (Nakamura; Formigoni; Ide, 2020).

A LGPD, em vigor no Brasil desde setembro de 2020, busca proteger direitos fundamentais, como liberdade, privacidade e livre desenvolvimento da personalidade ao regulamentar o tratamento de dados pessoais, tanto em meios físicos quanto digitais. Agentes que lidam com grandes volumes de informações são obrigados a se adequar aos termos dessa legislação. Para os de pequeno porte, a Resolução CD/ANPD nº 2, de 27 janeiro de 2022, flexibilizou as medidas, levando em conta suas limitações (Brasil, 2022). Em clínicas médicas e odontológicas, representantes do setor de saúde entre as empresas menores, a privacidade dos pacientes é muito importante.

Apesar da aparente distância entre a área odontológica e a gestão de dados, as clínicas possuem dados pessoais de pacientes e funcionários, justificando a importância de seguir a LGPD. Isso não apenas assegura os direitos dos titulares, mas também preserva questões éticas e evita possíveis implicações legais decorrentes da proteção de dados.

Este estudo se distingue de outras pesquisas devido ao seu foco no setor odontológico, que não é frequentemente abordado em avaliações semelhantes. Isso proporciona uma perspectiva para apoiar profissionais, proprietários de clínicas odontológicas e outros interessados no tema.

O artigo está organizado da seguinte forma: além desta introdução, a seção 2 apresenta o referencial teórico, a seção 3 aborda a metodologia adotada neste estudo, a seção 4 exibe os resultados e a seção 5 mostra as conclusões e as recomendações da pesquisa.

2 Referencial Teórico

2.1. Dado, Informação e Conhecimento

Os termos dado, informação e conhecimento, embora conectados, não são semanticamente idênticos, conforme delineado por Correia (2009). Os dados são registros ou indícios vinculados a um objeto, conferindo-lhes um valor, seja quantitativo ou qualitativo. As informações, por sua vez, resultam da organização e agrupamento dos dados, gerando significado. O conhecimento surge quando a informação é compreendida, internalizada como verdadeira e armazenada para uso futuro. Assim, a informação, contextualizada, adquire valor social, especialmente para organizações, ao auxiliá-las em decisões estratégicas. Essa interpretação das informações resulta na geração de conhecimento, conforme a perspectiva de Lyra (2015).

2.2. Segurança da Informação

Os avanços na Tecnologia da Informação permitem o processamento e armazenamento ágeis, exigindo que empresas busquem soluções eficazes (Juarez; Alves; Nunes; De Oliveira, 2022). Ter informações de terceiros pode representar riscos à privacidade, tornando a Segurança da Informação essencial para proteger dados pessoais (Associação Brasileira de Normas Técnicas [ABNT], 2013). A área de segurança da informação busca defender informações contra várias ameaças, eletrônicas ou físicas, preservando a confidencialidade, integridade e disponibilidade dos dados (União Européia, 2016).

Mattord e Whitman (2012) explicam que a Segurança da Informação se baseia na proteção dos ativos informacionais, assegurando a confidencialidade, integridade e disponibilidade por meio de estratégias, tecnologia e educação. A confidencialidade, definida pela Norma Associação Brasileira de Normas Técnicas (2022), restringe informações a indivíduos autorizados (ABNT, 2016), visando evitar violações e proteger a privacidade (Caiçara, 2007). Estratégias como classificação de dados e criptografia são empregadas para resguardar a confidencialidade.

A Integridade, segundo a Associação Brasileira de Normas Técnicas (2022), refere-se à precisão e completude. Mattord e Whitman (2012) descrevem como a qualidade de ser inteiro e não corrompido. Para preservar a integridade das informações, são usados métodos de detecção de falhas nos sistemas de arquivos após ataques de vírus.

A Disponibilidade, definida pela Associação Brasileira de Normas Técnicas (2016), possibilita o acesso à informação por uma entidade autorizada. Samonas e Coss (2014) a descrevem como a característica da informação que permite acesso sem obstruções. Enquanto a Integridade e a Confidencialidade necessitam de proteção, a Disponibilidade garante acesso a usuários autorizados.

Os princípios da Segurança da Informação (SI) buscam proteger dados contra acessos não autorizados, garantir a disponibilidade e preservar a integridade (Piurcosky; Costa; Frogeri; Calegario, 2019). A evolução tecnológica tornou a proteção de dados um desafio significativo para várias entidades (Viana da Silva; Scherf; Silva, 2020). A segurança cibernética, segundo Trinks, Albuquerque, Nunes e Mota (2022), protege sistemas de informação, dados e serviços contra acessos não autorizados ou uso indevido, intencional ou acidental.

2.3. Lei Geral de Proteção de Dados

A LGPD, Lei nº 13.709 de 2018, aborda o tratamento de dados pessoais, em meio físico ou digital, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e desenvolvimento pessoal previstos na Constituição Federal de 1988. Essa legislação atua como complemento às proteções já estabelecidas pela Lei Nº 8.078, de 11 de setembro de 1990 conhecida como Código de Defesa do Consumidor e pelo Marco Civil da Internet (Lei nº 12.965/2014).

Além disso, a LGPD estabeleceu a Autoridade Nacional de Proteção de Dados (ANPD) para regular a coleta, uso, processamento e compartilhamento de dados no país. A ANPD é responsável por receber denúncias e reclamações dos cidadãos e fiscalizar o cumprimento das normas da LGPD, aplicando sanções quando necessário (Brasil, 2018). Compreender os conceitos fundamentais presentes na legislação é crucial para sua aplicação efetiva.

Antes da implementação da LGPD no Brasil, a proteção de dados era abordada de maneira indireta em várias legislações, incluindo o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet (Lei nº 12.965/2014). No entanto, uma regulamentação específica para a proteção de dados só foi estabelecida anos mais tarde. Isso ocorreu após a proteção de dados ser reconhecida como um direito fundamental.

O tratamento de dados, conforme definido pela LGPD, abarca operações diversas com informações pessoais. Essas operações incluem desde a coleta até a eliminação, modificação e transferência dos dados, entre outras ações (Brasil, 2018).

Os princípios fundamentais da LGPD estabelecem diretrizes essenciais para o manuseio ético e legal de dados pessoais. O princípio da finalidade requer que o processamento dos dados seja transparente, específico e comunicado ao titular, sem uso posterior incompatível. Da mesma forma, o princípio da adequação demanda que o tratamento seja compatível com os propósitos divulgados e coerentes com a finalidade original. Nesse interim, o princípio da necessidade reforça a coleta restrita e proporcional, limitando-a ao mínimo necessário para atingir a finalidade inicial (Brasil, 2018).

