Universidade de Brasília
Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas Departamento de Administração

GIOVANNA SILVA CAMELO PAIVA

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

Brasília - DF
2023

GIOVANNA SILVA CAMELO PAIVA

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

Monografia apresentada ao Departamento de Administração como requisito parcial à obtenção do título de Bacharel em Administração.

Professor Orientador: Dr. Rafael Rabelo Nunes

Brasília - DF
2023

GIOVANNA SILVA CAMELO PAIVA

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

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília da aluna

Giovanna Silva Camelo Paiva

Dr., Rafael Rabelo Nunes
Professor-Orientador

Dr., Carlos André de Melo Alves
Professor-Examinador

Me., Fernando Rocha Moreira
Professor-Examinador

Brasília, 11 de abril de 2023.

AGRADECIMENTOS

Agradeço primeiramente ao meu orientador, Professor Rafael Rabelo Nunes, pelo apoio e paciência durante todo o período de construção deste trabalho. Obrigada pelas contribuições no âmbito acadêmico e pessoal, sendo fonte de inspiração ao ensinar a importância da paciência e resiliência no decorrer dos desafios.

Agradeço à minha família, em especial aos meus pais, Francisco e Alcione, que me criaram em um ambiente de harmonia onde a importância dos valores sempre foi ressaltada. Obrigada por sempre me guiarem em direção aos estudos, não medindo esforços em me proporcionar as melhores condições para chegar onde eu almejasse. Obrigada por sempre acreditarem em mim e por me ensinarem que o único caminho para a independência é através do esforço próprio. Agradeço também ao meu irmão, Gustavo, por ser fonte inesgotável de inspiração. O seu companheirismo me faz ir mais longe.

Por fim, agradeço aos meus amigos que compartilharam comigo tantos momentos durante toda a minha vida. Aos meus amigos de longa data, que se fazem presentes apesar do tempo e muitas vezes da distância física. Estarmos juntos nunca significou estarmos perto. E também aos amigos que fiz ao longo da jornada na Universidade de Brasília (UnB), que compartilharam comigo as maravilhas e adversidades de um curso de graduação, levarei todos esses momentos para a vida.

RESUMO

Com o avanço das tecnologias e da relevância das informações na sociedade atual, tornou-se essencial o gerenciamento dos dados de forma segura e responsável. Com isso, mundialmente, foram elaboradas legislações referentes à proteção de dados pessoais, a fim de tutelar o direito à privacidade das pessoas. No Brasil, a lei que rege a proteção de dados é chamada Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018), também conhecida como LGPD. Os agentes de tratamento de pequeno porte, controladores e operadores de dados pessoais, todavia, em razão de seu tamanho, poderiam apresentar eventuais limitações ao se adequarem à esta lei, cabendo à Autoridade Nacional de Proteção de Dados (ANPD) facilitar a conformidade destas empresas, através de adaptações da norma. Empresas atuantes na área da saúde devem dar especial atenção na adequação à LGPD, por tratarem diariamente de dados pessoais sensíveis, referentes à saúde. Este trabalho tem como objetivo avaliar o nível de aplicação da Lei Geral de Proteção de Dados Pessoais em clinicas odontológicas – representadas por profissionais da área – de duas unidades federativas do Brasil, Distrito Federal e Bahia. Para isso, foram realizadas entrevistas em profundidade com 10 profissionais, cirurgiões-dentistas, as quais foram analisadas por meio de análise de conteúdo. Como resultado, foram categorizados os principais aspectos de adequação neste contexto: Conhecimento da LGPD; Políticas de Segurança da Informação; Conscientização e Treinamento interno; Controle de Acesso; Segurança de Dados Pessoais e Armazenamento; Especificações do cotidiano em clínicas odontológicas; e, em seguida, a partir das análises destas categorias, concluiu-se que, ainda hoje, apesar da natureza da área, há pouco conhecimento sobre a LGPD, sendo seus aspectos desconhecidos por grande parte dos profissionais da área. Os resultados demonstram-se relevantes para os profissionais da área odontológica e para as autoridades e profissionais que trabalham com a aplicação desta lei no país.

Palavras-chave: Lei Geral de Proteção de Dados Pessoais; Privacidade de Dados Pessoais; Agentes de Tratamento de Dados; Clínicas Odontológicas.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ANPD – Autoridade Nacional de Proteção de Dados

ART. - Artigo

CDC - Código de Defesa do Consumidor

CEP - Código de Endereçamento Postal

CFM – Conselho Federal de Medicina

CFO - Conselho Federal de Odontologia

CID - Confidencialidade, Integridade e Disponibilidade

CPF – Cadastro de Pessoa Física

CRO - Conselho Regional de Odontologia

DPO - *Data Protection Officer*

ENISA - *The European Union Agency for Cybersecurity*

EPP – Empresa de Pequeno Porte

GDPR - *General Data Protection Regulation*

IEC - *International Eletrotechnical* Comission

ISO - *International Organization for Standardization*

LGPD – Lei Geral de Proteção de Dados

NBR – Norma Brasileira

PL - Projeto Lei

PLS - Projeto de Lei do Senado

PMEs – Pequenas e Microempresas

PSI - Política de Segurança da Informação

RG - Registro Geral

RIPD - Relatório de Impacto à Proteção dos Dados Pessoais

ROPA - *Record Of Processing Activities*

SENACON - Secretaria Nacional do Consumidor

TIC - Tecnologias da Informação e Comunicação

SUMÁRIO

1. INTRODUÇÃO

Atualmente, a sociedade impulsionada pelo movimento de Transformação Digital, caracterizado pelo avanço das tecnologias no cotidiano da população, em especial das Tecnologias da Informação e Comunicação (TIC), vivencia a Era dos Dados e da Informação, tendo em vista que o uso cada vez maior de plataformas digitais, ocasionou na intensificação da importância das informações. Esta nova realidade de avanço tecnológico e crescimento de bancos de dados, portanto, trouxeram inovações que refletem diretamente no aumento da qualidade, da produtividade e na redução dos custos, agregando valor aos produtos e serviços oferecidos, desse modo, tomando relevante importância no cotidiano e na economia da sociedade moderna (DE SOUZA; ALVARES; NUNES, 2022).

Considerando o contexto atual em que a sociedade está imersa, no qual há um constante crescimento na relevância das informações, observa-se a importância do gerenciamento dos dados de forma segura e responsável. As inovações na área da Tecnologia da Informação, têm contribuído para que dados e informações sejam processados e armazenados com agilidade, sendo necessário às empresas buscarem as melhores alternativas para viabilizar o processamento e o armazenamento desses dados e informações (JUAREZ; ALVES; NUNES; DE OLIVEIRA, 2022).

A Segurança da Informação, portanto, tornou-se um atributo essencial para a manutenção da privacidade e proteção dos dados pessoais dos indivíduos. A Segurança da informação abrange as medidas tomadas para defender as informações processadas dentro de um sistema (por exemplo, eletrônico ou físico) contra acesso não autorizado, uso, divulgação, interrupção, modificação, leitura, inspeção, gravação ou destruição. O modelo mais utilizado para orientar a gestão da segurança da informação dentro de uma organização é representado pela chamada tríade CID: confidencialidade, integridade e disponibilidade da informação (UNIÃO EUROPÉIA, 2016).

Com a intensificação dos fluxos de informação através do desenvolvimento da tecnologia, surgem novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, refletindo diretamente no direito à privacidade das pessoas. A possibilidade de uso indevido dos dados pessoais gera riscos envolvendo a violação à privacidade e à personalidade dos cidadãos na sociedade da informação (FINKELSTEIN; FINKELSTEIN, 2019).

O direito à privacidade está diretamente ligado ao direito da personalidade da pessoa humana e possui previsão constitucional (art 5º, inciso X), onde está previsto que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". E também está prevista no artigo 21 do Código Civil, onde diz que “a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma” (BRASIL, 2023).

Segundo Mendes (2014), “a disciplina da proteção de dados pessoais emerge no âmbito da sociedade da informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados em si, mas a pessoa que é titular desses dados”.

O objetivo das legislações relativas à proteção de dados é garantir que a pessoa física saiba quem tem seus dados, quais informações estão em posse e o que está sendo feito com essas informações, a fim de resguardar sua privacidade (NAKAMURA; FORMIGONI; IDE, 2020).

No Brasil, a lei que rege a proteção e dados é chamada Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), também conhecida como LGPD. A LGPD entrou em vigor em 18 de setembro de 2020, e versa sobre o tratamento de dados pessoais, dispostos em meios físicos ou digitais. A lei tem como principal intuito proteger os direitos fundamentais de liberdade, privacidade e do livre desenvolvimento de personalidade da pessoa natural, dispostos na Constituição Federal de 1988 (BRASIL, 2020).

O surgimento da LGPD, tornou obrigatório aos agentes de tratamento de dados pessoais, sobretudo, empresas, que são detentoras de um grande montante de dados pessoais de terceiros, a se adequarem aos termos descritos em lei. Os agentes de tratamento de pequeno porte, todavia, em razão de seu tamanho, poderiam apresentar eventuais limitações ao se adequarem à Lei Geral de Proteção de Dados Pessoais (GAVA, 2021).

A criação de uma lei que protege os dados pessoais, entretanto, deixou brechas que deveriam ser sanadas pela autoridade competente. A Autoridade Nacional de Proteção de Dados (ANPD) é o órgão da administração pública federal responsável

por zelar pela proteção de dados pessoais e por implementar e fiscalizar o cumprimento da LGPD no Brasil (BRASIL, 2020).

Considerando a observância desta problemática, a ANPD priorizou em sua agenda o estabelecimento de flexibilizações ao texto da LGPD, visando adequar a regulamentação à realidade de empresas de portes menores. Desse modo, em 28 de janeiro de 2022 foi publicado a Resolução CD/ANPD nº 2 que regulamenta a aplicação da Lei Geral de Proteção de Dados para agentes de tratamento de pequeno porte, trazendo flexibilizações de medidas definidas nos termos da lei (BRASIL, 2022).

Dentre as empresas de micro e pequeno porte, as clínicas médicas e odontológicas representam o setor da saúde neste nicho, e devem, especialmente, se atentarem à privacidade dos pacientes.

Apesar de à princípio não se relacionar a área odontológica com bancos de dados e informações, uma clínica detém diversos tipos de dados pessoais de seus pacientes e funcionários, portanto, observa-se, principalmente pela natureza do setor, a importância de as clínicas odontológicas estarem em conformidade com os direcionamentos tratados na LGPD. Desse modo, além de garantir os direitos fundamentais das pessoas titulares dos dados e exercer a manutenção de questões éticas intrínsecas à profissão, o cirurgião-dentista também evitará qualquer implicação de multas ou processos judiciais relativos à questão da proteção de dados.

1.1. JUSTIFICATIVA

A Lei Geral de Proteção de Dados (LGPD) é uma legislação que estabelece as regras para a coleta, armazenamento, uso e compartilhamento de dados pessoais de indivíduos no Brasil. Com a crescente utilização de tecnologias digitais no cotidiano das clínicas odontológicas, a implementação da LGPD se tornou uma questão crítica para garantir a proteção dos dados dos pacientes.

Alguns dos dados pessoais coletados pelas clínicas odontológicas são: nome, endereço, CPF, telefone e informações médicas, considerados dados sensíveis. Esses dados são essenciais para a prestação de serviços odontológicos, mas também podem ser utilizados de forma indevida ou expostos a riscos de segurança, o que pode levar a consequências graves para a privacidade dos pacientes.

Por essa razão, é fundamental que as clínicas odontológicas estejam em conformidade com a LGPD para garantir a proteção dos dados pessoais dos

pacientes. Além disso, a implementação da LGPD também traz benefícios para as próprias clínicas, que passam a ter processos mais eficientes e seguros de gestão de dados.

Observou-se, entretanto, que as clínicas odontológicas, apesar de coletarem uma grande quantidade de informações pessoais dos pacientes, não aparentavam estar em adequação com as implementações trazidas pela LGPD. Essa realidade motivou a presente pesquisa que visa identificar o nível de adequação e conhecimento desta lei neste meio.

Os resultados da pesquisa são de grande importância, uma vez que irá contribuir para o aprimoramento da proteção de dados pessoais dos pacientes e para o desenvolvimento de melhores práticas de gestão de dados nas clínicas odontológicas. Além disso, a pesquisa também pode auxiliar na conscientização dos profissionais da área sobre a importância da LGPD e em sua adaptação às mudanças na legislação.

1.2. OBJETIVO GERAL

O objetivo geral desta pesquisa é avaliar o nível de aplicação da Lei Geral de Proteção de Dados Pessoais em clinicas odontológicas – representadas por profissionais da área – de duas unidades federativas do Brasil, Distrito Federal e Bahia.

1.3. OBJETIVOS ESPECÍFICOS

a) Elaborar roteiro de entrevista semiestruturada para condução de entrevistas visando a avaliação da implementação dos requisitos dispostos na Lei Geral de Proteção de Dados em clínicas odontológicas;
b) Entrevistar profissionais da área odontológica que trabalhem em clínicas particulares de pequeno porte, baseado nas categorias previamente identificadas;
c) Identificar e qualificar o nível de adequação das clínicas odontológicas, em seus processos internos, tendo como base os parâmetros dispostos na Lei Geral de Proteção de Dados;
d) Analisar as categorias de adequação definidas *a priori*: Conhecimento da LGPD; Políticas de Segurança da Informação; Conscientização e

Treinamento interno; Controle de Acesso; Segurança de Dados Pessoais e Armazenamento; Especificações do cotidiano em clínicas odontológicas.

e) Identificar a maturidade atual das clínicas quanto à aplicação da Lei Geral de Proteção de Dados, além das percepções sobre a importância de conformidade e riscos relacionados à inobservância da lei.

2. REFERENCIAL TEÓRICO

Nesta seção serão abordados os principais conceitos para melhor entendimento do trabalho.

2.1. DADO, INFORMAÇÃO E CONHECIMENTO

Tratados recorrentemente como sinônimos, os dados, as informações e o conhecimento não são considerados termos semanticamente idênticos, apesar de estarem diretamente relacionados entre si. De forma simplificada, Correia (2009) estabelece um vínculo sistêmico entre os três termos, conceituando-os da seguinte forma:

- Dado: é o registro ou indício relacionável a algum objeto que lhe atribui um valor semântico quantitativo ou qualitativo;
- Informação: é o significado produzido pelo agrupamento de dados;
- Conhecimento: é a informação compreendida, tomada como verdadeira e guardada na memória para usos futuros.

Observa-se, portanto, que o nível de abstração está diretamente ligado com o conceito de cada um dos termos, sendo os dados relativamente mais abstratos que as informações, que, por sua vez, são mais abstratas que o conhecimento (MARINO, 2020).

Nesse sentido, Lyra (2015) compreende que a informação é o conjunto de dados tratados e organizados para representar um sentido em um determinado contexto. Logo, os dados, quando contextualizados, passam a ter valor para a sociedade, sobretudo, para as organizações, ao ajudá-las na tomada de decisões estratégicas. E essa geração de valor a partir da interpretação das informações é compreendida como conhecimento.

2.2. SOCIEDADE DA INFORMAÇÃO

A captação, o armazenamento e a disseminação de dados, apesar de não serem exclusivamente sucedidos por meios eletrônicos, tornou-se assunto em evidência nos últimos anos, em face da facilidade que os meios digitais trouxeram na captação e tratamento dos dados (FINKELSTEIN, 2019).

O movimento para a adoção de tecnologias digitais, que se convencionou chamar de Transformação Digital, vem sendo impulsionado pelo avanço das tecnologias, em especial as Tecnologias da Informação e Comunicação (TIC). Atualmente, a sociedade, impulsionada por essa transformação, vivencia a Era dos Dados e da Informação, tendo em vista que o uso cada vez maior de plataformas digitais, ocasionou na intensificação do tráfego e da manipulação de informações, e com isso trazendo inovações que refletem diretamente no aumento da qualidade, da produtividade e na redução dos custos, agregando valor aos produtos e serviços oferecidos à sociedade (DE SOUZA; ALVARES; NUNES, 2022).