A LGPD enfatiza ainda a importância do princípio do livre acesso, garantindo aos titulares o acesso gratuito e facilitado aos seus dados em tratamento. O princípio da qualidade dos dados destaca a necessidade de precisão, atualização e correção dos dados para atender às finalidades do tratamento. A transparência requer informações claras e acessíveis sobre o tratamento dos dados, incluindo os agentes envolvidos, respeitando segredos comerciais e industriais (Brasil, 2018).

Além disso, a segurança exige medidas técnicas e administrativas para proteger os dados contra acesso não autorizado, manipulação ilícita ou perda. O princípio da prevenção orienta ações para antecipar danos decorrentes do tratamento dos dados. A não discriminação proíbe o uso discriminatório,

ilícito ou abusivo dos dados, evitando prejuízos aos titulares. Por fim, o princípio da responsabilização e prestação de contas requer a demonstração de medidas eficazes adotadas pelos agentes de tratamento para cumprir as normas de proteção de dados (Brasil, 2018).

2.3.1 Tratamento de Dados Pessoais em Clínicas Odontológicas

No contexto brasileiro, o setor da saúde está entre os mais regulamentados, evidenciando-se na área odontológica através do Código de Ética Odontológica, previsto na Resolução do Conselho Federal de Odontologia (CFO) nº 118, de 11 de maio de 2012. Este documento estabelece os direitos e deveres dos profissionais, especialmente do cirurgião-dentista (Conselho Federal de Odontologia, 2012). O artigo 2º desse código enfatiza a prática da Odontologia em prol da saúde humana, coletiva e do meio ambiente, sem discriminação, reconhecendo que alguns dados tratados em clínicas odontológicas são sensíveis e demandam um cuidado especial (Mittlestadt; Floridi, 2016).

Embora não se associe imediatamente a área odontológica a bancos de dados, clínicas detêm diversos tipos de informações pessoais de pacientes e funcionários, incluindo dados sensíveis, como histórico de saúde geral e bucal. É relevante ressaltar que, de acordo com Favaretto *et al.* (2020), considerar os dados de saúde bucal menos sensíveis que outras categorias podem resultar em negligência ética. Hoffman (2009) destaca que esses dados podem ser usados de forma discriminatória, assim como dados relacionados à condição econômica dos pacientes (Peppet, 2014).

Esses dados coletados em clínicas odontológicas podem ser usados tanto para fins clínicos quanto secundários, como pesquisas ou estratégias de marketing (Favaretto; Shaw; De Clercq; Joda; Elger, 2020). O Código de Ética Odontológica já estabelecia regras sobre a coleta e guarda dessas informações, determinando deveres fundamentais dos inscritos, como resguardar o sigilo profissional, manter prontuários atualizados e proteger a privacidade do paciente (Conselho Federal de Odontologia, 2012).

Os prontuários dos pacientes são considerados documentos altamente sensíveis, concentrando informações desde fichas clínicas até dados complementares, como exames e registros de tratamento (Oliveira; Yarid, 2014). Com a transição para o meio digital, o estudo de Favaretto *et al.* (2020) ressalta preocupações éticas relacionadas à privacidade e confidencialidade dos dados, especialmente em prontuários digitais. O acesso não autorizado a esses dados e informações pode violar a privacidade dos pacientes (Cederberg; Walji; Valenza, 2014).

A LGPD estabeleceu normas específicas para a digitalização e utilização de sistemas informatizados para prontuários de pacientes, complementando legislações preexistentes. O cirurgião-dentista é reconhecido como o controlador dos dados, sendo responsável pelas decisões relativas ao tratamento de dados pessoais, enquanto as empresas responsáveis pela gestão dos sistemas são consideradas operadoras, realizando o tratamento de dados em nome do controlador, conforme estipulado pela LGPD. A legislação garante aos titulares dos dados uma série de direitos, incluindo acesso, correção, anonimização e exclusão das informações (Franco, 2021).

A adequação das clínicas odontológicas à LGPD não apenas protege os direitos fundamentais dos titulares dos dados, mas também resguarda a ética profissional e evita implicações legais. O cuidado com a confidencialidade e a segurança dos dados é fundamental para a integridade da prática

odontológica, considerando a sensibilidade das informações manipuladas (Franco, 2021).

3 Metodologia

Trata-se de uma pesquisa descritiva e exploratória. O trabalho possui características exploratórias, já que seu principal objetivo é aprimorar ideias ou descobrir intuições, o que requer um planejamento flexível capaz de considerar vários aspectos relacionados ao fato estudado (Gil, 2009). Ele é descritivo pois "consiste em investigações de pesquisa empírica cuja principal finalidade é o delineamento ou análise das características de fatos ou fenômenos, a avaliação de programas, ou o isolamento de variáveis principais ou chave" (Marconi; Lakatos, 2003, p. 187).

O estudo adotou uma abordagem predominantemente qualitativa, já que buscou compreender e explorar "universos de significados, motivos, aspirações, crenças, valores e atitudes", ou seja, um espaço mais profundo de relações e fenômenos que não podem ser mensurados apenas pela operacionalização de variáveis (Minayo, 2002, p. 21).

Neste presente estudo a coleta de dados abrangeu dez entrevistas semiestruturadas com cirurgiões-dentistas, visando explorar suas percepções sobre o impacto da LGPD no contexto da área, bem como abordar questões relativas à aplicabilidade dessa legislação no cotidiano de consultórios odontológicos. A seleção dos participantes considerou a necessidade de entrevistar profissionais que detivessem experiências relevantes relacionadas à rotina e à gestão de consultórios e clínicas odontológicas, possibilitando a coleta de informações pertinentes.

As entrevistas semiestruturadas são caracterizadas pela ausência de uma estrutura inflexível, proporcionando um diálogo flexível que permite ao entrevistado expressar livremente suas opiniões sobre o tema em análise (Silverman, 2011). Além disso, conferem ao entrevistador a flexibilidade para explorar a ordem, a profundidade e a apresentação das questões de acordo com as respostas e circunstâncias específicas do entrevistado (Barros; Duarte, 2011).

Ao selecionar os entrevistados, foram estabelecidos critérios mínimos, exigindo que fossem profissionais atuantes na área de cirurgia-dentária em consultórios ou clínicas odontológicas. Estudantes ainda não graduados e profissionais aposentados foram excluídos. Adicionalmente, a amostra de entrevistados foi diversificada, incluindo empreendedores, proprietários de clínicas, profissionais autônomos e aqueles que desempenham suas atividades em clínicas de terceiros.

Dado que a maior parte dos tópicos abordados na pesquisa está relacionada a dados de gerenciamento e particularidades profissionais individuais dos entrevistados, optou-se por segmentar as respostas de maneira anônima. Para tal, foi empregada uma numeração de 1 a 10 para identificação de cada entrevistado, utilizando-se também siglas, como por exemplo, E01, E02, e assim por diante.

A relação completa dos entrevistados, juntamente com informações sobre a função profissional, porte da clínica em que atuam e estado de residência, encontra-se detalhada no Quadro 1.

Quadro 1 - Relação de Entrevistados

Entrevistado	Porte da Clínica	Função	UF
--------------	------------------	--------	----

E01	Microempresa	Proprietário	DF
E02	Autônomo (Pessoa física)	Autônomo	DF
E03	Empresa de pequeno porte	Contratado	DF
E04	Autônomo (Pessoa física)	Autônomo	DF
E05	Microempresa	Proprietário	DF
E06	Autônomo (Pessoa física)	Autônomo	DF
E07	Microempresa	Contratado	DF
E08	Microempresa	Contratado	BA
E09	Autônomo (Pessoa física)	Autônomo	BA
E10	Microempresa	Contratado	BA

Fonte: Dados das entrevistas.

O protocolo de entrevista compreendia um conjunto de 22 questões, cuja adaptação durante o curso das entrevistas era contingente à evolução das respostas individuais de cada entrevistado. Tal abordagem permitia a personalização do diálogo, viabilizando a investigação aprofundada e a compreensão de temáticas específicas relacionadas a cada participante.

Realizou-se a análise dos resultados por meio do Método de Análise de Conteúdo proposto por Bardin (2016), uma metodologia para a análise de dados qualitativos que se desdobra em três fases principais: (i) Pré-análise, em que o pesquisador estabelece os objetivos do estudo e seleciona o corpus a ser examinado; (ii) Exploração do material, Categorização ou Codificação, momento em que o pesquisador realiza uma leitura não sistemática do conteúdo para adquirir uma compreensão global; e (iii) Tratamento dos resultados, Inferências e Interpretação, fase em que o pesquisador examina os dados coletados e elabora as conclusões do estudo.

As respostas dos entrevistados foram organizadas, de acordo com cada grupo temático pré-estabelecido, facilitando a posterior análise de cada categoria individualmente e facilitando a visualização para posteriormente serem analisados os padrões das informações coletadas e a comparação das respostas obtidas.

Foram utilizadas como base 6 categorias definidas para a realização da análise de conteúdo da pesquisa, sendo consolidadas, juntamente com suas respectivas definições, no Quadro 2, nos termos apresentados no 'Guia Orientativo sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte', disponibilizado pela ANPD (Brasil, 2021) e no documento disponibilizado pela ENISA, 'Diretrizes para Pequenas e Microempresas sobre o Segurança de Dados Pessoais em Processamento' (Enisa, 2016).

Quadro 2 - Categorias de Análise de Conteúdo da Pesquisa

Categoria	Descrição
1. Conhecimento da LGPD	Análise do nível de conhecimento e aplicação da lei.
2. Políticas de Segurança da Informação	A política de segurança da informação - PSI, consiste em um conjunto de diretrizes e regras que tem por objetivo possibilitar planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização.
3. Conscientização e Treinamento interno	Essa conscientização implica informar e sensibilizar todos os funcionários da organização, especialmente aqueles diretamente envolvidos na atividade de tratamento de dados, sobre as obrigações legais existentes na LGPD e em normas e orientações editadas pela ANPD.
4. Controle de Acesso	O controle de acesso consiste em uma medida técnica para garantir que os dados sejam acessados somente por pessoas autorizadas. Ele consiste em processos de autenticação, autorização e auditoria. <ul style="list-style-type: none"> • A autenticação identifica quem acessa o sistema ou os dados; • a autorização determina o que o usuário identificado pode fazer; • a auditoria registra o que foi feito pelo usuário.
5. Segurança de Dados Pessoais e Armazenamento	Esta categoria de medidas está principalmente relacionada ao processamento de dados pessoais em bancos de dados ou outros sistemas relevantes (incluindo armazenamento em nuvem). Refere-se também ao tratamento de dados pessoais por colaboradores com recurso a estações de trabalho específicas ou outros dispositivos.
6. Especificações do cotidiano em clínicas odontológicas	Pontos de aplicação das diretrizes da lei direcionadas ao cotidiano de uma clínica odontológica.

Fonte: adaptado de Brasil, 2021; Enisa, 2016

4 Resultados e Discussões

Buscando compreender as principais percepções e aspectos relativos às categorias pré-definidas neste trabalho, serão analisadas, de forma individual, cada uma delas, observando sua base teórica em correlação com a aplicação no cotidiano, através da análise das informações coletadas nas entrevistas realizadas com os profissionais atuantes da área odontológica.

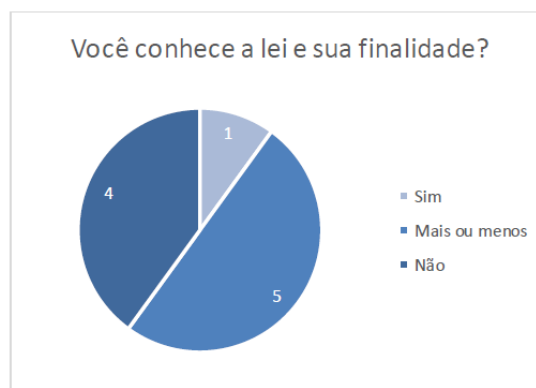
4.1 Conhecimento da LGPD

A primeira categoria estudada na análise das entrevistas foi quanto ao conhecimento da Lei Geral de Proteção de Dados no meio odontológico. Neste contexto, buscava-se aferir o nível de conhecimento e aplicação desta lei nas respectivas clínicas em que trabalhavam os entrevistados.

4.1.1 Conhecimento Geral

Observou-se, à princípio que a grande maioria dos entrevistados detinha nenhum ou pouco conhecimento quanto a lei e sua finalidade, conforme demonstrado na Figura 1.

Figura 1 - Gráfico de conhecimento pelos entrevistados da LGPD



Fonte: O autor

As respostas neste tópico se mostraram mais objetivas e, de modo geral, demonstraram um conhecimento superficial da lei por parte dos entrevistados. No mesmo sentido, quando questionados sobre às consequências da inobservância da lei, os entrevistados E01, E03, E04, E06, E08 e E10 responderam objetivamente que desconheciam, enquanto os demais (E02, E05, E07 e E09) alegaram entender que as consequências da inobservância da lei teriam um caráter punitivo.

Conforme apontado por Ganut (2021), a adequação à LGPD não é prioridade para pequenas empresas, sendo o ritmo do processo de conformidade com a lei diretamente relacionado com o tamanho da empresa, visto que são necessários o investimento em recursos com pessoal, tecnologia e compliance.

Quando questionados acerca da Resolução nº 2 da ANPD, que confere aos micro e pequenos empresários e, agentes de tratamento de dados, condições especiais na adequação da LGPD, foi unânime a resposta no sentido de desconhecimento total desta resolução, mesmo quando explicado aos entrevistados sobre do que ela tratava.