O crescimento exponencial no volume de dados e a alta velocidade com que são gerados é representado pelo grande fenômeno do século 21, o *Big Data*. De acordo com o Glossário Gartner (2021), o *Big Data* são os ativos de informação de alto volume, alta velocidade e/ou alta variedade, que necessitam de formas inovadoras e econômicas para o processamento de informações, que permitem insights aprimorados, tomada de decisões e automação de processos. O *Big Data* é originado, portanto, através das ações de usuários nas plataformas e ambientes digitais que produzem informações, organizadas e compiladas através de algoritmos matemáticos (SALGADO LEME; BLANK, 2020).

Nesse sentido, um vasto volume de informação é produzido a todo segundo, principalmente nos ambientes virtuais da internet, nos quais os dados são constantemente gerados a partir da constatação de sites visitados, do tempo gasto nestes sites, da coleta de preferências de compras, da identificação da localização do usuário, entre outros exemplos de situações virtuais geradoras de informação (CARVALHO, 2018).

Este fluxo de informação, quando coletado por organizações empresariais e utilizado para fins lucrativos, é chamado de Economia Informacional ou Monetização de Dados. Segundo Cohen (2002), verifica-se que neste novo modelo de economia, focado na comercialização de dados, a principal mudança está na forma como a informação é utilizada.

Conforme Adjei (2015), a monetização das informações é o processo no qual há a transformação dos dados em mercadorias, gerando rentabilidade ao responsável pela sua coleta e/ou tratamento. Complementa Vital (2018) que, na realidade da Economia da Informação, os dados são considerados o “novo petróleo”, ou seja,

possuem alto valor monetário, integrando diretamente os ativos das organizações empresariais.

Assim, novas possibilidades de rentabilidade são observadas pelas organizações neste novo contexto atual, podendo haver a utilização dos dados para o uso próprio ou para a venda a terceiros. Conforme Yamagata (2017), há duas abordagens para a monetização de dados, a interna e a externa. A abordagem interna ocorre quando os dados são transformados em conhecimento, auxiliando na tomada de decisões e na alavancagem dos resultados da empresa. Já a abordagem externa, trata da transformação dos dados em produtos de interesse de terceiros, resultando na comercialização dessas informações.

Além das empresas com finalidades lucrativas, os dados também são de suma importância para outros tipos de entidades. De acordo com Finkelstein (2019), há o interesse público na coleta e utilização dos dados, para fins de segurança pública, investigação criminal e combate a ilícitos, por exemplo.

Portanto, nota-se que a Sociedade da Informação é caracterizada não só pelo uso das tecnologias de informação e comunicação, mas pelo modo que o uso dessas tecnologias transforma a sociedade, influenciando no comportamento das pessoas e moldando o contexto social, político e econômico global.

Segundo Manuel Castells (2001), na era da informação "a geração, processamento e transmissão de informação torna-se a principal fonte de produtividade e poder", e no mesmo sentido, define que a Sociedade da Informação é um conceito usado para descrever uma sociedade que faz o melhor uso das Tecnologias da Informação e Comunicação, utilizando a informação como o centro da atividade humana.

O avanço tecnológico e crescimento de banco de dados, portanto, facilitou a transmissão e o armazenamento das informações, tomando relevante importância no cotidiano e na economia da sociedade moderna.

2.3. SEGURANÇA DA INFORMAÇÃO

Considerando o contexto atual em que a sociedade está imersa, no qual há um constante crescimento na relevância das informações, observa-se a importância do gerenciamento dos dados de forma segura e responsável. As inovações na área da Tecnologia da Informação, têm contribuído para que dados e informações sejam

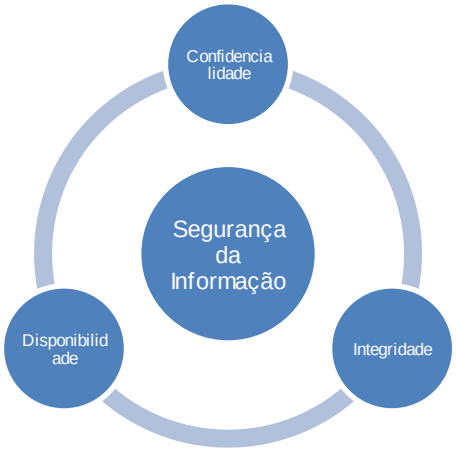
processados e armazenados com agilidade, sendo necessário às empresas buscarem as melhores alternativas para viabilizar o processamento e o armazenamento desses dados e informações (JUAREZ; ALVES; NUNES; DE OLIVEIRA, 2022).

Conforme Ziraba e Okolo (2018), a informação é considerada a base para vantagens competitivas na economia atual, entretanto, deter a posse de informações de terceiros pode representar grande ameaça interna para as organizações, possibilitando a violação da privacidade de seus clientes e funcionários.

A Segurança da Informação, portanto, tornou-se um atributo essencial para a manutenção da privacidade e proteção dos dados pessoais dos indivíduos. Segundo a norma ABNT NBR ISO/IEC 27002 (2013), "a Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" Segurança da Informação é a proteção da informação quanto a vários tipos de ameaças, de modo a garantir a continuidade do negócio, minimizar o risco para o negócio, maximizar o retorno sobre o investimento e as oportunidades de negócio (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

A Segurança da Informação abrange as medidas tomadas para defender as informações processadas dentro de um sistema (por exemplo, eletrônico ou físico) contra acesso não autorizado, uso, divulgação, interrupção, modificação, leitura, inspeção, gravação ou destruição. O modelo mais utilizado para orientar a gestão da segurança da informação dentro de uma organização é representado pela chamada tríade CID: confidencialidade, integridade e disponibilidade da informação (UNIÃO EUROPÉIA, 2016), conforme disposto na Figura 1.

Figura 1: Tríade CID



(Fonte: adaptado de ENISA, 2016, p. 10)

Neste sentido, segundo Whitman e Mattord (2012), a Segurança da Informação se fundamenta na proteção da confidencialidade, integridade e disponibilidade dos ativos da informação. Esta segurança é alcançada através de mecanismos de defesa relacionados à aplicação de políticas, uso de tecnologia, medidas educativas, treinamento e conscientização, preservando a informação em seu armazenamento, processamento ou transmissão (WHITMAN; MATTORD, 2012).

A Norma ISO/IEC 27000 (2016) define os princípios da segurança da informação da seguinte forma:

I. Confidencialidade:

A confidencialidade é definida como a "propriedade de que as informações não sejam disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2016).

Na prática, a confidencialidade trata de assegurar que somente indivíduos autorizados tenham acesso às informações armazenadas ou transmitidas por algum meio. A importância de sua manutenção é garantir que indivíduos não tenham acesso acidental ou intencional a informações quando não autorizados (CAIÇARA, 2007).

Segundo Whitman e Mattord (2012), a confidencialidade das informações é importante para a proteção de dados pessoais de funcionários e consumidores, e a não preservação dessas informações pode destruir a reputação de uma empresa e levá-la a cometer litígios e ao pagamento de multas regulatórias. Para proteger a confidencialidade das informações, podem ser tomadas algumas medidas, como por exemplo:

a) Classificação da informação;
b) Armazenamento seguro de documentos;
c) Aplicação de políticas gerais de segurança;
d) Treinamento dos guardiões da informação e usuários finais;
e) Criptografia das informações.

II. Integridade:

A Integridade é definida como a "propriedade de precisão e completude" (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2016).

Whitman e Mattord (2012) definem que o princípio da Integridade é "a qualidade de ser inteiro, completo e incorrupto". Segundo o autor, uma ameaça à integridade do

ativo ocorre quando ele é exposto a corrupção, dano, destruição ou outra interrupção de seu estado autêntico. Além disso, todo ativo se torna vulnerável à corrupção quando passam por simples processamentos diários como, por exemplo, a inserção, o armazenamento, ou as transmissões destes dados.

Para proteger a integridade das informações, utiliza-se métodos de detecção de falhas na integridade de um sistema de arquivos, em razão de um ataque de vírus. O principal método é procurar alterações no estado dos arquivos, conforme indicado pelo tamanho destes ou, em sistemas operacionais mais avançados, através do valor de hash ou soma de verificação dos arquivos (WHITMAN; MATTORD, 2012).

III. Disponibilidade:

A disponibilidade é definida como a propriedade de “a informação ser acessível e utilizável quando uma parte autorizada a exigir” (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2016).

Na prática a Disponibilidade, segundo Whitman e Mattord (2012), trata da característica da informação que permite o acesso do usuário ao dado sem interferência ou obstrução e em um formato utilizável. Os princípios da Integridade e da Confidencialidade da informação devem ser protegidos, diminuindo a vulnerabilidade e as ameaças de ataques, a Disponibilidade, por sua vez, não implica na acessibilidade da informação a qualquer usuário, mas sim, significa que o dado estará disponível apenas para usuários autorizados.

Portanto, nesse sentido, Piurcosky, Costa, Frogeri e Calegario (2019), resumem que os princípios da Segurança da Informação (SI) têm como objetivo assegurar a proteção das informações contra acessos não autorizados (Confidencialidade); manter a disponibilização das informações (Disponibilidade) e ser íntegra e autêntica em seus devidos fins (Integridade).

Segundo Lyra (2015), atualmente, o bem mais valioso das organizações são seus bancos de dados, local de armazenamento de dados em sua forma bruta, observa-se, portanto, a importância de aplicação de práticas relacionadas à Segurança da Informação (SI) para as organizações, públicas ou privadas, visando reduzir os riscos relacionados ao tráfego de informações em formato digital.

Conforme Viana da Silva, Scherf e Silva (2020), com a revolução da tecnologia da informação, *big data* e internet das coisas, a proteção de dados se tornou um

problema para os indivíduos, empresas, governos, organizações internacionais e alguns outros atores.

Neste sentido, a segurança cibernética pode ser definida como a proteção dos sistemas de informação (*hardware, software* e infraestrutura associada), dos dados neles contidos e dos serviços que prestam, contra acessos não autorizados, danos ou uso indevido, incluindo danos causados intencionalmente pelo operador do sistema, ou acidentalmente, a partir da falha em seguir os procedimentos de segurança (TRINKS; ALBUQUERQUE; NUNES; MOTA, 2022).

2.4. PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Com a intensificação dos fluxos de informação através do desenvolvimento da tecnologia, surgem novas possibilidades de armazenamento, utilização e manipulação de informações pessoais, refletindo diretamente no direito à privacidade das pessoas. A possibilidade de uso indevido dos dados pessoais gera riscos envolvendo a violação à privacidade e à personalidade dos cidadãos na sociedade da informação (FINKELSTEIN; FINKELSTEIN, 2019).

O direito à privacidade está diretamente ligado ao direito da personalidade da pessoa humana e possui previsão constitucional (art 5º, inciso X), onde está previsto que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação". E também está prevista no artigo 21 do Código Civil, onde diz que "a vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (BRASIL, 2023).

Conforme leciona Flores (2013), os direitos da personalidade podem ser classificados em:

- Direitos de ordem física: visam tutelar a integridade dos valores da natureza física do homem, compreendendo o direito à vida e a integridade corporal;
- Direitos de ordem intelectual: visam tutelar a integridade intelectual abrangendo o direito do autor, liberdade religiosa, liberdade de expressão e ao segredo;

- Direitos de ordem moral: visam tutelar a integridade moral, tais como o direito à honra, à privacidade, à imagem e ao nome.

Neste sentido, Fiuza (2009) esclarece que a pessoa humana é composta por todos estes atributos tutelados pelo direito à personalidade, cujo principal objetivo é a proteção e a promoção da pessoa humana e de sua dignidade.

O direito à proteção dos dados pessoais, por sua vez, também possui previsão constitucional, sendo incluída no rol de direitos fundamentais através da Emenda Constitucional nº 115 de 2022. Prevê a Constituição em seu artigo 5º, inciso LXXIX, que "é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais" (BRASIL, 2022).

Segundo Mendes (2014), "a disciplina da proteção de dados pessoais emerge no âmbito da sociedade da informação, como uma possibilidade de tutelar a personalidade do indivíduo, contra potenciais riscos a serem causados pelo tratamento de dados pessoais. A sua função não é a de proteger os dados em si, mas a pessoa que é titular desses dados".

Com o amplo oferecimento de dados pessoais na rotina virtual da atualidade, o indivíduo muitas vezes perde o controle sobre suas próprias informações, logo após oferecê-las, desconhecendo sobre a sua utilização e a finalidade que serão usadas. A proteção de dados, portanto, diz respeito ao equilíbrio entre o controlador dos dados pessoais e o titular, que muitas vezes desconhece como se dá o tratamento de suas informações, suas finalidades ou os seus possíveis riscos (MUHLEN; SCHNEIDER, 2020).

O fluxo de dados se tornou um componente essencial para o comércio, as comunicações e as interações sociais, desse modo, a proteção de dados pessoais passou a ser uma preocupação para grande parte dos países. Nesse contexto, muitos países têm adotado novas regras de proteção de dados ou modernizado as que já tinham (IRAMINA, 2020).

De modo geral, o princípio fundamental que rege o uso de dados pessoais é o consentimento da pessoa que deve ser obtido a partir de uma solicitação clara, objetiva e simples, explicando quais dados serão capturados, como serão utilizados e por quanto tempo serão mantidos (MUHLEN; SCHNEIDER, 2020).

De acordo com Whitman e Mattord (2012), a privacidade aplicada no contexto da proteção de dados, pode ser definida da seguinte forma:

> Privacidade significa que quando os dados são coletados, usados e armazenados por uma organização, eles só podem ser usados para o propósito declarado pelo proprietário dos dados no momento em que foram coletados. Ele governa o que a organização pode ou não fazer com as informações fornecidas. Privacidade é muitas vezes confundida com confidencialidade. A privacidade diz respeito aos usos dos dados, enquanto a confidencialidade diz respeito ao acesso aos dados (WHITMAN; MATTORD, 2012, p 488).

O objetivo das legislações relativas à proteção de dados é garantir que a pessoa física saiba quem tem seus dados, quais informações estão em posse e o que está sendo feito com essas informações, a fim de resguardar sua privacidade (NAKAMURA; FORMIGONI; IDE, 2020).

2.5. ORIGEM LGPD

A Lei Geral de Proteção de Dados surgiu devido à necessidade de garantir a segurança dos dados pessoais em meio à sociedade da informação, possuindo embasamento em legislações já vigentes no exterior.

2.5.1 Panorama Internacional: GDPR

Atualmente, o principal marco regulatório sobre proteção de dados é a GDPR (*General Data Protection Regulation*), em português, “Regulamento Geral sobre a Proteção de Dados”, vigente em todo território da União Europeia. A legislação consolida a importância da proteção de dados pessoais e é considerada como a principal referência sobre o assunto no mundo, influenciando legislações de países como os Estados Unidos, e, sobretudo, do Brasil.

A GDPR foi aprovada pelo Parlamento da União Europeia em 14 de abril de 2016, e entrou em vigor em 25 de maio de 2018, em substituição à Diretiva de Proteção de Dados de 1995 (Diretiva 95/46/EC). Nesta regulamentação, promulgada em meados dos anos 90, estabelecia-se de forma ultrapassada o processamento dos dados na União Europeia, carecendo de conceitos modernos relacionados às novas tecnologias e à sociedade da informação. Além disso, a Diretiva estabelecia que cada Estado-Membro da União Europeia deveria firmar lei própria sobre proteção de dados, havendo uma ausência de harmonização entre as regulamentações dos países europeus (UNIÃO EUROPEIA, 1995)

Dessa forma, de modo geral, conforme destaca Viana da Silva, Scherf e Silva (2020), a GDPR foi regulamentada objetivando principalmente (a) unificar as leis de privacidade de dados pela Europa; (b) proteger e empoderar a privacidade de dados dos cidadãos da União Europeia e (c) reformular a forma que as organizações locais lidavam com os dados.