4.1.2 Nível de conformidade com a LGPD

Em relação ao nível de conformidade das clínicas onde os entrevistados exercem suas atividades, nota-se que, em sua maioria, os profissionais expressam a falta de conformidade com a legislação ou indicam não estar devidamente adaptados a ela, principalmente por desconhecerem os termos legais.

Os entrevistados revelaram várias razões para o conhecimento limitado sobre a LGPD na área odontológica. Entre elas, mencionaram desafios na compreensão integral da lei, falta de interesse, negligência e a percepção de inovação da lei em relação à digitalização na odontologia, associada a uma confiança excessiva em softwares.

Um das principais razões mencionadas para justificar a dificuldades de adequação e difusão da lei por parte dos dentistas foi a utilização de

prontuários físicos (em papel) e utilização limitada de softwares e tecnologia nos respectivos consultórios.

O prontuário, seja ele físico ou digital, é constituído do mesmo formato, e é o documento mais importante para o registro da assistência prestada ao paciente (Telles; Maruco; Silva, 2021). De acordo com Rodrigues (2021) o prontuário é um documento constituído por um conjunto de informações, sinais e imagens registradas, geradas a partir de fatos sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a continuidade da assistência prestada ao indivíduo.

Contudo, essa compreensão inadequada é evidenciada entre os profissionais da área odontológica no que se refere ao alcance da LGPD, a qual deve ser aplicada em todos os contextos de tratamento de dados pessoais, não se limitando apenas aos dados virtuais.

Entre as razões apontadas pelos entrevistados, destaca-se a ausência de inclusão desse tema nos programas educacionais voltados aos profissionais da área, principalmente durante a formação universitária e nos cursos de pós-graduação e especialização. Essa lacuna foi mencionada pelos entrevistados como uma das principais questões.

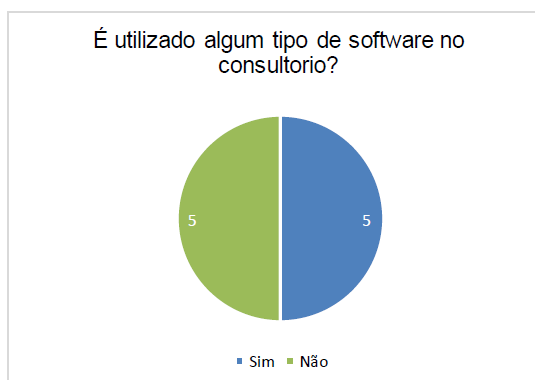
4.2 POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Nesta categoria, examina-se a presença e efetividade das Políticas de Segurança da Informação (PSI), isto é, a verificação da existência de diretrizes ativas nas clínicas que permitam o planejamento, a execução e o monitoramento de ações vinculadas à segurança da informação.

4.2.1 Utilização de Softwares

Embora os serviços odontológicos tradicionais sejam realizados presencialmente, a presença crescente de softwares para a gestão de consultórios tem incentivado parte dos dentistas a migrar para o meio digital. Isso é notável na adoção de prontuários digitais, onde cerca de metade dos entrevistados utiliza softwares em seus consultórios, como mostra a Figura 2.

Figura 2 - Utilização de softwares pelos entrevistados



Fonte: O autor

É relevante notar que uma parcela dos entrevistados está no estágio inicial do processo de digitalização de suas clínicas, apontando benefícios na organização dos registros dos pacientes. Entretanto, eles também mencionam dificuldades na adaptação das clínicas aos softwares disponíveis, muitas vezes utilizados de maneira básica, limitando-se ao armazenamento dos dados

obtidos durante a consulta. Outros tipos de informações, como os dados pessoais contendo CPF, endereço, entre outros, permanecem armazenados em locais distintos.

Cabe destacar que, segundo a LGPD, mesmo quando uma atividade de tratamento de dados seja executada por prestador de serviço, como é o caso de empresas de softwares, o dentista que requisita as informações de seus pacientes é responsável pelo tratamento de dados, e em caso de irregularidades responderá da mesma forma ao ocorrido (Atheniense, 2019).

Contudo, ao examinar os entrevistados que declararam não utilizar software em suas clínicas, identificaram-se predominantemente dois perfis: profissionais autônomos ou que atuam em clínicas de pequeno porte, e profissionais com uma trajetória consolidada ao longo de vários anos, os quais enfrentam dificuldades ou não veem necessidade na digitalização integral de seus consultórios.

A relação de entrevistados e seus respectivos portes e forma de utilização de prontuários pode ser observado no Quadro 3.

Quadro 3 - Relação Entrevistado x Porte x Tipo de Prontuário

Entrevistado	Porte da Clínica	Tipo Prontuário
E01	Microempresa	Digital
E02	Autônomo (Pessoa física)	Físico
E03	Empresa de pequeno porte	Ambos
E04	Autônomo (Pessoa física)	Físico
E05	Microempresa	Físico
E06	Autônomo (Pessoa física)	Físico
E07	Microempresa	Digital
E08	Microempresa	Digital
E09	Autônomo (Pessoa física)	Ambos
E10	Microempresa	Físico

Fonte: O Autor

4.2.2 Tratamento de Dados

A ausência de um responsável designado para o tratamento de dados nas clínicas foi observada através da análise das entrevistas realizadas. Entre os 10 entrevistados, apenas um (E03) indicou possuir um responsável pelo tratamento de dados na clínica, desempenhando simultaneamente funções administrativas e financeiras.

Os demais entrevistados comumente relataram que o tratamento de dados era uma responsabilidade partilhada por todos os profissionais envolvidos na

operação da clínica, não sendo atribuída a uma pessoa específica. Em clínicas menores, a responsabilidade pelo tratamento de dados tendia a ser compartilhada entre o proprietário e um profissional de secretariado.

Conforme tratado por Telles *et al.* (2021), para se cumprir as exigências da LGPD, deve existir uma pessoa ou empresa responsável pelas informações coletadas dos pacientes e pelo tratamento dos dados, tanto obtidos em meio físico, como digital.

No que concerne ao registro das ações efetuadas com os dados pessoais nas clínicas, observou-se que, geralmente, ocorre o registro do tratamento dos dados, especialmente em clínicas digitalizadas, onde softwares específicos ou sistemas computacionais automatizam o registro.

Em outros casos, verificou-se que as anotações são comumente realizadas manualmente em fichas clínicas e prontuários dos pacientes, além da utilização de agendas. Nestes contextos, quando há inclusão de nova informação, é comum haver um controle dos registros, como a data de inserção daquela informação.

De modo geral, na área da saúde, nos prontuários em papel, é obrigatória a legibilidade da letra do profissional que atendeu o paciente (Conselho Federal de Medicina, 2002). Deve-se atentar também ao excesso de abreviações, siglas e sinais impróprios, que podem dificultar a compreensão do documento, ou siglas restritas às especialidades e aquelas com várias interpretações (Garritano *et al.*, 2020).

Outro aspecto relevante referente ao registro das manipulações de exames e radiografias sob posse da clínica foi mencionado por um dos entrevistados (E06), exemplificando uma das práticas de tratamento de dados pessoais.

4.3 Conscientização e Treinamento Interno

Durante as entrevistas, o tema do treinamento dos funcionários sobre a confidencialidade dos dados dos pacientes e suas responsabilidades no tratamento dessas informações foi abordado. É essencial informar e sensibilizar os funcionários, especialmente os envolvidos diretamente no manejo de dados, sobre as obrigações legais da LGPD e as diretrizes da ANPD.

Embora a maioria dos entrevistados tenha mencionado a preocupação em conscientizar os funcionários, apenas o Entrevistado 03 destacou a implementação formal de um treinamento sobre proteção de dados e LGPD. Os dentistas demonstram essa preocupação fundamentada no Código de Ética Odontológica, estabelecido pela Resolução CFO 118, de 11 de maio de 2012, que regula os direitos e deveres dos cirurgiões-dentistas.

Em seu art. 2º, o Código de Ética Odontológica descreve a profissão como, "A Odontologia é uma profissão que se exerce em benefício da saúde do ser humano, da coletividade e do meio ambiente, sem discriminação de qualquer forma ou pretexto". Desse modo, por se tratar de uma profissão da área da saúde, alguns dos dados tratados em uma clínica odontológica podem ser classificados como sensíveis, necessitando um tratamento especial e mais cuidadoso do que uma empresa que não trata com essa modalidade de dados (Mittlestadt; Floridi, 2016).

A Lei Geral de Proteção de Dados vem ao encontro do dever de sigilo do paciente presente na área da saúde e desta forma corrobora a importância e a necessidade da preservação dos dados pessoais dos pacientes em instituições de saúde (Telles; Maruco; Silva, 2021).

Com base nas evidências das entrevistas, foi possível observar que os dentistas, apesar do desconhecimento detalhado da LGPD, tendem a se alinhar, de certa forma, com os termos da lei, devido à atenção dedicada à privacidade

dos dados dos pacientes, conforme destacado no código de ética profissional da área.

4.4 Controle de Acesso

O controle de acesso visa garantir que os dados sejam acessados apenas por indivíduos autorizados, utilizando processos de autenticação, autorização e auditoria. A autenticação identifica quem está acessando o sistema ou dados; a autorização define as permissões concedidas ao usuário autenticado; e a auditoria registra as ações executadas pelo usuário durante o acesso (BRASIL, 2021).

As respostas dos entrevistados apontaram para uma limitação no controle do acesso dos funcionários aos dados da clínica. Nas clínicas avaliadas, não há uma distinção clara entre dados sensíveis e não sensíveis. Todos estão contidos no mesmo documento e o prontuário, acessível a todos os funcionários. No entanto, há restrições na capacidade de edição dos dados sensíveis, reservada a certos profissionais, como os dentistas responsáveis pelo atendimento, enquanto outros funcionários, como as secretárias, têm acesso ao prontuário, mas não permissão para modificá-lo.

Os dados de saúde mantidos por uma clínica odontológica são considerados altamente sensíveis, dado o potencial discriminatório de seu uso (Hoffman, 2009). Essa sensibilidade é especialmente enfatizada quando se trata de informações relacionadas a menores de idade. Um dos entrevistados (E08) destacou a necessidade de manter em sigilo dados sensíveis de menores, justificando a exclusão da anamnese da ficha inicial do paciente.

De fato, dados pertinentes a menores devem ser tratados com especial cuidado, como enfatizado por Atheniense (2019), que ressalta a obrigação de prestação de informações relacionadas a menores por meio de seus representantes legais, responsáveis pelo consentimento explícito.

4.5 Segurança e Armazenamento de Dados Pessoais

Essa categoria de medidas está associada ao processamento de dados pessoais em bancos de dados ou sistemas, incluindo armazenamento em serviços de nuvem. Também abrange o tratamento de dados por colaboradores através de dispositivos como smartphones. A LGPD se aplica a qualquer entidade que colete dados. Caso haja armazenamento inadequado levando a vazamentos ou problemas, a responsabilidade recai sobre o profissional, clínica ou hospital responsável pelos dados (Atheniense, 2019).

Com relação à duração do armazenamento dos dados pessoais, foram coletadas respostas que foram organizadas na Tabela 1.

Tabela 1 - Relação Tempo de armazenamento de dados x Quantidade

Tempo de armazenamento dos dados pessoais	Quantidade
Não descarta	02
2 anos	02
10 anos	04
20 anos	02

Fonte: Dados da Entrevista.

Observa-se, pelas respostas dos entrevistados, que não há um consenso em relação ao período de armazenamento dos prontuários odontológicos. Isso decorre da existência de três fontes diversas de informação. A primeira (20

anos) deriva da Lei 13.787/18, que regula a digitalização, uso de sistemas informatizados para armazenar e gerenciar prontuários de pacientes.

O Conselho Federal de Odontologia (CFO), no parecer nº 125/92, também aborda essa temática, estipulando que a posse do prontuário pertence ao paciente, sendo a sua custódia responsabilidade do profissional, e deve ser arquivado por, no mínimo, 10 anos após a última consulta do paciente.

Por fim, o Código de Defesa do Consumidor (CDC), em seu artigo 27, estabelece um prazo de prescrição de 5 anos para qualquer reivindicação de reparação de danos decorrentes de produtos ou serviços, com a contagem do prazo a partir do conhecimento do dano e sua autoria (Saraiva, 2011).

4.6 Especificações do Cotidiano em Clínicas Odontológicas

Nesta categoria, são examinados os aspectos práticos e a aplicação das diretrizes legais no contexto operacional diário de uma clínica odontológica.

4.6.1 Política de Privacidade

Com a implementação da LGPD, empresas e organizações precisam criar ou ajustar suas políticas de privacidade para abordar o tratamento de dados pessoais dos clientes. Essas políticas devem incluir procedimentos, tipos e métodos de coleta, justificativas, além de esclarecer a finalidade da coleta. Também devem especificar se os dados serão compartilhados com terceiros, respeitando a autonomia do titular quanto ao compartilhamento de suas informações (Siebra; Xavier, 2020).

Diante disso, questionou-se aos entrevistados se, antes do paciente se vincular à clínica ou agendar uma consulta, eles são informados sobre a Política de Privacidade adotada na clínica. As respostas indicaram a existência de um termo de consentimento assinado pelos pacientes, autorizando o uso dos dados contidos no cadastro das informações pessoais e do prontuário, efetuado no momento da assinatura do contrato.