Apesar de expansivas, conforme ressaltam Finkelstein *et al.* (2019), os regulamentos e as leis que tratam sobre a proteção de dados, baseiam-se na premissa de que todo cidadão possui a expectativa de privacidade, podendo ser restringida apenas em face de acordo, contrato, lei ou consentimento unilateral. Neste sentido, compreende Doneda (2014):

> O ponto fixo de referência nesse processo é que, entre os novos prismas para a abordagem da questão, mantém-se uma constante referência objetiva a uma disciplina jurídica específica para os dados pessoais, que manteve o nexo de continuidade com a disciplina da privacidade, da qual é uma espécie de herdeira, atualizando-a e impondo-lhe características próprias (DONEDA, 2014, p. 25).

Desse modo, visando proteger a privacidade dos indivíduos, a GDPR traz normas que exigem maior responsabilização e transparência das empresas no tratamento dos dados pessoais, e a obrigatoriedade do expresso consentimento do titular para o uso de seus dados (IRAMINA, 2020).

A norma regula sobre o tratamento de qualquer dado pessoal ou informação que se relaciona a um indivíduo identificado ou identificável. Isso porque, com a implementação da lei, buscou-se proteger, além do dado e de seu valor econômico, a privacidade como um todo, evitando-se comportamentos discriminatórios e exposições não desejadas da vida privada do titular (ROCHFELD, 2018).

2.5.2 Panorama Nacional: Origem LGPD

No Brasil, antes da LGPD, a questão da proteção de dados era tratada indiretamente em legislações como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. Contudo, uma regulamentação específica sobre o assunto só surgiria anos depois, após o direito à proteção de dados adquirir o enfoque de direito fundamental, e a Lei Geral de Proteção de Dados entrar em vigor em 18 de setembro de 2020 (LUGATI; ALMEIDA, 2020).

De forma cronológica, em 1990, o Código de Defesa do Consumidor, em seu artigo 43, expõe a proteção dada ao titular de dados frente a banco de dados e cadastros. Exigia-se que o consumidor fosse comunicado sobre a abertura de cadastros, fichas e registros de dados pessoais e de consumo. (LUGATI; ALMEIDA, 2020). Entretanto, segundo Andrade e Moura (2019), a legislação consumerista visava regular os bancos de dados, e não se importava de fato com a necessidade do consentimento dos titulares.

Anos depois, surge em 2011 a "Lei do Cadastro Positivo" (Lei nº 12.414/2011), que estabeleceu regulamentação sobre dados derivados de operações financeiras e adimplementos dos consumidores, que tornavam mais fácil a concessão de crédito. A exigência que a lei traria, quanto ao consentimento do titular para que ocorra o tratamento de dados, seria, de acordo com Lugati e Almeida (2020), a introdução do sistema *opt-in* no ordenamento jurídico brasileiro.

Neste mesmo período, surgiram algumas outras leis, como a Lei de Acesso à Informação (Lei nº 12.527/2011), cujo objetivo, segundo Bioni (2022), é dar maior transparência, ativa e passiva, para as informações e dados produzidos ou custodiados por órgãos e entidades público, e a Lei Carolina Dieckmann (Lei nº 12.737/2012), relacionadas à criminalização da obtenção de dados pessoais sem consentimento, através de aparelhos eletrônicos.

Em 2014, o Marco Civil da Internet (Lei nº 12.965/2014), surge na tentativa de regular o uso da internet, através de leis não penais, visando evitar um possível retardo na evolução tecnológica do país causada pelas abordagens restritivas e prescritivas (BIONI, 2020). A lei possui artigos visando a proteção à confidencialidade e inviolabilidade da vida privada digital e os fluxos de tráfego da Internet, exigindo o consentimento expresso do usuário para tratamento de dados, além de garantir que a guarda e disponibilização de registros de conexão e de acesso a aplicações na internet resguardem a intimidade, honra e imagem de seus usuários (FINKELSTEIN; FINKELSTEIN, 2019).

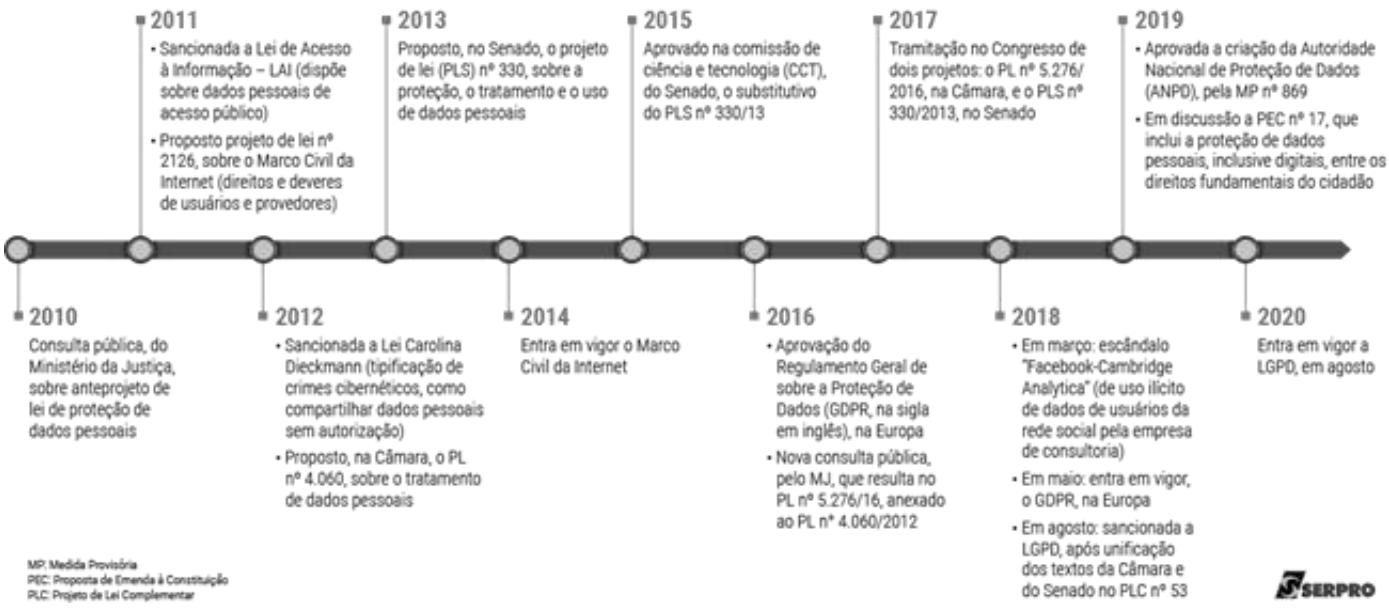
Mesmo com o Marco Civil da Internet, o Brasil ainda carecia de uma legislação mais abrangente e específica sobre proteção de dados, seja de natureza digital ou não. Além disso, após a GDPR traçar em seu artigo 46, a necessidade de legislação específica e adequação de outros países aos regulamentos de proteção de dados, o Brasil foi impulsionado a criar sua própria legislação (LUGATI; ALMEIDA, 2020).

Nessa linha, a partir de 2015, a discussão sobre o tema começou a ganhar mais espaço no Brasil, tramitando projetos de lei na Câmara (PL nº 5276/2016) e no Senado Federal (PLS nº 330/2013) para regulamentar, em lei própria, a proteção de dados pessoais.

Em 2018, segundo Finkelstein *et al.* (2019), a disseminação de casos com possíveis implicações no controle dos processos eleitorais democráticos e o escândalo da *Cambridge Analytica,* empresa de consultoria britânica, que coletava dados, em plataformas de mídia social, como o *Facebook*, sem autorização expressa e sem publicar resultados, levou à aceleração dos trâmites legislativos referentes à Lei Geral de Proteção de Dados que foi sancionada em agosto de 2018 e entrou em vigor em 18 de setembro de 2020.

Na Figura 2, e é possível verificar os principais marcos no processo de surgimento da Lei Geral de Proteção de Dados no Brasil.

Figura 2: Linha do tempo da proteção de dados pessoais e da Lei Geral de Proteção de Dados Pessoais, no Brasil



(Fonte: SERPRO, disponível na *internet*)

2.6. LEI GERAL DE PROTEÇÃO DE DADOS

A Lei Geral de Proteção de Dados (Lei nº 13.709, de 14 de agosto de 2018), também conhecida como LGPD, entrou em vigor em 18 de setembro de 2020, e versa sobre o tratamento de dados pessoais, dispostos em meios físicos ou digitais. A lei tem como principal intuito proteger os direitos fundamentais de liberdade, privacidade e do livre desenvolvimento de personalidade da pessoa natural, dispostos na Constituição Federal de 1988. Esta lei complementa a proteção já anteriormente normatizada pelo Código de Defesa do Consumidor e pelo Marco Civil da Internet (BRASIL, 2018).

Com intuito de regular a coleta, o uso, o processamento e o compartilhamento de dados no país, a LGPD instituiu a Autoridade Nacional de Proteção de Dados (ANPD). O cidadão pode denunciar ou efetuar reclamações diretamente à esta entidade que deverá fiscalizar e aplicar sanções quando não cumprido as normas estabelecidas na LGPD (BRASIL, 2018).

Para aplicar da Lei Geral de Proteção de Dados, se faz necessário compreender a conceituação proposta para os principais elementos dispostos em seu corpo textual.

2.6.1 Dados

No Brasil, antes da LGPD, a questão da proteção de dados era tratada indiretamente em legislações como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. Contudo, uma regulamentação específica sobre o assunto só surgiria anos depois, após o direito à proteção de dados adquirir o enfoque de direito fundamental, e a Lei Geral de Proteção de Dados entrar em vigor em 18 de setembro de 2020 (LUGATI; ALMEIDA, 2020).

I. Dados Pessoais

O Dado Pessoal é o bem protegido pela LGPD, e é definido por ela como qualquer "informação relacionada a pessoa natural identificada ou identificável". Portanto, na prática, entende-se que dados pessoais são todas as informações relacionadas a uma pessoa, que possibilite identificá-la diretamente ou indiretamente, através de associações com outras informações.

Segundo o Guia de Proteção de Dados (2021), elaborado pela ANPD, alguns exemplos de dados pessoais são: Nome e Sobrenome; Endereço residencial; Endereço de e-mail; Gênero; Data de nascimento; Número de documentos como RG, CPF e Carteira de Trabalho; Dados de geolocalização de um telefone celular; Número de telefone pessoal; entre outros.

Observa-se que a LGPD não traz um rol taxativo de todos os dados pessoais, portanto, é possível considerar como dado pessoal diversas informações a depender do contexto em que está inserida.

II. Dados Pessoais Sensíveis

Os Dados Sensíveis são definidos pela Lei como qualquer "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (BRASIL, 2018). Os dados pessoais sensíveis, diferentemente dos dados pessoais, são apresentados em lei de forma taxativa, enquanto os dados pessoais são uma categoria mais ampla.

Os dados sensíveis devem ser tratados de forma mais cautelosa, visto que eventual incidente de segurança destes dados pode ocasionar danos maiores aos direitos de seus titulares, por exemplo, a descriminação (BRASIL, 2018).

O artigo 11 da Lei Geral de Proteção de Dados discorre sobre as hipóteses específicas de tratamento de dados pessoais sensíveis, sendo necessário o consentimento expresso do titular do dado quanto ao uso de suas informações para finalidades específicas.

III. Dados Anonimizados

Segundo a Lei Geral de Proteção de Dados, o dado anonimizado é qualquer "dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento" (BRASIL, 2018). Logo, considera-se dado anonimizado aquele que perde possibilidade de associação, direta ou indireta, a um indivíduo no momento em que é tratado.

Conforme o Guia de Boas Práticas da LGPD (BRASIL, 2020), elaborado pelo governo federal, a técnica de anonimização é a responsável por retirar a relação de

identificação entre o dado e seu titular. A partir do momento que o dado é anonimizado, ou seja, não é possível a associação, direta ou indireta, entre dado e titular, esse dado sai do escopo da legislação, por não mais se tratar de um dado pessoal, conforme previsto no art. 12 da LGPD.

2.6.2 Tratamento de Dados

O tratamento de dados abrange qualquer atividade que utilize um dado pessoal na execução de sua operação. A LGPD traz o conceito de tratamento de dados em seu art. 5º como “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração” (BRASIL, 2018).

Conforme apresentado pelo Governo Federal, através Guia de Boas Práticas da LGPD (BRASIL, 2020), as operações de tratamento de dados podem ser exemplificadas da seguinte forma:

> ACESSO - ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
>
> ARMAZENAMENTO - ação ou resultado de manter ou conservar em repositório um dado;
>
> ARQUIVAMENTO - ato ou efeito de manter registrado um dado em qualquer das fases do ciclo da informação, compreendendo os arquivos corrente, intermediário e permanente, ainda que tal informação já tenha perdido a validade ou esgotado a sua vigência;
>
> AVALIAÇÃO - analisar o dado com o objetivo de produzir informação;
>
> CLASSIFICAÇÃO - maneira de ordenar os dados conforme algum critério estabelecido;
>
> COLETA - recolhimento de dados com finalidade específica;
>
> COMUNICAÇÃO - transmitir informações pertinentes a políticas de ação sobre os dados;
>
> CONTROLE - ação ou poder de regular, determinar ou monitorar as ações sobre o dado;
>
> DIFUSÃO - ato ou efeito de divulgação, propagação, multiplicação dos dados;
>
> DISTRIBUIÇÃO - ato ou efeito de dispor de dados de acordo com algum critério estabelecido;
>
> ELIMINAÇÃO - ato ou efeito de excluir ou destruir dado do repositório;
>
> EXTRAÇÃO - ato de copiar ou retirar dados do repositório em que se encontrava;

> MODIFICAÇÃO - ato ou efeito de alteração do dado;
>
> PROCESSAMENTO - ato ou efeito de processar dados visando organizá-los para obtenção de um resultado determinado;
>
> PRODUÇÃO - criação de bens e de serviços a partir do tratamento de dados;
>
> RECEPÇÃO - ato de receber os dados ao final da transmissão;
>
> REPRODUÇÃO - cópia de dado preexistente obtido por meio de qualquer processo;
>
> TRANSFERÊNCIA - mudança de dados de uma área de armazenamento para outra, ou para terceiro;
>
> TRANSMISSÃO - movimentação de dados entre dois pontos por meio de dispositivos elétricos, eletrônicos, telegráficos, telefônicos, radioelétricos, pneumáticos, etc.;
>
> UTILIZAÇÃO - ato ou efeito do aproveitamento dos dados. (BRASIL, 2020)

Portanto, o tratamento de dados pessoais abrange muito além da coleta e utilização dos dados pessoais, sendo de suma importância que o titular e os agentes de tratamento dos dados se conscientizem.

2.6.3 Princípios da LGPD:

Há 10 princípios que norteiam a atividade de tratamento de dados na Lei Geral de Proteção de Dados (LGPD). Os princípios estão dispostos no art. 6º da legislação e estão relacionados entre si:

I. Finalidade:

Previsto no inciso I do art. 6º da LGPD, o princípio da finalidade é interpretado como a "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades" (BRASIL, 2018).

Desse modo, entende-se que os dados deverão ter a indicação clara e completa das razões que justifiquem a sua coleta. Conforme o Guia do Núcleo de Proteção de Dados do Conselho Nacional de Defesa do Consumidor em parceria com a ANPD e a SENACON, o tratamento dos dados pessoais deve possuir um objetivo específico, claro e, necessariamente, ser informado ao titular. O tratamento não deverá ocorrer objetivando finalidades genéricas e não informadas (BRASIL, 2021).

II. Adequação:

O princípio da adequação está previsto no inciso II do art. 6º da LGPD, e é definido como “compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento” (BRASIL, 2018). Ou seja, o tratamento dos dados deve ser coerente com a sua destinação. A coleta deve ser compatível com a atividade fim do tratamento.

III. Necessidade:

O Princípio da Necessidade está previsto no inciso III do art. 6º da LGPD, que o define como “limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados” (BRASIL, 2018).