Outro momento ressaltado pelos entrevistados, no qual se solicita a permissão dos pacientes para a utilização de dados, refere-se à obtenção de consentimento para o uso de imagens, seja com propósito acadêmico ou para divulgação em plataformas de redes sociais.

Conforme delineado por Vanrell (2002), os registros odontológicos constituem um conjunto de registros formalizados pelo profissional e paciente no contexto clínico, tendo a potencialidade de servir como evidência em contextos jurídicos. O prontuário engloba informações como anamnese, consentimento informado, progressão do tratamento, registros fotográficos e radiográficos do paciente, bem como cópias de prescrições e atestados.

4.6.2 Uso dos dados pessoais para objetivos diversos

Os dados obtidos em clínicas odontológicas podem ser empregados com propósitos primários, contribuindo diretamente ao longo do tratamento, ou para propósitos secundários, como pesquisas ou outras finalidades, como estratégias de marketing ou fins acadêmicos (Favaretto; Shaw; De Clercq; Joda; Elger, 2020).

Alguns entrevistados indicaram o uso dos dados pessoais dos pacientes com fins comerciais e de marketing, visando a atração e reconquista de clientes anteriores. Outros mencionaram a utilização dos dados dos pacientes para propósitos acadêmicos, especialmente por entrevistados que ocupam cargos de professores ou estão envolvidos em programas de mestrado.

4.6.3 Prontuários

Conforme destacado por Telles *et al.* (2021), o prontuário médico é um registro elaborado pelo profissional de saúde, destinado a abarcar de maneira integral todas as informações pertinentes ao paciente. Dentro deste registro, os elementos obrigatórios incluem a identificação do paciente, anamnese, exame físico, hipóteses diagnósticas, diagnóstico definitivo e detalhamento do tratamento realizado. É imperativo que todas as informações sejam expostas de maneira concisa e estruturada.

Nesse contexto, foi indagado aos entrevistados quais dados eram registrados nos prontuários de suas respectivas clínicas. As respostas apresentadas por todos os entrevistados mantiveram um padrão, evidenciando a inclusão de informações cadastrais, histórico médico, dados abarcando a saúde bucal e geral do paciente, bem como os procedimentos realizados na clínica. Ademais às informações relacionadas à identificação e estado de saúde do paciente, alguns entrevistados também referiram a inclusão de registros referentes a pagamentos nos prontuários.

4.6.4 Utilização de dispositivo móveis e redes sociais

Um aspecto relevante na transformação digital dos consultórios é a utilização de aplicativos de mensagens, como o WhatsApp, por profissionais da saúde. Segundo Atheniense (2019), o envio inadvertido de informações clínicas sensíveis a terceiros, sem consentimento prévio ou medidas de proteção, é considerado ilegal. Em situações de clonagem de contas, eventuais vazamentos também são de responsabilidade do profissional ou da clínica, pois são considerados controladores dos dados pessoais dos pacientes, o que implica responsabilidade legal por falhas de segurança dos aplicativos e riscos de penalidades (Atheniense, 2019).

Os entrevistados indicaram principalmente o uso do WhatsApp em clínicas e por dentistas para agendamentos, questões administrativas e comunicação direta com pacientes após procedimentos. Durante a pandemia de Covid-19, o Conselho Federal de Odontologia estabeleceu modalidades de teleodontologia, como telemonitoramento entre consultas e teleorientação por cirurgiões-dentistas para identificar o momento adequado para atendimento presencial, registrando todas as ações no prontuário (Conselho Federal de Odontologia, 2020).

Em relação ao atendimento remoto, parte dos entrevistados mencionou não realizar esse tipo de consulta ou limitar-se a consultas orientativas e de urgência. Por fim, quanto ao uso do Instagram, a maioria dos entrevistados informou não utilizá-lo para fins profissionais. Aqueles que mencionaram utilizar a plataforma o fazem apenas como um meio informativo, como apresentado na Tabela 2.

Tabela 2 - Relação Utilização de Instagram x Quantidade

Utilização de Instagram?	Quantidade
Sim	01
Sim (informativo)	02
Não	07

Fonte: Dados da Entrevista.

5 CONCLUSÃO

Na Sociedade da Informação, a gestão segura de dados é fundamental, especialmente para clínicas odontológicas, que lidam com informações sensíveis de saúde. Este estudo qualitativo exploratório com cirurgiões-dentistas buscou avaliar a implementação da LGPD nessas clínicas.

A maioria dos entrevistados demonstrou conhecimento limitado sobre a LGPD e a Resolução nº 2 da ANPD, revelando lacunas na divulgação das flexibilizações da lei. As limitações no conhecimento na odontologia podem ser atribuídas ao uso persistente de prontuários físicos, à adoção limitada de tecnologia nos consultórios e à falta de abordagem sobre LGPD nos currículos de odontologia.

Foi notado um déficit na designação de um responsável pelo tratamento de dados, desrespeitando as diretrizes da LGPD. Embora haja preocupação com o sigilo dos dados, falta formalização dessas práticas, possivelmente relacionada ao código de ética profissional odontológica.

A pesquisa destacou o uso frequente do WhatsApp e das teleconsultas para agendamentos e orientações, mas revelou a carência de orientações efetivas sobre a LGPD para os profissionais, baseadas no Código de Ética Odontológica, indicando pouca influência da LGPD e desconhecimento sobre suas sanções.

Apesar dos avanços digitais, os profissionais carecem de orientação sobre a aplicação eficaz da LGPD. Os resultados podem aprimorar a proteção dos dados dos pacientes e desenvolver práticas de gestão de dados mais eficazes, contribuindo para a conscientização sobre a LGPD e seus impactos, e auxiliando na identificação de lacunas na aplicação desta legislação.

Este estudo se depara com limitações, abarcando restritamente profissionais da odontologia como público-alvo, limitações no número de entrevistados e a restrição geográfica a determinados estados.

No entanto, vislumbra-se como uma iniciativa futura de aprimoramento a replicação deste trabalho expandindo o escopo da pesquisa para englobar uma amostragem mais abrangente de profissionais, múltiplas funções dentro das clínicas e distintos estados do Brasil.

REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. ISO/IEC 27000. **Informação Tecnológica. Segurança da Informação. Técnicas e metodologias.** São Paulo, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27002: **Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação.** Rio de Janeiro, 2013.

ATHENIENSE, Alexandre. **A LGPD e seus efeitos para a prática médica e gestão de saúde.** Outubro de 2019. Disponível em: <https://l1nq.com/pXEtI>. Acesso em: 25 mar. 2023.

BARDIN, Laurence. **Análise de conteúdo.** Edição revista e ampliada. São Paulo: Edições 70 Brasil; [1977] 2016.