Portanto, a coleta de dados deve ocorrer de forma restritiva, devendo ser tratados unicamente dados indispensáveis para atingir a finalidade inicialmente estabelecida.

IV. Livre Acesso:

Disposto no inciso IV do art. 6º da LGPD, o Princípio do Livre Acesso é definido como “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais”. Desse modo, o titular possui o direito de acessar os seus dados pessoais em tratamento, a qualquer tempo e de forma gratuita e facilitada (BRASIL, 2018).

V. Qualidade dos Dados:

O Princípio da Qualidade dos Dados está previsto no inciso V do art. 6° da LGPD, e é definido como: “garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento” (BRASIL, 2018).

Portanto, deve ser garantido que os dados pessoais tratados estejam corretos, precisos e atualizados, não havendo manipulação de dados de qualidade questionável.

VI. Transparência:

Previsto no inciso VI do art. 6º da LGPD, o Princípio da Transparência trata da “garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre

a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial" (BRASIL, 2018).

Garante-se a informação do titular quanto a forma que seus dados estão sendo tratados, bem como sobre os agentes de tratamento envolvidos, respeitando os segredos comerciais e industriais que devem ser preservados.

VII. Segurança:

O Princípio da Segurança, previsto no inciso VII do art. 6º da LGPD, trata sobre a "utilização de medidas 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 difusão" (BRASIL, 2018).

Basicamente este princípio se refere à necessidade de haver medidas relacionadas à segurança da informação, devendo os dados serem protegidos através de medidas técnicas e administrativas, evitando situações ilícitas e acessos não autorizados aos dados armazenados.

VIII. Prevenção:

Previsto no inciso VIII do art. 6º da LGPD, o Princípio da Prevenção trata da "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais" (BRASIL, 2018).

Entende-se quanto a este princípio que deverão ser tomadas providências de proteção aos dados, buscando antecipar possíveis eventualidades relacionadas ao tratamento que ocasionem danos aos titulares.

IX. Não discriminação:

O Princípio da Não Discriminação está previsto no inciso IX do art. 6º da LGPD, e trata da "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos". Este princípio impede que os dados tratados sejam manipulados de forma que prejudique, de forma discriminatória, ilícita ou abusiva, os seus titulares (BRASIL, 2018).

X. Responsabilização e Prestação de contas:

Por fim, o último princípio, chamado Princípio da Responsabilização e Prestação de Contas, está previsto no inciso X do art. 6º da LGPD, e trata sobre a

“responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas” (BRASIL, 2018).

Portanto, espera-se que os agentes de tratamento, controlador e operador, demonstrem todas as medidas tomadas que comprovem o cumprimento e eficácia da lei.

2.6.4 Figuras da LGPD

I. Titular de dados e seus direitos:

O titular de dados pessoais, conforme a LGPD, é a “pessoa natural a quem se referem os dados pessoais que são objeto de tratamento” (BRASIL, 2018). Ou seja, a depender do contexto, todos os indivíduos são considerados titulares de dados pessoais e, portanto, serão protegidos pela Lei Geral de Proteção de Dados.

É assegurado a todos os titulares de dados pessoais possuir a titularidade de seus dados e a garantia de seus direitos fundamentais de liberdade, de intimidade e de privacidade (Art. 17, LGPD). O rol dos direitos dos titulares está previsto no art. 18 da LGPD e os principais direitos assegurados pela lei podem ser observadas na Quadro 1 (BRASIL, 2018).

Quadro 1: Direitos dos Titulares de Dados

Direitos dos Titulares de Dados	**Previsão legal (LGPD)**
Direito de confirmação sobre a existência de tratamento;	Art. 18, inciso I
Direito ao livre acesso aos dados;	Art. 18, inciso II
Direito à correção dos dados caso estejam desatualizados, incompletos ou inexatos;	Art. 18, inciso III
Direito à anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade à Lei;	Art. 18, inciso IV
Direito à exclusão definitiva dos dados pessoais fornecidos a determinada aplicação de internet, através de seu requerimento, ao término da relação entre as partes;	Art. 7º, X
Direito à portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a	Art. 18, inciso V

regulamentação da autoridade nacional, observados os segredos comercial e industrial;	
Direito à eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei;	Art. 18, inciso VI
Direito de requerer a revogação do consentimento a qualquer tempo;	Art. 8º, § 5º
Direito de solicitar informações sobre as entidades com quem houve uso compartilhado de seus dados pessoais e sobre as consequências de não fornecer o seu consentimento para o tratamento de dados pessoais quando o pedem.	Art. 18, inciso VII e VIII

(Fonte: Lei Geral de Proteção de Dados, BRASIL, 2018)

II. Os agentes de tratamento:

Os agentes de tratamento são aqueles que coletam, usam, compartilham ou utilizam de alguma outra maneira os dados pessoais de terceiros. A Lei Geral de Proteção de Dados prevê dois agentes: o controlador e o operador. Além dos agentes, também há o Encarregado, figura diretamente selecionada pelos agentes de tratamento (BRASIL, 2018).

III. Controlador

A Lei Geral de Proteção de Dados (LGPD) traz a figura do Controlador em seu inciso VI do art. 5º, definindo-o como: “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais” (BRASIL, 2018).

O Controlador é, portanto, a pessoa ou empresa que toma as principais decisões quanto ao tratamento de dados, bem como possui o maior interesse neste, e, por tal motivo, é sobre quem recai a maior parte da responsabilização, respondendo por danos patrimoniais, morais, individuais ou coletivos, caso a lei não seja cumprida. As sanções para o descumprimento da lei estão definidas no artigo 52 da LGPD, abrangendo multas, advertência, publicização da infração, bloqueio ou eliminação de dados pessoais (BRASIL, 2018).

O principal papel do Controlador é garantir que a lei e os princípios que a regem estejam sendo cumpridas, devendo prestar contas aos titulares e à Autoridade Nacional de Proteção de Dados (ANPD) sempre que solicitado. Além disso, é o

controlador quem seleciona o Operador e o Encarregado para atuarem em seu nome (BRASIL, 2020).

Também é de responsabilidade do Controlador a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), previsto no inciso XVII do art. 5º da LGPD, onde é definido como a "documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco" (BRASIL, 2018). Basicamente, trata-se de um documento importante para atestar a conformidade da empresa com o tratamento de dados.

Nesse sentido o Guia de Boas Práticas da LGPD (BRASIL, 2020), elaborado pelo Governo Federal, traz que:

> O Relatório de Impacto à Proteção dos Dados Pessoais (RIPD) representa documento fundamental a fim de demonstrar que o controlador realizou uma avaliação dos riscos nas operações de tratamento de dados pessoais que são coletados, tratados, usados, compartilhados e quais medidas são adotadas para mitigação dos riscos que possam afetar as liberdades civis e direitos fundamentais dos titulares desses dados (BRASIL, 2020, p. 33)

A Autoridade Nacional de Proteção de Dados (ANPD), portanto, poderá solicitar a elaboração do RIPD ao controlador, contendo, de acordo com o art. 38 da LGPD, como conteúdo mínimo "a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados" (BRASIL, 2018).

O Governo Federal dispôs em seu Guia de Boas Práticas da LGPD (BRASIL, 2020), uma sugestão dos passos a serem seguidos para a elaboração do relatório, podendo ser adaptado de acordo com a realidade de cada entidade, conforme demonstrado na Figura 3.

I. Operador

A Lei Geral de Proteção de Dados (LGPD) traz a figura do Operador em seu inciso VII do art. 5º, definindo-o como: "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador" (BRASIL, 2018).

Figura 3: Etapas da Fase de Elaboração do RIPD

Figura 1 Etapas da Fase de Elaboração do RIPD

(Fonte: Guia de Boas Práticas da LGPD, BRASIL 2020, p. 34)

O Operador deve realizar o tratamento dos dados pessoais de acordo com as instruções do Controlador e em conformidade com a lei. Caso haja alguma violação à lei, o Operador, junto ao Controlador, também deverá responder por danos patrimoniais, morais, individuais ou coletivos gerados pelo descumprimento da legislação (BRASIL, 2018).

II. Encarregado (DPO)

O Encarregado de Dados é definido pela LGPD (Art. 5º, VIII) como "pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados" (BRASIL, 2018).

Desse modo, o Controlador deve indicar um Encarregado de Dados para facilitar a comunicação entre os agentes de tratamento (Controlador e Operador), os titulares dos dados e a ANPD. A identidade e informações de contato do encarregado devem ser divulgados, para que assim, o titular de dados possa, sempre que achar necessário, requerer seus direitos quanto aos dados pessoais perante ele (BRASIL, 2018).

No exterior, mais especificamente no território da União Europeia, onde rege a GDPR, o Encarregado é conhecido com DPO (*Data Protection Officer*) e, na prática, assim como no Brasil, atua também como suporte na tomada de decisões das empresas, verificando se as atividades estão em conformidade com a Lei Geral de Proteção de Dados.

A figura do Encarregado é obrigatória para todas as empresas, independentemente de seu porte. Porém, a LGPD, em seu artigo 41, estabelece que a ANPD poderá estabelecer normas complementares sobre a definição e as atribuições do encarregado, tratando inclusive sobre hipóteses de dispensa da necessidade de sua indicação, baseado na natureza e no porte da entidade ou no volume de operações de tratamento de dados (BRASIL, 2018).

2.7. PROTEÇÃO DE DADOS DAS MICRO E PEQUENAS EMPRESAS

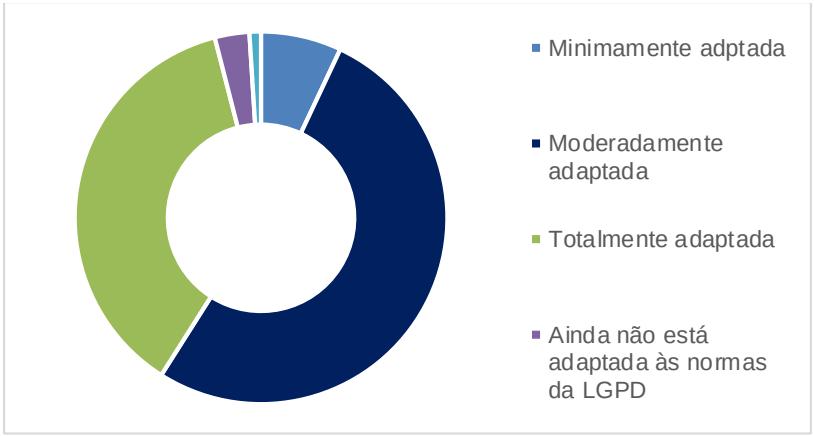
A partir das alterações trazidas pela Lei nº 13.853 de 2019, foram incluídas na Lei Geral de Proteção de Dados (Lei n° 13.709 de 2018), em seu artigo 55-J, algumas competências vinculadas à Autoridade Nacional de Proteção de Dados (ANPD). Dentre essas competências foi definido, no inciso XVIII, que a autoridade estava apta a:

> editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte, bem como iniciativas empresariais de caráter incremental ou disruptivo que se autodeclarem startups ou empresas de inovação, possam adequar-se a esta Lei (BRASIL, 2018).

Os agentes de tratamento de pequeno porte, em razão de seu tamanho, podem apresentar eventuais limitações ao se adequarem à Lei Geral de Proteção de Dados Pessoais (LGPD). Esta dificuldade pode ser observada através de dados captados por uma pesquisa feita pela empresa de *Software* Capterra, entre os dias 16 e 23 de junho de 2021, quase 1 (um) ano após a entrada em vigor da lei. Nesta pesquisa foi mensurado que somente 3 (três) a cada 10 (dez) pequenas ou microempresas no

Brasil se adequaram à LGPD. Ou seja, apenas 37%, das 305 empresas questionadas, disseram estar totalmente adequadas à legislação (GAVA, 2021). Na Figura 4, está representado um gráfico com o resultado da pesquisa.

Figura 4: A adequação das PMEs em relação à Lei Geral de Proteção de Dados Pessoais (LGPD)



(Fonte: adaptado de GAVA, 2021)

Entende-se que a baixa taxa de conformidade das pequenas e microempresas à LGPD, pode ser dada por algumas possíveis causas, dentre as hipóteses estão: a dificuldade em revisar as atividades de toda a empresa; a necessidade de contratação de equipe multidisciplinar de profissionais com conhecimentos em áreas, como direito e segurança da informação; treinamento da equipe; onerosidade excessiva da adequação; entre outros motivos.

De acordo com a pesquisa "LGPD do Mercado Brasileiro", realizada em conjunto pela ABNT, pelos escritórios de advocacia Alvaréz Marsal e SERUR, pela Consultoria HLFMAP e pela *startup* do ramo de privacidade *Privacy Tools*, obteve-se os principais desafios que as empresas enfrentam para adequar-se à LGPD, representados na Tabela 1.

No mesmo sentido da pesquisa realizada pela Capterra, o estudo também constatou que a adequação à LGPD não é prioridade para pequenas empresas, sendo esta preocupação maior às empresas mais suscetíveis a sofrer processos judiciais e danos reputacionais. O ritmo do processo de conformidade com a lei está diretamente relacionado com o tamanho da empresa, visto que são necessários o investimento em recursos com pessoal, tecnologia e *compliance* (GANUT, 2021).

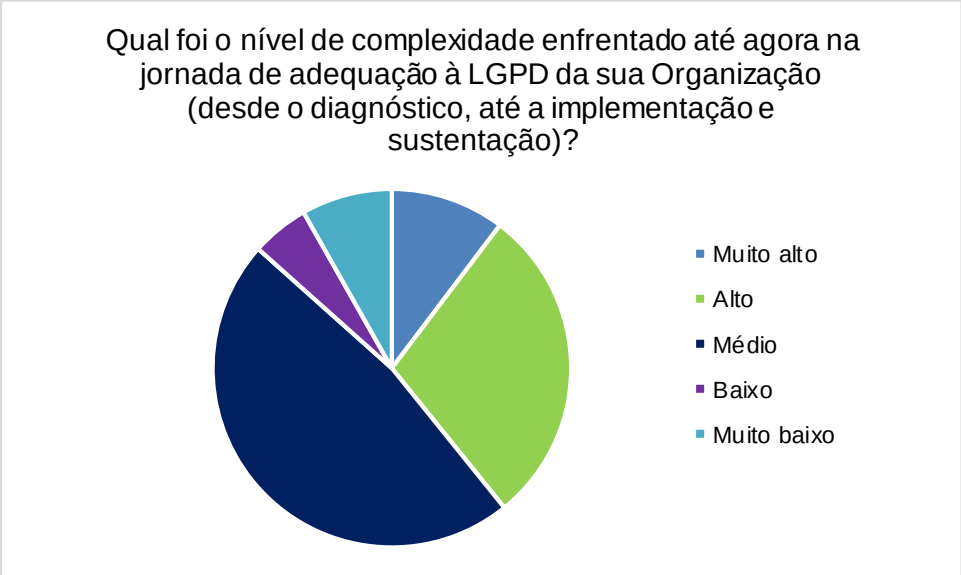
Tabela 1: Desafios para adequação à LGPD

Quais os principais desafios enfrentados/ a enfrentar pela sua Organização para se adequar à LGPD?	%
Ausência de definição e liderança da Proteção de Dados	40,2%
Falta de orçamento	38,1%
Falta de definição clara dos aspectos da lei	36,1%
Falta de conhecimento técnico	29,9%
Falta de referência técnica	27,8%
Outros	14,4%

(Fonte: adaptado GANUT, 2021, p. 7)

As novas regras impostas pela LGPD para o tratamento de dados pessoais, necessitam que haja o investimento de recursos, tanto de pessoal quanto financeiro, das organizações para que ocorra a sua adequação. Devido a esta dificuldade, o porte da empresa, o contexto das operações que a envolvem e a área de atuação, acabam refletindo diretamente na conformidade das empresas à lei, conforme indicado na Figura 5, que representa a relação realizada pela pesquisa "LGPD do Mercado Brasileiro" (GANUT, 2021):

Figura 5: Nível de complexidade na jornada de adequação à LGPD



(Fonte: adaptado GANUT, 2021, p. 6)

2.8. RESOLUÇÃO CD/ANPD Nº 2

Considerando a observância da problemática, envolvendo a adequação das pequenas e microempresas à lei, a ANPD priorizou em sua agenda o estabelecimento de flexibilizações ao texto da LGPD, visando adequar a regulamentação à realidade de empresas de portes menores.

Desse modo, em 30 de agosto de 2021, a ANPD publicou uma minuta de resolução, regulamentando a aplicação da LGPD para microempresas, empresas de pequeno porte e startups, que, em seguida, foi aberta para consulta pública, sendo discutida em audiência pública, nos dias 14 e 15 de setembro de 2021 (BRASIL, 2021).

A Autoridade Nacional de Proteção de Dados (ANPD) trouxe uma série de flexibilizações nesta minuta da resolução, tratando da adequação das normas à realidade das empresas de portes menores que vêm enfrentando dificuldades em entrar em conformidade com os requisitos dispostos na LGPD (BRASIL, 2021).

No dia 28 de janeiro de 2022 a ANPD publicou a Resolução CD/ANPD nº 2 que regulamenta a aplicação da Lei Geral de Proteção de Dados para agentes de tratamento de pequeno porte, trazendo flexibilizações de medidas definidas nos termos da lei (BRASIL, 2022).

Foi definido, em seu artigo 2º, os tipos de agentes de tratamento de pequeno porte abrangidos pela nova regulamentação, são eles (BRASIL, 2022):

I - agentes de tratamento de pequeno porte: microempresas, empresas de pequeno porte, *startups*, pessoas jurídicas de direito privado, inclusive sem fins lucrativos, nos termos da legislação vigente, bem como pessoas naturais e entes privados despersonalizados que realizam tratamento de dados pessoais, assumindo obrigações típicas de controlador ou de operador;

II- microempresas e empresas de pequeno porte: sociedade empresária, sociedade simples, sociedade limitada unipessoal, nos termos do art. 41 da Lei nº 14.195, de 26 de agosto de 2021, e o empresário a que se refere o art. 966 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), incluído o microempreendedor individual, devidamente registrados no Registro de Empresas Mercantis ou no

Registro Civil de Pessoas Jurídicas, que se enquadre nos termos do art. 3º e 18-A, §1º da Lei Complementar nº 123, de 14 de dezembro de 2006;

lll- *startups*: organizações empresariais ou societárias, nascentes ou em operação recente, cuja atuação caracteriza-se pela inovação aplicada a modelo de negócios ou a produtos ou serviços ofertados, que atendam aos critérios previstos no Capítulo ll da Lei Complementar nº 182, de 1º de junho de 2021; e

lV - zonas acessíveis ao público: espaços abertos ao público, como praças, centros comerciais.

Além disso, o artigo 3º define que não serão beneficiadas pelas flexibilizações da resolução, agentes de tratamento de pequeno porte que realizem tratamento de alto risco para os titulares dos dados. A resolução define em seu artigo 4º, que o tratamento de alto risco será caracterizado pela cumulação de no mínimo dois critérios, um critério geral e um critério específico, dentre os a seguir indicados (BRASIL, 2022):

I - critérios gerais:

a) tratamento de dados pessoais em larga escala; ou

b) tratamento de dados pessoais que possa afetar significativamente interesses e direitos fundamentais dos titulares;

ll - critérios específicos:

a) uso de tecnologias emergentes ou inovadoras;

b) vigilância ou controle de zonas acessíveis ao público;

c) decisões tomadas unicamente com base em tratamento automatizado de dados pessoais, inclusive aquelas destinadas a definir o perfil pessoal, profissional, de saúde, de consumo e de crédito ou os aspectos da personalidade do titular; ou

d) utilização de dados pessoais sensíveis ou de dados pessoais de crianças, de adolescentes e de idosos.

De forma geral, as principais flexibilizações trazidas pela Resolução nº 2 da ANPD (BRASIL, 2022) estão apresentadas na Tabela 2.

Tabela 2: Principais Flexibilizações da pela Resolução nº 2 da ANPD

Tema	Resolução
Das obrigações relacionadas aos direitos do titular	**Flexibilização do atendimento** às requisições dos titulares por meio eletrônico ou impresso. "Art. 7º Os agentes de tratamento de pequeno porte devem disponibilizar informações sobre o tratamento de dados pessoais e atender às requisições dos titulares em conformidade com o disposto nos arts. 9º e 18 da LGPD, por meio: I - eletrônico; II - impresso; ou III - qualquer outro que assegure os direitos previstos na LGPD e o acesso facilitado às informações pelos titulares. Art. 8º Fica facultado aos agentes de tratamento de pequeno porte, inclusive àqueles que realizem tratamento de alto risco, organizarem-se por meio de entidades de representação da atividade empresarial, por pessoas jurídicas ou por pessoas naturais para fins de negociação, mediação e conciliação de reclamações apresentadas por titulares de dados."
Do Registro das Atividades de Tratamento	**Simplificação do Registro de Operações de Tratamento** (ROPA ou Inventário), de modo que a ANPD fornecerá modelo simplificado; "Art 9º Os agentes de tratamento de pequeno porte podem cumprir a obrigação de elaboração e manutenção de registro das operações de tratamento de dados pessoais, constante do art. 37 da LGPD, de forma simplificada."
Das Comunicações dos Incidentes de Segurança	Procedimento simplificado de **comunicação de incidentes de segurança**, que contará com regulamentação específica a ser publicada pela ANPD; "Art. 10. A ANPD disporá sobre flexibilização ou procedimento simplificado de comunicação de incidente de segurança para agentes de tratamento de pequeno porte, nos termos da regulamentação específica."
Do Encarregado pelo Tratamento de Dados Pessoais	**Dispensa** da obrigação de nomear um DPO/Encarregado de Tratamento de Dados Pessoais, desde que disponibilize um canal de comunicação com o titular de dados para atender a função do encarregado "Art. 11. Os agentes de tratamento de pequeno porte não são obrigados a indicar o encarregado pelo tratamento de dados pessoais exigido no art. 41 da LGPD."
Da Segurança e das Boas Práticas	Possibilidade de **simplificação da Política de Segurança da Informação**, baseado no risco e escala de tratamento, contendo apenas os itens essenciais para a proteção de dados pessoais contra incidentes ou violações; "Art. 12. Os agentes de tratamento de pequeno porte devem adotar medidas administrativas e técnicas essenciais e necessárias, com base em requisitos mínimos de segurança da informação para proteção dos dados pessoais, considerando, ainda, o nível de risco à privacidade dos titulares de dados e a realidade do agente de tratamento.

	Parágrafo único. O atendimento às recomendações e às boas práticas de prevenção e segurança divulgadas pela ANPD, inclusive por meio de guias orientativos, será considerado como observância ao disposto no art. 52, §1º, VIII da LGPD. Art. 13. Os agentes de tratamento de pequeno porte podem estabelecer política simplificada de segurança da informação, que contemple requisitos essenciais e necessários para o tratamento de dados pessoais, com o objetivo de protegê-los 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 política simplificada de segurança da informação deve levar em consideração os custos de implementação, bem como a estrutura, a escala e o volume das operações do agente de tratamento de pequeno porte. § 2º A ANPD considerará a existência de política simplificada de segurança da informação para fins do disposto no art. 6º, X e no art. 52, §1º, VIII e IX da LGPD.”
Dos Prazos Diferenciados	**Prazo em dobro** para resposta às requisições dos titulares de dados e realização de comunicações em caso de incidentes de segurança, observada a regulamentação própria a ser publicada sobre o tema pela ANPD. “Art. 14. Aos agentes de tratamento de pequeno porte será concedido prazo em dobro: I - no atendimento das solicitações dos titulares referentes ao tratamento de seus dados pessoais; II - na comunicação à ANPD e ao titular da ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares; III - no fornecimento de declaração clara e completa, prevista no art. 19, II da LGPD; IV - em relação aos prazos estabelecidos nos normativos próprios para a apresentação de informações, documentos, relatórios e registros solicitados pela ANPD a outros agentes de tratamento. ” Art. 15. Os agentes de tratamento de pequeno porte podem fornecer a declaração simplificada de que trata o art. 19, I, da LGPD no prazo de até quinze dias, contados da data do requerimento do titular. ”

(Fonte: adaptado da Resolução nº 2 da ANPD, BRASIL, 2022)

De acordo com o art. 6º da Resolução, a dispensa ou flexibilização das obrigações dispostas no regulamento não isenta os agentes de tratamento de pequeno porte do cumprimento dos demais dispositivos da LGPD.

2.9. LGPD EM CLÍNICAS ODONTOLÓGICAS

Em razão de sua natureza, o setor da saúde é um dos mais regulados no Brasil. A exemplo disso, a área da odontologia possui sua doutrina específica, o chamado Código de Ética Odontológica, objeto da Resolução do Conselho Federal de Odontologia - CFO 118, de 11 de maio de 2012. O documento tem como finalidade

regular os direitos e os deveres dos profissionais inscritos no CRO, especialmente do cirurgião-dentista (CONSELHO FEDERAL DE ODONTOLOGIA, 2012).

De acordo com o art. 2º do Código de Ética Odontológica, “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).

Apesar de à princípio não se relacionar a área odontológica com bancos de dados e informações, uma clínica detém diversos tipos de dados pessoais de seus pacientes e funcionários, como por exemplo: nome, CPF, endereço, dados relacionados ao plano de saúde, e, principalmente, dados referentes ao seu histórico de saúde geral e bucal.

Segundo Favaretto *et al.* (2020), questões éticas importantes podem acabar sendo negligenciadas caso seja presumido que os dados de saúde bucal são menos sensíveis do que, por exemplo, dados de saúde mental ou doenças infecciosas estigmatizantes. Ao contrário do que se pensa, os dados de saúde bucal devem ser considerados altamente sensíveis, por haver diversas possibilidades de utilizá-los de forma discriminatória (HOFFMAN, 2009). Além disso, clínicas odontológicas detém outros tipos de dados que também podem ser usados de forma discriminatória, como a discriminação econômica, onde há uma desigualdade de preços apresentados aos pacientes a depender de seu perfil econômico (PEPPET, 2014).

Portanto, entende-se que os dados coletados em clínicas odontológicas podem ser utilizados para fins clínicos, ou seja, com finalidade de agregar no decorrer do tratamento; ou para fins secundários, como pesquisas ou outros fins, como *marketing* (FAVARETTO *et al.*, 2020).

Dentro da área da odontologia, a importância de resguardar os dados pessoais dos pacientes já era tratada anteriormente ao surgimento da Lei Geral de Proteção de Dados (LGPD). O Código de Ética Odontológica (CONSELHO FEDERAL DE ODONTOLOGIA, 2012) já estabelecia regras sobre a coleta e guarda dessas informações, conforme previsto no artigo 9º, que estabelece os deveres fundamentais dos inscritos, tais como:

•. Resguardar o sigilo profissional;

•. Elaborar e manter atualizados os prontuários na forma das normas em vigor, incluindo os prontuários digitais;

•. Resguardar sempre a privacidade do paciente;

•. Registrar os procedimentos técnico-laboratoriais efetuados, mantendo-os em arquivo próprio, quando técnico em prótese dentária.

Portanto, o sigilo do cirurgião-dentista quanto às informações do paciente é fundamento ético inalienável à profissão, e devendo os dados, antes de tudo, serem tratados com máxima confidencialidade.

Por possuir uma quantidade de dados abrangente, o prontuário de um paciente é considerado um dos documentos de maior sensibilidade em posse de uma clínica odontológica. Basicamente trata-se da reunião de todos os arquivos gerados durante o tratamento do paciente. Neste documento, de acordo com o Conselho Federal de Odontologia (CFO), encontra-se desde documentos considerados fundamentais como: ficha clínica, identificação do profissional e do paciente, anamnese, exame clínico, plano de tratamento, evolução do tratamento e possíveis intercorrências; até documentos suplementares como: receitas, atestados, contrato de locação dos serviços odontológicos e exames complementares, todos estes considerados dados sensíveis (OLIVEIRA; YARID, 2014).

Com o avanço da tecnologia nos ambientes empresariais, os prontuários passaram a ser amplamente utilizados em seu formato digital. Favaretto *et al.* (2020), destacam que, devido ao aumento da utilização de prontuários digitais no meio da odontologia, os principais problemas éticos associados a esta nova realidade são justamente aqueles relacionados à privacidade e a manutenção da confidencialidade dos dados e do anonimato do paciente.

Cederberg *et al.* (2014), destacam que os registros odontológicos eletrônicos incluem cada vez mais dados sensíveis e complementares sobre os pacientes, como gráficos dentários automáticos, informações gerais de saúde do paciente, desenvolvimento de planos de tratamento, capturas radiográficas da boca e fotografia intraoral, que podem ser vinculados e analisados para diversos fins sem o consentimento do paciente.

Quanto à utilização de prontuários digitais, Cederbeg *et al.* (2014) afirmam que as questões relacionadas a segurança dos dados são vitais, visto que as informações

confidenciais do paciente podem ser acessadas mais facilmente por terceiros não autorizados, resultando em violação da privacidade e confidencialidade do paciente (CEDERBERG; WALJI; VALENZA, 2014).

Desse modo, tendo em vista a necessidade de manutenção da segurança deste documento, em 27 de dezembro de 2018, foi sancionada a lei nº 13.787, que dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.

Porém, apenas com o surgimento da Lei Geral de Proteção de Dados foi possível unificar a temática de proteção de dados em uma lei específica, ajudando a guiar os profissionais na adequação das clínicas em complementação aos regulamentos já existentes.

Entende-se, de acordo com Franco (2021), que em um consultório, o cirurgião-dentista pode ser classificado como o controlador dos dados, pois compete a este as decisões referentes ao tratamento dos dados pessoais, enquanto o operador seria, por exemplo, a empresa do *software* utilizado pela administração da clínica, pois compete a este a realização do tratamento dos dados pessoais a comando do controlador.

Conforme Franco (2021), o consultório odontológico deve se atentar em garantir aos titulares dos dados, sem nenhuma onerosidade, o acesso aos seguintes direitos previstos na LGPD:

1. Confirmação da existência de tratamento;
2. Acesso aos dados;
3. Retificação dos dados quando houver erro;
4. Anonimização dos dados;
5. Bloqueio e oposição;
6. Portabilidade;
7. Acesso a Informação;
8. Revogação do consentimento;
9. Revisão de decisões automatizadas;
10. Eliminação dos dados.

Ainda segundo Franco (2021), foi estabelecido no Guia de Impacto da LGPD em Consultórios Odontológicos, alguns exemplos práticos de conformidade que podem ser aplicadas no dia a dia de uma clínica, indicados no Quadro 2.