BARROS, Antonio; DUARTE, José. (orgs.). **Métodos e técnicas de pesquisa em Comunicação.** São Paulo: Atlas, 2ª, 2011.

BRASIL. **Checklist de Medidas de Segurança para Agentes de Tratamento de Pequeno Porte.** Agência Nacional de Proteção de Dados (ANPD), Out 2021. Disponível em: Checklist alinhado - vf (www.gov.br). Acesso em: 08 fev. 2023.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília, 2019. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em: 16 jan. 2023.

BRASIL. **Decreto-lei nº 10.406, de 10 de janeiro de 2002**. Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/110406compilada.htm. Acesso em: 16 jan. 2023.

BRASIL. **Guia de Boas Práticas Lei Geral de Proteção de Dados (LGPD)**. Comitê Central de Governança de Dados, 2020 Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-eprotecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 08 fev. 2023.

BRASIL. **Guia do Consumidor: Como Proteger seus Dados Pessoais: Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor, em parceria com a ANPD e a Secretaria Nacional do Consumidor (SENACON), Agência Nacional de Proteção de Dados (ANPD), 2021**. Disponível em: <https://acesse.one/BGOBK>. Acesso em: 04 fev. 2023.

BRASIL. **Guia Orientativo Sobre Segurança da Informação para Agentes de Tratamento de Pequeno Porte. Agência Nacional de proteção de Dados (ANPD), Out 2021**. Disponível em: [guiavf.pdf \(www.gov.br\)](http://www.gov.br). Acesso em: 08 fev. 2023

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados (LGPD). Diário Oficial da União, Brasília, DF, 15 ago. 2018. Seção 1, p. 1. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 04 fev. 2023.

BRASIL. **Lei nº 13.787, de 27 de dezembro de 2018**. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113787.htm. Acesso em: 04 fev. 2023.

BRASIL. **Minuta de Resolução: Aplicação da LGPD para Agentes de Tratamento de Pequeno Porte**. Ago, 2021. Disponível em: <https://acesse.one/ctKzI>. Acesso em: 25 mar. 2023.

BRASIL. **Resolução CD/ANPD Nº 2, de 27 de janeiro de 2022**. Diário Oficial da União, Brasília/DF, 28 jan. 2022, Edição 20, Seção 1, p. 6. Disponível em: <https://www.in.gov.br/en/web/dou/-/resolucaocd/anpd-n-2-de-27-de-janeiro-de-2022-376562019>. Acesso em: 04 fev. 2023.

CAIÇARA, J. **Informática, Internet e Aplicativos**. 1. ed. Paraná: IBPEX, 2007.

CEDERBERG, Robert; WALJI, Muhammad; VALENZA, John. Electronic health records in dentistry: clinical challenges and ethical issues. **Springer Science and Business Media LLC**, pp. 1-12. Cham, Switzerland, 2014. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-08973-7_1. Acesso em: 10 fev. 2023.

CONSELHO FEDERAL DE MEDICINA. Resolução nº 1.638, de 18 de julho de 2002. **Diário Oficial da União**, Brasília, DF, 5 ago. 2002. Seção 1, p. 191. Disponível em: http://www.portalmedico.org.br/resolucoes/CFM/2002/1638_2002.htm. Acesso em: 06 abr. 2023.

CONSELHO FEDERAL DE ODONTOLOGIA. **Resolução nº 118, de 11 de maio de 2012**. Regulamenta a atividade profissional de Odontologia no Brasil. Disponível em: https://website.cfo.org.br/wp-content/uploads/2018/03/codigo_etica.pdf. Acesso em: 8 fev. 2023.

CONSELHO FEDERAL DE ODONTOLOGIA. **Resolução nº 226, de 04 de junho de 2020.**

Dispõe sobre o exercício da Odontologia a distância, mediado por tecnologias, e dá outras providências. Disponível em:

<https://sistemas.cfo.org.br/visualizar/atos/RESOLU%c3%87%c3%830/SEC/2020/226>. Acesso em: 6 abr. 2023.

CORREIA, Marcos Balster Fiore. **A Comunicação de Dados Estatísticos por intermédio de Infográficos: Uma Abordagem Ergonômica.** Dissertação de Mestrado – Pontifícia Universidade Católica, Rio de Janeiro, 2009.

Disponível em: https://www.maxwell.vrac.pucRio.br/14038/14038_4.PDF. Acesso em: 4 fev. 2023.

DE SOUZA, Francisco Luziario; ALVARES, Lillian Maria Araujo de Rezende; NUNES, Rafael Rabelo. Elementos-chave da Transformação Digital que influenciam na Curadoria Digital: Uma Revisão Sistemática de Literatura sob o método TEMAC. **RISTI (PORTO)**, v. E46, p. 463-476, 2022.

ENISA. **Guidelines for SMEs on the security of personal data processing.**

Dezembro de 2016. Disponível em:

<https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-securityof-personal-data-processing>. Acesso em: 15 jan. 2023

FAVARETTO, Maddalena; SHAW, David.; DE CLERCQ, Eva.; JODA, Tim.; ELGER, Bernice Simone. Big data and digitalization in dentistry: a systematic review of the ethical issues. **International Journal of Environmental Research and Public Health**, v. 17, n. 7, p. 2495, 2020. Disponível em:

<https://doi.org/10.3390/ijerph17072495>. Acesso em: 10 fev. 2023.

FINKELSTEIN, Maria Eugenia; FINKELSTEIN, Claudio. Privacidade e Lei Geral de Proteção de Dados Pessoais. **Revista de Direito Brasileira**,

Florianópolis, SC, v. 23, n. 9, p. 284-301, mai./ago. 2019. Disponível em: <https://www.indexlaw.org/index.php/rdb/article/view/5343/4545>. Acesso em: 4 fev. 2023.

FRANCO, S. **Como a Lei Geral de Proteção de Dados (LGPD) impactará as clínicas odontológicas?**. Arujá, junho de 2021. In: Odonto Summit.

Disponível em: <https://encr.pw/bHhDl>. Acesso em: 06 mar. 2023.

GARRITANO, Célia Regina de Oliveira; JUNQUEIRA, Felipe Holanda; LOROSA, Ely Felyppy Soares; FUGIMOTO, Mayara Sanae; MARTINS, Wallace Hostalacio Avelar. Avaliação do prontuário médico de um hospital universitário. **Revista Brasileira de Educação Médica**, v. 44, n. 1, p. 1-6, 2020.

<https://doi.org/10.1590/1981-5271v44.1-20190123>. Disponível em:

<https://www.scielo.br/j/rbem/a/wNjpyTrSQLYhmNQhsP9zccM/?lang=pt&format=pdf>. Acesso em: 25 mar. 2023.