Quadro 2: Exemplos práticos de aplicabilidade da LGPD em clínicas odontológicas

Tema	O que fazer?
1) Marcação de consultas	• Limitar as informações coletadas pela clínica; • Informar ao paciente que a clínica garante que seus direitos sejam respeitados; • Informar a política de privacidade da clínica; • Disponibilizar na clínica a Política de Privacidade
2) Preservar Privacidade do Prontuário	• Limitar as informações coletadas necessárias e uso dos arquivos dos pacientes de acordo com os objetivos bem definidos (monitoramento dos pacientes). • Excluir os arquivos de pacientes sobre alguma informação que tenha excedido o período de retenção recomendado, através de contrato ou resolução de conselho regional. • Estabelecer medidas de segurança apropriadas para o arquivo de pacientes. • A clínica deve garantir que o uso de registros de "pacientes" respeite os princípios fundamentais da proteção de dados pessoais.
3) Exclusão de dados no prontuário	• Qualquer informação, não relacionada ao assunto da consulta do paciente ou que não seja essencial para o diagnóstico ou a prestação de cuidados deve ser excluída. Exemplo: não é relevante coletar dados sobre informações da vida privada do paciente que não sejam clinicamente necessárias (por exemplo, religião do paciente, orientação sexual, orientação filosófica ou política, etc).
4) Tempo de armazenamento dos dados	• É importante levar em consideração os prazos de prescrição para quaisquer ações de responsabilidade e/ ou disposições especiais. Afastada a informação quanto às questões de responsabilidade é imperioso destacar o que é informado na legislação específica sobre o tema de armazenamento de prontuário. A saber: 10 anos a partir da data da última consulta do paciente;
5) Política de Privacidade	• A política de privacidade e termos de uso sempre devem estar acessíveis ao paciente.
6) Uso de Whatsapp	• É permitida para elucidar dúvidas, tratar de aspectos evolutivos e passar orientações ou intervenções de caráter emergencial. • Toda a informação tem absoluto caráter confidencial e não pode extrapolar os limites dos usuários no diálogo, nem tampouco

	podem circular em grupos recreativos, mesmo que composto apenas por dentista.
7) Teleorientação	• Em relação ao exercício da Odontologia a distância, o Conselho Federal de Odontologia (CFO) apresentou um Guia de Esclarecimento sobre a Resolução-CFO nº 226/2020, que regulamenta o exercício da odontologia a distância, publicado no dia 4 de junho de 2020. • É essencial garantir que na plataforma escolhida pelo cirurgião-dentista haja infraestrutura gerenciamento de riscos e requisitos obrigatórios para assegurar o registro digital apropriado e seguro. • Deve ser apresentado ao paciente um Termo de Consentimento para que, por meio de informações claras e objetivas, ele esteja ciente das particularidades que envolvem a telorientação, em especial naquilo que se refere à privacidade e à proteção dos dados.

(Fonte: adaptado de FRANCO, 2021)

Observa-se, portanto, principalmente pela natureza do setor, a importância de as clínicas odontológicas estarem em conformidade com os direcionamentos tratados na LGPD. Desse modo, além de garantir os direitos fundamentais das pessoas titulares dos dados e exercer a manutenção de questões éticas intrínsecas à profissão, o cirurgião-dentista também evitará qualquer implicação de multas ou processos judiciais relativos à questão da proteção de dados.

3. MÉTODOS E TÉCNICAS DE PESQUISA

Levando em consideração os objetivos de pesquisa estabelecidos, nesta seção são descritos os métodos e técnicas de pesquisa utilizadas.

3.1. TIPOLOGIA E DESCRIÇÃO GERAL DOS MÉTODOS DE PESQUISA

A fim de avaliar e compreender o nível de aplicação da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709 de 2018) em empresas de micro e pequeno porte, ou qualquer agente de tratamento de dados de pequeno porte, optou-se pela aplicação do estudo especificamente no nicho de clínicas odontológicas, por haver o tratamento de dados sensíveis (referentes à saúde), em seu cotidiano. Para adentrar neste tema, foi realizada uma pesquisa do tipo exploratória e de abordagem qualitativa, visando a coleta de informações sobre o assunto, para posteriormente realizar uma análise mais detalhada e rigorosa sobre a problemática.

Pesquisas de finalidade exploratórias, de acordo com Gil (2019), buscam esclarecer conceitos iniciais e permitir que estudos posteriores sejam desenvolvidos com maior precisão e definição de problemas e hipóteses. De acordo com o autor, esse tipo de pesquisa busca proporcionar uma visão geral de forma aproximativa sobre determinado tema e geralmente é utilizado quando o tema escolhido ainda não foi muito explorado, dificultando a formulação de hipóteses precisas e operacionalizáveis. Deste modo, essa modalidade de pesquisa se mostrou compatível com o presente trabalho, que aborda um tema recente e ainda não muito estudado em discussões acadêmicas.

Inicialmente, foi desenvolvida uma revisão da literatura sobre dados, segurança cibernética, proteção e privacidade de dados. Neste momento também foram abordados a origem das normatizações de proteção de dados pessoais no Brasil e no mundo e seus respectivos princípios e diretrizes, além da aplicação dessas normas para agentes de tratamento de pequeno porte e, especialmente, em clínicas odontológicas, a fim de que se permitisse um entendimento preliminar a respeito do objeto da pesquisa.

Posteriormente, foi realizada a coleta de dados primários obtidos através de entrevistas semiestruturadas. Na execução de entrevistas, segundo Gerhardt e Silveira (2009), utiliza-se um roteiro previamente estabelecido, com perguntas predeterminadas, objetivando a obtenção de diferentes respostas à uma mesma

pergunta, possibilitando, posteriormente, que sejam comparadas. As entrevistas semiestruturadas não possuem uma estrutura rígida, de forma que se torne uma conversa flexível permitindo que o entrevistado fale livremente sobre o tópico em questão (SILVERMAN, 2011), e o entrevistador tenha a flexibilidade de poder explorar a ordem das perguntas, sua profundidade e a forma em que se apresenta, de acordo com as respostas e circunstâncias do entrevistado (BARROS; DUARTE, 2011).

Nas entrevistas foram analisadas as percepções de cirurgiões-dentistas sobre o impacto da LGPD no contexto da área, bem como questões da aplicabilidade da lei no cotidiano de um consultório odontológico. O questionário de entrevista semiestruturado utilizado nesta pesquisa pode ser conferido na seção de apêndices deste documento.

3.2. PARTICIPANTES DA PESQUISA

Para realizar as entrevistas na profundidade necessária foram selecionados profissionais, cirurgiões-dentistas, que atuam profissionalmente, em clínicas e consultórios odontológicos. A escolha dos participantes, portanto, se deu de forma não probabilística por conveniência, considerando a necessidade de entrevistar indivíduos que possuíssem experiências relacionadas ao cotidiano e à administração de consultórios e clínicas odontológicas, permitindo a obtenção das informações necessárias.

Na escolha dos entrevistados, levou-se em consideração critérios mínimos como ser um profissional que exerça atualmente a profissão de cirurgião-dentista em consultórios ou clínicas odontológicas, sendo excluídos estudantes ainda não formados e profissionais aposentados. Além disso, a amostra de entrevistados é diversificada no sentido de haver empreendedores, proprietários de clínicas, autônomos e profissionais que atuam em clínicas de terceiros. Por conveniência, foram realizadas 10 entrevistas *online* com indivíduos residentes no estado da Bahia e no Distrito Federal.

Considerando que a maior parte dos assuntos abordados na pesquisa tratam de dados de gerenciamento e particularidades profissionais de cada um dos entrevistados, optou-se por segmentar as respostas de forma anônima, utilizando-se uma numeração de 1 a 10 para realizar a identificação de cada entrevistado, incluindo também siglas como, por exemplo, *E01, E02* em diante.

A relação dos entrevistados e suas respectivas informações quanto à função profissional, porte da clínica em que trabalha e estado de residência pode ser observada no Quadro 3.

Quadro 3: 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)

3.3. PROCEDIMENTO DE COLETA E ANÁLISE DE DADOS

Para conduzir a entrevista, foi elaborado um roteiro de pesquisa inspirado em documentos de orientação para conformidade da LGPD em pequenas e microempresas, disponibilizados pela ANPD (BRASIL, 2021) e pela ENISA (ENISA, 2016), além do estudo sobre o impacto e aplicação da LGPD em clínicas odontológicas (FRANCO, 2021). O direcionamento da pesquisa visava o estudo aprofundado de questões consideradas essenciais, pelas autoridades oficiais de proteção de dados, para um agente de tratamento de pequeno porte estar em adequação com a lei. Além disso, o questionário foi segmentado em grupos temáticos pré-definidos, tendo como referência o '*Checklist* de Medidas de Segurança para Agentes de Tratamento de Pequeno Porte', também disponibilizado pela ANPD (BRASIL, 2021). As categorias pré-estabelecidas podem ser observadas abaixo:

- Conhecimento da LGPD;
- Políticas de Segurança da Informação;
- Conscientização e Treinamento interno;
- Controle de Acesso;
- Segurança de Dados Pessoais e Armazenamento;

- Especificações do cotidiano em clínicas odontológicas.

Inicialmente, o roteiro continha em sua totalidade 22 perguntas, que ao longo das entrevistas poderiam ser readaptadas de acordo com a progressão das respostas de cada entrevistado. Dessa forma, possibilitando o aprofundamento e entendimento de questões específicas de cada entrevistado.

As entrevistas foram realizadas individualmente e de forma *online,* através da plataforma de reunião virtual, durante o mês de janeiro de 2023, e totalizaram, em média, uma duração aproximada de 20 minutos. Os áudios das entrevistas foram gravados mediante autorização dos entrevistados com o objetivo exclusivo de realizar a transcrição literal das perguntas e respostas obtidas.

Por fim, optou-se em analisar os resultados através do Método de Análise de Conteúdo de Bardin (2016), uma técnica de análise de dados qualitativos que consiste em 3 (três) etapas principais:

(i) Pré-análise: etapa na qual o pesquisador define o objetivo do estudo e seleciona o material a ser analisado;

(ii) Exploração do material, Categorização ou Codificação: etapa na qual o pesquisador lê o material de forma não sistemática para ter uma compreensão geral;

(iii) Tratamento dos resultados, Inferências e Interpretação: etapa na qual o pesquisador analisa os dados coletados e elabora as conclusões.

Figura 6: Desenvolvimento de Pesquisa de Acordo com Bardin (1977)

(Fonte: MENDES; MISKULIN, 2017)

A etapa de pré-análise, consistiu na transcrição das entrevistas a fim de organizar as informações coletadas e prepará-las para, posteriormente, serem exploradas e analisadas. Neste momento, também foi realizada uma pré-análise do conteúdo, onde foram destacados alguns trechos considerados relevantes para o estudo e alinhados aos objetivos de pesquisa traçados.

Na segunda etapa, de Exploração do Material, para uma melhor visualização dos dados coletados, foi construída uma planilha de análise das informações compartilhadas pelos entrevistados, sendo as respostas coletadas divididas nas categorias pré-estalecidas da pesquisa.

Segundo Bardin (2016), as categorias podem ser criadas *a priori* ou a *posteriori*, isto é, a partir apenas da teoria ou após a coleta dos dados. Optou-se, neste trabalho, pela categorização *a priori*, utilizando as categorias pré-definidas no momento de construção do questionário e que levou em consideração elementos tratados no referencial teórico do trabalho (OLIVEIRA *et al*., 2003).

Portanto, durante a segunda etapa, as respostas dos entrevistados foram organizadas, de acordo com cada grupo temático pré-estabelecido, facilitando a posterior análise de cada categoria individualmente. Nesta etapa, os trechos destacados anteriormente também foram agrupados, facilitando a visualização para posteriormente serem analisados os padrões das informações coletadas e a comparação das respostas obtidas.

3.4. CATEGORIAS ANALISADAS

Serão utilizadas como base 6 categorias definidas para a realização da análise de conteúdo da pesquisa, sendo consolidadas, juntamente com suas respectivas definições, no Quadro 4, 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 4: Categorias de Análise de Conteúdo da Pesquisa

Categoria	Descrição
4.1. Conhecimento da LGPD	Análise do nível de conhecimento e aplicação da lei.
4.2. 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 o planejamento, a implementação e o controle de ações relacionadas à segurança da informação em uma organização.
4.3. 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.
4.4. 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. • 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.
4.5. 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.
4.6. 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.

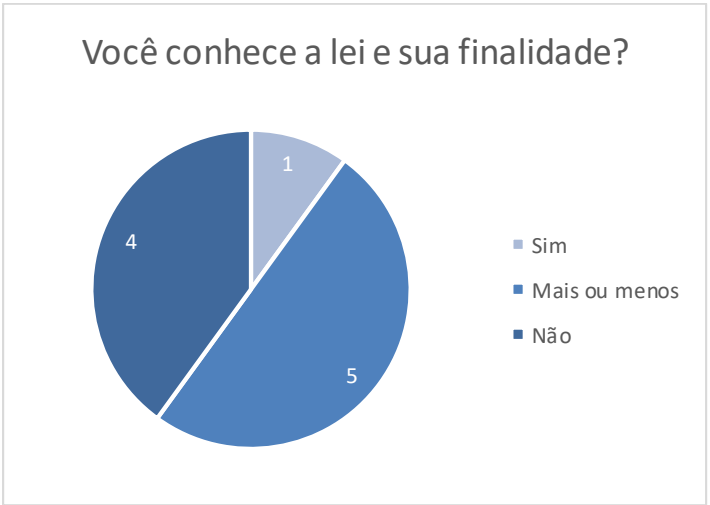
4.1. CONHECIMENTO DA LGPD

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 7.

Figura 7: 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, conforme alguns trechos destacados abaixo:

> *Então eu conheço a lei. Já li um pouco a respeito, mas não cheguei a me aprofundar, então não sei muitos detalhes sobre ela. Entrevistado 01*

> *Sim, superficialmente, mas tenho (conhecimento). Entrevistado 02*

> *Eu conheço superficialmente, né? Eu sei que é uma lei para garantir a privacidade e o sigilo, eu acho, assim do paciente. Mas não conheço a fundo. Entrevistado 05*

> *Eu conheço a lei, não ela propriamente dita, né? Com todos seus detalhes, especificações, mas entendo a importância dela assim também. Entrevistado 07*

> *Assim, conheço, mas bem pouco. Entrevistado 09*

O Entrevistado 03 demonstrou conhecer um pouco mais afundo sobre a lei e destacou que na clínica em que trabalha foram contratados profissionais da área de tecnologia para realizar o treinamento de toda a equipe do consultório para adequação à Lei Geral de Proteção de Dados, conforme o trecho abaixo.

> *A gente tá começando a conhecer na verdade, né? O Dr. contratou uma empresa para fazer o serviço. Eles passaram pra gente mais ou menos, por alto, o que que era. E pediu pra gente procurar entrar nos trâmite (sic) de segurança. Até onde eu entendo é justamente pra segurança dos dados dos clientes, né? [...] pra não vazar para fora da clínica e ficar protegido até com certa hierarquia dentro da clínica, de quem tem acesso as informações. Mas aí o principal é proteger as informações do cliente. [...] Por que a gente tem posse das informações do paciente, como CPF, endereço e exames, né? E dependendo dos exames, a gente tem acesso a laudos. Né e que você não pode passar para frente, né? Passar para algum outro médico sem permissão do paciente. A gente tem, digamos assim, um pouquinho da vida privada da pessoa dentro da nossa empresa. Entrevistado 03*

Alguns entrevistados, entretanto, demonstraram não conhecer absolutamente nada sobre a lei:

> *Não. Não tenho nem noção desta lei. Entrevistado 04*

> *Não, não tenho (conhecimento). Entrevistado 06*

> *Não. Acredita que depois que você falou comigo, eu fui rapidinho no Google para dar uma olhada. Entrevistado 08*

> *Ah, não. Na verdade, eu nunca tinha ouvido falar até então. Entrevistado 10*

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 alguns trechos destacados abaixo:

> *Eu conheço. Pelo menos deve ser bem grave. Entrevistado 02*

> *Acredito que possa ser alguma multa, né? Em cima do faturamento do consultório, alguma coisa assim. Entrevistado 05*

> *Olha, conhecer, eu não sei não, mas eu imagino que tenha um caráter punitivo, né? Em relação a legislação assim, né? Com certeza. Entrevistado 07*

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

Com relação ao nível de conformidade das clínicas onde os entrevistados trabalham, percebe-se que, majoritariamente, os profissionais consideram não estar em conformidade com a lei ou acreditam não estar adequadamente adaptados à esta,

principalmente por desconhecerem os seus termos, conforme demonstra os seguintes trechos:

> *Eu não sei se ela (clínica) está em conformidade com a lei. Em alguns detalhes eu até acho que sim, mas acho que deveria me aprofundar nesse assunto. Entrevistado 01*

> *Eu sei da importância, mas eu não sei se eu estou. Como que faz para estar? É simplesmente saber disso? Eu tenho que entrar em algum local? Entrevistado 02*

> *É, eu sei que é muito importante assim, né? Por conta dessas questões que eu falei de garantir sigilo e privacidade dos dados do paciente, mas como eu nem conheço a fundo, acredito que o meu consultório não esteja dentro do dessas conformidades. Entrevistado 05*

> *Estamos. [...] Claro que a gente não faz da forma, provavelmente que deveria ser feita, né? Porque não é uma coisa que é passado pra gente assim, na graduação, assim é uma coisa que a gente mais aprende pelo senso comum, né? Vivendo a vida. Mas a gente tenta proteger bastante os dados dos pacientes, né? Para que aquilo não saia de dentro do consultório mesmo. Entrevistado 07*

> *Certo, então eu como eu não sabia, não conhecia. Eu não sei lhe dizer se o que eu faço está dentro dessa lei, entendeu? Entrevistado 08*

> *É assim, eu sei no básico, sabe? Mas assim, se eu tiver passando, fazendo alguma coisa ou negligenciando alguma coisa assim, pode passar, né? Muita coisa. Às vezes a gente pode passar despercebido, sim. Entrevistado 09*

Conforme pontuaram Favaretto *et al.* (2020), questões éticas importantes coletadas em clínicas odontológicas podem ser negligenciadas caso seja presumido que os dados de saúde bucal não são tão sensíveis quando dados de outras áreas da saúde humana, ocasionando no desconhecimento da lei.

Tendo em vista, de forma geral, o entendimento superficial acerca do tema da LGPD, foi questionado aos entrevistados quais seriam as possíveis razões desta falta de conhecimento da legislação por parte dos profissionais da área de odontologia. Foram pontuadas diversas razões, dentre elas estão o acesso remoto de terceiros (parceiros) e a dificuldade de leitura da lei em sua integridade (E03); desinteresse por parte dos profissionais da área (E06); negligência (E09); lei inovadora relacionada à digitalização da odontologia e demasiada confiança na utilização dos *softwares* (E07), conforme os trechos abaixo:

> *É, não é muito divulgado e uma questão de dificuldade é justamente a gente trabalhar com alguns parceiros nossos com acesso virtual da máquina, né? Então é esse é um problema onde eu vejo que qualquer parceiro nosso que tenha acesso, a gente vai ter que pedir para eles assinarem um termo onde eles se comprometem. Então assim, a gente acredita que a gente vai achar um pouquinho de resistência em algumas partes. [...] O que eu tenho de adequar? É muita coisa para a gente poder adequar, sim. [...] Acho que muita coisa para você ler" Entrevistado 03*

> *Eu acredito que seja por falta de interesse, tanto de dentistas ou então de quem realmente divulga esse tipo de trabalho, de lei." Entrevistado 06*

> Eu acho que os *dentistas em si são muito negligentes com relação a isso, não dão importância. É uma classe que não dá importância mesmo assim. Até quando acontece algum problema, né? E aí? É, eu acho que a gente foca muito no conhecimento clínico, na saúde, tudo questão do paciente e esquece muito meios legais. Estou falando por mim, me incluindo, né? No caso. Entrevistado 09*

> *Eu acho que primeiro que essa lei veio mais para adequar, né? Nesse mundo digital que estamos vivendo assim, né? Então, é um grande processo. O meio digital, apesar de estar muito tempo na nossa vida, querendo ou não, é uma coisa nova, então acho que sempre vai ter dificuldade para a gente integrar assim. Mas eu acho que é mais contar com softwares assim, sabe? Por que a questão ética de não ter a comunicação né, de espalhar esses dados acredito que todas as profissões já fazem esse embasamento. Mas quando a gente pensa, por exemplo, em coisa de dados, mesmos digital, né? É, por exemplo, na nossa clínica, a gente conta com um software, né? Que é o prontuário digital, né? E ali fica armazenado todos os dados, mas, sinceramente, eu acredito que não há uma busca de se é um software 100% confiável. Quais são as coisas que tem nele que pode evitar, por exemplo, um hacker, alguma coisa do tipo. Entrevistado 07*

Umas 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, conforme os seguintes trechos:

> *Eu não sou totalmente digital ainda. Eu ainda tenho prontuários em papel e tal, né? Então tem assim, eu não tenho muitos dados [...] não, digitalizei todo o meu atendimento, entendeu? Então eu não tive essa preocupação ainda, né? Entrevistado 02*

> *Acho que nem o conselho né, nem a associação (divulga). É, a gente faz muito curso e tudo e às vezes falam dos contratos para a gente fazer, mas como a gente já tem 30, quase 34 anos de formado, desde a da formação, o hábito é fazer o prontuário, a ficha clínica, no papel, né? Entrevistado 04*

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.

O que retrata uma percepção equivocada dos profissionais da área odontológica quando a abrangência da LGPD, devendo ser aplicada em qualquer situação de tratamento de dados pessoais e não apenas nos dados virtuais.

Todavia, a razão mais apontada pelos entrevistados foi o fato de não ser um tema ensinado e apresentado aos profissionais da área, sobretudo, na universidade e nos cursos de pós-graduação e especialização. Os entrevistados trouxeram este ponto, conforme observado nas seguintes falas:

> *Eu acho que é mais assim, pela falta de acesso de, por exemplo, na faculdade, não é muito falado sobre isso. Então eu acho que a falta de informação a respeito assim, de inserir isso na odontologia, sabe? Acho que na faculdade eles não abordam muito sobre isso e a gente começa a vida profissional, fazendo assim, mais ou menos o que a gente acha certo, né? Guardando os prontuários e tal, mais do que como a gente acha do que realmente seguindo essa lei, porque é uma coisa que não é nos dada na faculdade assim. E poucas pessoas da área falam sobre isso. Acredito que em clínica, que tem vários consultórios, isso possa funcionar melhor assim, né? Só que no meu caso, que é um consultório só, é uma cadeira odontológica, não tenho acesso a isso. Entrevistado 05*

> *Olha, eu acredito, até porque, como a gente faz os cursos, não é passado para a gente, né? Porque, normalmente, por exemplo, se eu estou num curso de especialização, vamos supor, eu acho que uma parte deveria ser voltada para isso, né? "Olha, existe". Ou em algum momento da graduação. Eu não sei porque tem muito tempo que eu fiz graduação, né? Então eu não sei lhe dizer se hoje na graduação já é passado isso, para o aluno, que existe essa lei, entendeu? Inclusive eu fiz especialização. Eu tive a parte da odontologia legal, mas não foi falado dessa lei, entendeu? [...] Então eu acho que é mais assim porque dificilmente eu entraria no Google. Se você não tivesse me falado pra ver se existe uma lei, entendeu? Entrevistado 08*

> *Rapaz, eu acho que assim, ó, é um assunto que não sei se todas as faculdades têm, né? Eu tive aula, eu tive, acho que 2 ou 3 matérias, mas eu acho que é muito básico, você passa ali, acaba sendo bem superficial, é muito decoreba. Você decora depois que você vai para uma clínica odontológica, você foca muito mais no conhecimento clínico do que em questão de leis. Entrevistado 09*

> *É, na verdade, eu não faço ideia, eu não tive aula disso na faculdade, pelo menos. Sobre ética e bioética, por exemplo, então talvez estivesse inserida nesse contexto que não é uma matéria oferecida na minha graduação de maneira assim específica, sabe? Então, era uma matéria optativa na faculdade que eu não peguei. Ética odontológica. Era optativa, então não peguei a disciplina, então também não tive contato. Entrevistado 10*

Ao comparar as respostas obtidas com a 'Pesquisa LGPD no Mercado Brasileiro' (GANUT, 2021), tratada no referencial teórico, com as respostas obtidas nas entrevistas, observamos alguns pontos de semelhança e alguns pontos de diferença nos resultados. Enquanto a pesquisa de Ganut, apontou como principais desafios na adequação à LGPD: a ausência de definição e liderança de Proteção de Dados e falta de orçamento. Os entrevistados apontaram questões diferentes como: dificuldades com parceiros; desinteresse por parte dos profissionais da área; negligência dos profissionais e a confiança na utilização dos softwares.

Todavia, alguns pontos se assemelharam, como a falta de definição clara dos aspectos da lei, falta de conhecimento técnico e falta de referência técnica.

4.2. POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

Nesta categoria analisa-se a existência de políticas de segurança da informação - PSI, ou seja, se há diretrizes vigentes nas clínicas que possibilitem o planejamento, a implementação e o controle de ações relacionadas à segurança da informação.

4.2.1 Utilização de Softwares

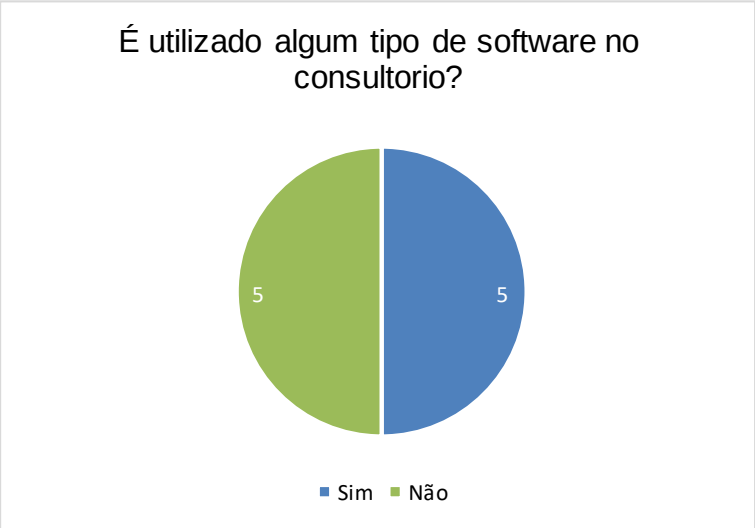
Sabe-se que a transformação digital pode ser observada em todas as esferas do cotidiano das pessoas atualmente, principalmente nos ambientes de trabalho. Apesar do serviço prestado pelos profissionais da área da odontologia ser majoritariamente realizado presencialmente, a diversidade de oferta de softwares exclusivos para administração de consultórios odontológicos, e suas supostas vantagens, fez com que parte dos dentistas migrassem ou iniciassem a migração para o meio digital, sobretudo, quando se refere à utilização dos prontuários digitais.

Conforme pontua Almeida (2016), existem desvantagens, dos prontuários de papel em relação ao eletrônico. Ilegibilidade, ambiguidade, perda frequente da informação, multiplicidade de pastas, dificuldade de pesquisa coletiva, falta de

padronização, dificuldade de acesso e fragilidade do material são algumas delas. Entretanto, a crescente geração de informação sobre os pacientes e a demanda de fácil acesso, num contexto de constante progresso na informática, despertaram o interesse pelo desenvolvimento do prontuário digital.

Na prática, observa-se que metade dos entrevistados de fato utilizam *softwares* em seus consultórios, conforme demonstrado na Figura 8.

Figura 8: Utilização de *softwares* pelos entrevistados



(Fonte: o Autor)

Destaca-se que grande parte dos entrevistados estão iniciando o processo de digitalização de suas clínicas, relatando haver vantagens na organização dos dados dos pacientes. Todavia, também relatam sobre a dificuldade de adequação das clínicas aos *softwares,* que muitas vezes são utilizados em seu formato simples, apenas para armazenamento dos dados coletados em momento de consulta, enquanto outros tipos de dados, como a ficha de identificação contendo CPF, endereço, etc., ficam guardados em outros locais, conforme relatado nos trechos abaixo:

> *Eu trabalho com um software, odontológico, né. Específico para odontologia. E nele a gente tem alguns termos, assim, contratos. Enfim, que a gente usa com os pacientes. Mas não sei se está de acordo com a lei, entendeu? [...] inclusive tem uma parte de contrato que fala bastante sobre dados, imagens e outros detalhes, mas o contrato é muito raso. Não acho que tem todas as informações que deveriam ser passadas. Entrevistado 01*

> *É, eu tenho, eu tenho no computador, um programa chama Easy Dental. Mas eu não coloco nada de dados pessoais assim. Movimentação financeira,*

> *essas coisas de dados da pessoa ali, entendeu? Eu não abasteço, eu uso ele simples, com questionário e para fazer um planejamento, um tratamento, com aqueles característicos, aqueles pontinhos, aqueles dentinhos e tal, depois ir pro paciente, mas eu não tenho toda a vida da pessoa ali não entendeu? Você que tem que fazer o backup. Entrevistado 02*

> *A gente trabalha com Software odontológico, que aí é onde entra aquela parte que eu falei, onde a gente vê um pouquinho de dificuldade, de barreira. Lógico que o programa, eu penso que, também já deve estar conhecendo (a lei). [...] Aí a gente trabalha com isso, um software onde guardar todas as informações de paciente. Entrevistado 03*

> *É, a gente conta com o nosso (software). Não é um específico para proteção de dados, mas querendo ou não é um prontuário digital, então as coisas que ficam lá é pra ficar lá, né? Não é pra ter nenhum vazamento, até porque dentro do próprio software a gente consegue é limitar os acessos de cada profissional que vai estar ali mexendo, né? Então, é mais isso como ajuda, mas nada muito específico. Entrevistado 07*

Observou-se, entretanto, uma relação de perfis ao analisar aqueles que disseram não utilizar *software* em suas respectivas clínicas, pontuando-se principalmente dois perfis, os profissionais autônomos ou que trabalham em clínicas pequenas e os profissionais que já estão formados há vários anos e possuem dificuldade ou não vem necessidade de digitalizar todo o consultório. Alguns relatos podem ser observados abaixo:

> *Não, eu não uso nenhum sistema, eu uso no papel mesmo toda essa parte de prontuário, de dados do paciente, de tratamento é feito no papel e cada um tem o seu prontuário, guardado no consultório mesmo. Entrevistado 05*

> *Não, eu não tenho nenhum, é tudo anotada em ficha clínica, no papel mesmo, mas não tenho nenhum assim. É desse detalhe aí eu não, não tenho conhecimento e aí eu não pratico. Entrevistado 06*

> *Não digital, não. O meu é geralmente é tudo escrito mesmo. É muita papelada, eu preciso mudar isso aí. Entrevistado 09*

A relação de entrevistados e seus respectivos portes e forma de utilização de prontuários pode ser observado no Quadro 5.

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 acorrido (ATHENIENSE, 2019).

Quadro 5: Relação Entrevistado x Porte x Tipo de Prontuário

Entrevistado	Porte	Digital ou Físico
E01	Micro	Digital
E02	Autônomo	Físico
E03	EPP	Ambos
E04	Autônomo	Físico
E05	Micro	Físico
E06	Autônomo	Físico
E07	Micro	Digital
E08	Micro	Digital
E09	Autônomo	Ambos
E10	Micro	Físico

(Fonte: o Autor)

4.2.2 Tratamento de Dados

A ausência de um responsável pelo tratamento de dados nas clínicas também foi observada a partir da análise das entrevistas realizadas. Dentre os 10 entrevistados, apenas um (E03) respondeu ter um responsável pelo tratamento de dados do consultório, sendo ele um administrador da clínica, também responsável pela área financeira e administrativa.

Dentre os outros entrevistados foi comum a resposta que o tratamento de dados era realizado por todas as pessoas que trabalhavam no consultório, não cabendo a responsabilidade à uma pessoa específica.

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.

Observou-se também que em consultórios menores a responsabilidade pelo tratamento de dados da clínica geralmente era compartilhada entre o dono do consultório e um profissional de secretariado, conforme os trechos abaixo:

> *Não, eu sou responsável por todas as anotações clínicas, por todas as observações clínicas. Eu tenho uma secretária, mas o trabalho que ela faz lá é realmente um trabalho operacional, nada técnico. Quem faz as anotações, quem faz os procedimentos sou eu, agora quem guarda os prontuários é ela, raramente eu faço esse trabalho. Entrevistado 06*

> *Eu tenho uma funcionária só, que tem acesso. Ela tem acesso a agenda, porque, na verdade, quando o paciente chega a primeira vez, quem faz o cadastro é ela. Então quem alimenta o sistema é ela, entendeu? Do cadastro e da agenda. Mas, por exemplo, quem alimenta o sistema da evolução do tratamento? Aí sou eu quem faço essa parte, entendeu? Entrevistado 08*

> *Não, não sou eu, é a funcionária da gente que é auxiliar também. Ela tem acesso aos prontuários e ela que administra essa parte, mas a gente não tem nenhum específico para essa função. Entrevistado 10*

De acordo com Telles *et al*. (2021), é proibido facilitar o manuseio e conhecimento dos prontuários, papeletas e demais folhas de observações médicas sujeitas ao segredo profissional, por pessoas não obrigadas ao mesmo compromisso.