GIL, Carlos Antonio. **Métodos e Técnicas de Pesquisa Social**, 7ª Edição, São Paulo: Atlas, 2019.

HOFFMAN, Sharona. Employing e-health: the impact of electronic health records on the workplace. **Kansas Journal of Law & Public Policy**, v. 19, p. 409, 2009. Disponível em: <https://core.ac.uk/download/pdf/214106457.pdf>.

Acesso em: 10 fev. 2023.

JUAREZ, Davidson; ALVES, Carlos André de Melo; NUNES, Rafael Rabelo; DE OLIVEIRA, Roque Magno. Benefícios e Riscos do Uso da Computação em Nuvem no Setor Público: Uma análise baseada em artigos disponibilizados em bases dados acadêmicos de 2017 a 2021. **RISTI (PORTO)**, v. E49, p. 537-549, 2022.

LUGATI, Lys Nunes; ALMEIDA, Juliana Evangelista de. Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa. **Revista de Direito**, Viçosa, v. 12, n. 2, 2020. Disponível em: <https://periodicos.ufv.br/revistadir/article/view/10597/5880>. Acesso em: 25 jan. 2023.

LYRA, Mauricio Rocha. **Governança da segurança da informação**. Brasília, DF: 2015

MARCONI, Marina de Andrade, LAKATOS, Eva Maria. **Fundamentos de metodologia científica**. 5. ed., São Paulo: Atlas, 2003.

MATTORD, Hebert J.; WHITMAN, Michael E. **Roadmap for Information Security for IT and Infosec Managers**. 2012. Disponível em: <https://acesse.one/rdNVb>. Acesso em: 04 fev. 2023.

MENDES, Schertel. **Privacidade e proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental**. 1ª. ed. São Paulo: Saraiva Educação, 2014

MINAYO, Maria Cecília de Souza. **Pesquisa Social: Teoria, Método e Criatividade**. 21. ed., Petrópolis: Editora Vozes, 2002.

MITTELSTADT, Brent Daniel; FLORIDI, Luciano. The ethics of big data: current and foreseeable issues in biomedical contexts. In: *Electronic health records and data management*. Cham, Switzerland: **Springer**, 2016. p. 303-341. Disponível em: https://link.springer.com/chapter/10.1007/978-3-319-33525-4_19. Acesso em: 04 fev. 2023.

NAKAMURA, Emilio; FORMIGONI FILHO, José Reynaldo; IDE, Marcos Cesar. Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais. In: *WORKSHOP DE REGULAÇÃO, AVALIAÇÃO DA CONFORMIDADE E CERTIFICAÇÃO DE SEGURANÇA*, 5. 2019, São Paulo. Anais [...]. **Porto Alegre: Sociedade Brasileira de Computação**, 2019. p. 11-16. DOI: <https://doi.org/10.5753/wrac.2019.14032>. Acesso em: 04 fev. 2023.

OLIVEIRA, Danilo; YARID, Sérgio. Prontuário odontológico sob a ótica de discentes de Odontologia. **Revista de Odontologia da UNESP**, São Paulo, v. 43, n. 3, p. 158-164, 2014. Disponível em: <https://doi.org/10.1590/rou.2014.031>. Acesso em: 8 fev. 2023.

PEPPET, Scott. Regulating the internet of things: first steps toward managing discrimination, privacy, security and consent. **Texas Law Review**, v. 93, p. 85, 2014. Disponível em: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/tlr93&div=5&id=&page=>. Acesso em: 10 fev. 2023.

PIURCOSKY, Fabrício Pelloso; COSTA, Marcelo Aparecido; FROGERI, Rodrigo Franklin; CALEGARIO, Cristina Lelis Leal. **A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos**. [S.l.], 2019. Disponível em: https://blogs.konradlorenz.edu.co/files/rsn_1023_02_peloso-piurcosky.pdf. Acesso em: 20 fev. 2023.

RODRIGUES, Laura Secfém. LGPD na saúde: a importância da Lei nº 13.787/18 para os prontuários. **Revista Consultor Jurídico**, [S.l.], v.21, n.3, p.1-3, mar. 2021. Disponível em: <https://www.conjur.com.br/2021-mar-21/opiniaio-lgpd-saude-importancia-lei-1378718>. Acesso em: 25 mar. 2023.

SAMONAS, Spyridon; COSS, David. The CIA strikes back: Redefining confidentiality, integrity and availability in security. **Journal of Information System Security**, 10(3), 2014.

SARAIVA, Analuiza Sarmiento. A importância do prontuário odontológico - com ênfase nos documentos digitais. **Revista Brasileira de Odontologia**, 68(2), 157-160, 2011. Disponível em: <https://revista.aborj.org.br/index.php/rbo/article/download/295/245#:~:text=O%20Conselho%20Federal%20de%20Odontologia,anos%20%C3%A0%20%C3%A9poca%20do%20%C3%BAltimo>. Acesso em: 25 mar. 2023.

SILVERMAN, David. **Doing Qualitative Research: A Practical Handbook**. Londres: Sage, 2011.

SIEBRA, Sandra; XAVIER, Gabriela Araújo. Políticas de privacidade da informação: caracterização e avaliação. **BIBLOS**, [S. l.], v. 34, n. 2, 2020. DOI: 10.14295/biblos.v34i2.11870. Disponível em: <https://periodicos.furg.br/biblos/article/view/11870>. Acesso em: 24 mar. 2023.

TELLES, E. T. G.; MARUCO, F. O. R.; SILVA, V. D. S. T. A implementação da Lei Geral de Proteção de Dados no exercício profissional na área da saúde. **Revista Jurídica**, v1, n1, Ago/Nov 2021. Disponível em: <https://revista.unisal.br/lo/index.php/revdir/article/view/1535>. Acesso em: 24 mar. 2023.

TRINKS, Virginia de Melo Dantas ; ALBUQUERQUE, Robson Oliveira ; NUNES, Rafael Rabelo ; MOTA, Gibran Ayupe. Strategic assessment of cyber security contenders to the Brazilian agribusiness in the Beef Sector. **Information**, 13(9), p. 431, 2022. DOI:10.3390/info13090431.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. **Diário Oficial da União Europeia**, Luxemburgo, v. 38, n. L 281, p. 31-50, 23 nov. 1995. Disponível em: <https://eurlex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046>. Acesso em: 06 abr. 2023.

VANRELL, Jorge Paulete. **Odontologia legal e antropologia forense**. Rio de Janeiro: Guanabara Koogan, 2002.

DA SILVA, Marcos Viana; SCHERF, Erick da Luz; DA SILVA, José Everton. The right to data protection versus “security: contradictions of the rights - discourse in the brazilian general personal data protection act (LGPD). **Revista Direitos Culturais**, v. 15, n. 36, p. 209-232, 27 abr. 2020.