Por tal motivo, terceiros agindo em nome do profissional da saúde, como subordinado, como é o caso da secretária, a responsabilidade por seguir a lei é de todos os envolvidos - ela, o profissional da saúde, e a clínica ou o hospital em questão. Isso significa que, se a sua clínica coleta dados ou a sua secretária coleta dados em seu nome, você é o responsável pela preservação, tratamento e armazenamento correto desses dados e pode ser obrigado a indenizar em caso de vazamento que gere prejuízo ao titular do dado (ATHENIENSE, 2019).

Quanto o registro das ações realizadas com os dados pessoais em posse das clínicas, observa-se que no geral ocorre o registro do tratamento dos dados, principalmente nas clínicas digitalizadas, cujos *softwares* ou próprio sistema do computador realiza a anotação automaticamente, conforme os relatos abaixo:

> *Olha, não controlamos, existe por meio do próprio software. Ele mostra pra gente o que foi feito, mas os que foram apagados não, a gente não tem acesso mais, é apagado mesmo. Entrevistado 01*

> *É no próprio o próprio sistema, ele meio que já faz isso automático, né? Entrevistado 07*

Nos demais casos nota-se que normalmente são realizadas anotações à mão nas fichas clínicas e prontuários do paciente, além da utilização de agendas. Neste sentido, quando há alguma adição de informação, também há certo controle dos registros como, por exemplo, a data em que foi inserida aquela informação, conforme retrata o trecho abaixo:

> *Quando inicia o dia, a secretária coloca as fichas clínicas, todas do dia. E cada paciente, se não dá tempo, entre um paciente e outro, no fim do dia a gente escreve no prontuário tudo o que aconteceu, né. O dia, que o procedimento foi feito, o que que aconteceu, então tudo fica anotado diariamente. Entrevistado 04*

> *É, eu coloco assim no prontuário do paciente, a data do início do tratamento, e aí cada dia que eu faço algum procedimento tem a data ao lado, mas só isso. Entrevistado 05*

> *Quando eu vou fazer qualquer mudança igual você falou né, ou alguma mudança ou alguma divulgação, ou que seja, até na questão dos dados ou alguma coisa que já está lá a muito tempo, então geralmente quem faz sou eu. Eu registro. Toda mudança que é feita a quem registra sou eu. Entrevistado 09*

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 exemplo de registro quando há o tratamento de dados pessoais também foi mencionada por uma das entrevistadas (E06), tratando das manipulações de exames e radiografias sob posse do consultório, conforme o trecho abaixo:

> *Por exemplo, quando é preciso que eu devolva um exame radiográfico que é do paciente. Eu faço anotação de que o próprio paciente levou a radiografia ou qualquer exame complementar que esteja em minha posse. Entrevistado 06*

4.3. CONSCIENTIZAÇÃO E TREINAMENTO INTERNO

Também foi abordado durante as entrevistas o tópico relacionado a conscientização e treinamento dos funcionários das clínicas quanto a importância de manter em sigilo os dados pessoais dos pacientes e da responsabilidade que todos os funcionários possuem no tratamento destes dados.

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.

Neste sentido, a grande maioria dos entrevistados relataram que em suas respectivas clínicas há a preocupação de realizar essa conscientização dos funcionários, entretanto, não há nenhuma formalidade com relação a isso. Com exceção do Entrevistado 03, nenhum dos entrevistados informou haver qualquer tipo de treinamento formal para conscientizar os funcionários da importância da proteção de dados e da LGPD.

Um dos pontos abordados pelos entrevistados que explicaria a preocupação dos dentistas, mesmo desconhecendo a LGPD afundo, em conscientizar os funcionários quanto a importância do sigilo está baseado no regimento da odontologia e ética profissional da área, conforme apontado nos trechos abaixo:

> *É, existe uma conversa, né? Já foi passado isso para elas, em relação à importância do prontuário, até por conta do nosso regimento. Isso por conta do nosso CRO. Enfim, a gente sabe que deve guardar o contrato, os contratos, os cadastros por pelo menos 10 anos. Então é isso foi orientado, né? Mas não, não tem, uma regra quanto as edições de prontuários ou exclusão de algum tipo de tratamento, por exemplo, entendeu? Entrevistado 01*

> *Tenho todo cuidado com relação ao sigilo profissional, tudo isso, isso ela sempre foi alertada à secretária, está comigo há 10 anos. Então é assim, eu tenho esse tipo de preocupação, principalmente no que se refere a paciente que faz uso de medicamento controlado todo esse, porque isso é um sigilo, né? Entrevistado 06*

> *Então assim, o que é conversado é a questão da confiabilidade né, a questão dos pacientes, tudo que é conversando lá e que é feito lá fica lá. Com relação à proteção dos arquivos, a chave do escritório também é algo que fica com ela, então ela tem que ter o máximo de cuidado quando eu não estou. Quando ela trabalha com outro dentista, eu deixo a chave do armário também é com ela. [..] É explicado. Entrevistado E09*

A doutrina específica na área da odontologia é chamada de Código de Ética Odontológica, objeto da Resolução do Conselho Federal de Odontologia - CFO 118, de 11 de maio de 2012. O documento tem como finalidade regular os direitos e os deveres do cirurgião-dentista, profissionais inscritos no CRO.

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).

O Código de Ética é algo ensinado na graduação de odontologia, assim como em outras profissões que também possuem códigos de ética específicos. O Código de Ética de Odontologia possui regras rígidas relacionadas ao dever de sigilo quanto aos dados pessoais e sobre manuseio e armazenamento de prontuário de paciente.

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). Tendo isso em vista, a partir da análise das entrevistas foi possível observar que os dentistas, apesar de desconhecerem a LGPD a fundo, acabam se adequando de certa maneira aos termos da lei, devido a atenção dada à privacidade dos dados dos pacientes, salientado no código de ética profissional da área.

4.4. CONTROLE DE ACESSO

O controle de acesso consiste em medidas que garantam que os dados sejam acessados somente por pessoas autorizadas, consistindo em processos de autenticação, autorização e auditoria, descritos abaixo:

> • 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 (BRASIL, 2021, p. 10).

Neste sentido, foi questionado aos entrevistados se suas respectivas clínicas possuem algum controle quanto ao nível de permissividade dos funcionários, consistindo no controle de acesso baseado nas necessidades de cada função aos dados pessoais sob posse da clínica. Os relatos foram no sentido de haver pouco controle sobre o acesso dos funcionários aos dados. Observa-se os relatos nos trechos destacados abaixo:

> *Mais ou menos é, os dentistas têm acesso aos dados, mas não conseguem editá-los, por exemplo. Eles não conseguem editar todos os dados e, principalmente, os dados cadastrais, como endereço, telefone, CEP, CPF, etc. Eles não visualizam, eles só visualizam os procedimentos que eles*

> *precisam ver. Agora os meus funcionários da equipe mesmo, da recepção, comercial, administrativo, esse tipo de coisa. Eles têm sim, acesso a tudo. Entrevistado 01*

> *É, não tem um cadeado no meu arquivo, né? Não tem nada disso não. E o do computador, o programa você abre a qualquer momento. Também não tem senha, não. Entrevistado 04*

> *Isso já tem essa limitação já. A Secretaria, ela vai ter acesso aos dados cadastrais. É, na verdade, a secretária, ela tem bastante acesso assim, mas os dentistas, no geral, eles vão ter acesso ali mais a plano de tratamento e querendo ou não, a gente tem acesso à uma parte importante, né? Que é a anamnese do paciente, né você ali vendo todas questões dele, então a gente também tem acesso a isso (os dentistas), mas a gente fica limitado, por exemplo, aos relatórios que é voltado a marketing, mas não necessariamente a marketing. Acho que entra também uma questão de prevenção, né? Que é essa fidelização do cliente, então, por exemplo, não são todos dentistas que tem acesso a quantos pacientes, por exemplo, faltaram mês passado? Quantos pacientes estão com o orçamento aberto? Quantos pacientes não finalizaram o tratamento? Não são todos que tem esse acesso. Entrevistado 07*

> *Isso de acessar geralmente essas coisas dos pacientes, só eu mesmo e administradora geral do consultório, como se fosse minha gerente né. Ela que gerencia essa parte assim. Ela tem acesso. Somente eu e ela. Entrevistado 09*

> *Todo mundo que trabalha na clínica pode ter acesso aos prontuários. Não fica em nenhum armário fechado, nem nada. Entrevistado 10*

Com relação aos dados de saúde, tendo em vista que os dados pessoais sensíveis, gozam de uma proteção especial pela LGPD, e sugere-se que os agentes de tratamento de pequeno porte que armazenam dados dessa natureza implementem soluções que dificultem a identificação do titular, como as técnicas de pseudonimização (BRASIL, 2021).

Entretanto, na prática foi observado que os entrevistados afirmaram não haver, em suas respectivas clínicas, tratamento especial ou diferente para estes dados em específico. Algumas das razões identificadas para os dados sensíveis serem tratados da mesma forma que os dados não-sensíveis é o fato de estarem todos contidos em um único documento, o prontuário, físico ou digital, sendo um documento essencial e de fácil acesso pelos funcionários do consultório. Observa-se um trecho tratando sobre este tema:

> *Não, não é uma segurança maior, não assim também. É porque, como é uma clínica que envolve saúde, querendo ou não para a gente conhecer o paciente, a gente já vai muito no íntimo dele, né. Então, todos nós precisamos saber disso, até mesmo para saber como vai ser o planejamento, né? Do procedimento, mas não há uma segurança maior assim. Entrevistado 07*

De fato, o único diferencial identificado foi a restrição da autorização de edição dos dados sensíveis por outros funcionários além do próprio dentista que atendeu o paciente, como por exemplo, a secretária, que tem acesso ao prontuário, porém não pode editá-lo, conforme retratado nos trechos abaixo:

> *Não, porque eu tenho o arquivo de fichas, né, de fichas clínicas. E aí o paciente que está agendado no dia, ela (secretária) que vai no arquivo, pega o prontuário e deixa na minha mesa. Mas quem faz as anotações sou eu e quem pede para aguardar sou eu e normalmente, ela só faz, ela tira e guarda. Entrevistado 06*

> *Ela tem acesso a agenda, porque, na verdade, quando o paciente chega a primeira vez, quem faz o cadastro é ela. Então quem alimenta o sistema é ela, entendeu? Do cadastro e da agenda. Mas, por exemplo, quem alimenta o sistema da evolução do tratamento? Aí sou eu quem faço essa parte, entendeu? Entrevistado 08*

Um relato particularmente exemplificador quanto a sensibilidade inerente aos dados de saúde que podem estar em posse de um cirurgião-dentista pode ser observado no trecho abaixo:

> *É a ficha clínica, tem a parte separada só de endereço, identificação e a parte de prontuário de perguntas. E tudo fica numa outra parte, interna da ficha, né? Mas assim, por exemplo, eu tenho paciente que tem AIDS e tudo e só a secretária sabe, lógico, já que tem que paramentar e tudo, mas nenhum outro paciente tem acesso, nem ninguém sabe que ele tem esse tipo de doença. Entrevistado 04*

À exemplo do relato acima, os dados de saúde, sob posse de uma clínica odontológica, portanto, devem ser considerados altamente sensíveis, por haver diversas possibilidades de serem utilizados de forma discriminatória (HOFFMAN, 2009).

Outra situação de sensibilidade mencionada nas entrevistas é a respeito de dados de menores de idade. Quando questionado sobre a razão de não colocar a anamnese na ficha inicial do paciente, o entrevistado 08 respondeu que trata de dados

sensíveis de menores de idades que deveriam ser mantidos em sigilo, conforme o trecho abaixo:

> *Tá, é o nome completo, data de nascimento, endereço, a identidade, CPF, se ele quiser, se ele não quiser a gente não põe. Tá, é só isso mesmo. [...] Ta aí eu já faço uma ficha a parte, inicialmente, que está só no meu computador, né, que é a anamnese, esse eu não coloco lá nesse banco de dados, tá? Ele fica todo num arquivo meu que só eu tenho acesso. Porque assim eu tenho um público muito grande de criança. Entendeu? E eu tenho crianças ainda com problemas, assim é psicológicos, de fazer xixi na cama de água, então isso eu acho que tem que estar particular, sabe? Então assim, 90% do meu público é criança e como eles são menores, eu não posso deixar uma informação. Entrevistado 08*

De fato, dados relacionados à menores de idade devem ser tratados com mais cautela, conforme aponta Atheniense (2019), para os menores de idade, todas as obrigações de informação devem ser prestadas por um de seus representantes legais, responsáveis pelo consentimento expresso.

4.5. SEGURANÇA E ARMAZENAMENTO DE DADOS PESSOAIS

Esta categoria de medidas está relacionada principalmente 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 através de outros dispositivos, como o telefone celular.

Aos entrevistados, foi questionado a forma de é realizado o armazenamento dos dados pessoais de pacientes, bem como quais são as medidas de segurança utilizadas para protegê-las. As respostas podem ser observadas abaixo:

- E01: *Software* – “Por meio desse software na nuvem, né? Então é essa é a segurança que eu tenho. Claro que eu confio na empresa que eu estou utilizando, porque é ela que detém todos os dados, sabe?"
- E02: Físico e *Software* - "Ele fica no sistema, só isso. E o prontuário em papel, aí fica no consultório. Depois eles vão ficando mais velhos no consultório. A gente vai guardando em casa"
- E03: *Software* – “É no próprio software, né? No próprio software, no *Easy Dental*, né, que ele fica nas nuvens, né? Que também é feito backup e apenas 1 pessoa tem acesso à nuvem”

- E04: Físicos
- E05: Físicos
- E06: Físicos
- E07: *Software* - "É, antes a gente fazia os prontuários físicos, né? E aí acho que no meio da pandemia a gente começou a fazer essa transição. É para *software* digital e deixar tudo ali armazenado. Algumas coisas ainda são feitas físicos, mas depois elas são anexadas nesse *software*, né?" Assim a gente ainda tem algumas falhas. Se a gente for pensar assim, é, por exemplo, a gente. Cada procedimento lançado ao dia é deveria ser assinado ao paciente, né? Só que a gente só lança isso no sistema, entendeu? Não há uma assinatura é diária do paciente a cada procedimento assim, né? Isso é um erro."
- E08: *Software* - "O armazenamento do cadastro do paciente, ele é todo feito no software. Quanto à exames, nem todo paciente a gente tem o exame físico. Hoje a gente está procurando evitar muito isso, até porque é muito espaço para você ter que guardar, entendeu? Então é muito melhor você ter isso tudo num banco de dados que você chega ali, qualquer lugar que você tiver você precisar ali, acessar, olhar um exame. Eu, eu acho muito mais fácil do que você pegar ele fisicamente, entendeu? E hoje a gente já tem um sistema de *scanner*, então nem modelo mais a gente faz físico, a gente escaneia a boca do paciente. Está tudo no computador."
- E09: Físico
- E10: Físico - "Na clínica, tudo na clínica. Todo mundo que trabalha na clínica pode ter acesso aos prontuários. Não fica em nenhum armário fechado, nem nada."

A Lei Geral de Proteção de Dados atinge qualquer um que colete dados. Caso o armazenamento dos dados ocorra incorretamente e haja o vazamento ou outro problema, a responsabilidade por armazenamento será diretamente do profissional responsável pelo dado, da clínica ou do hospital (ATHENIENSE, 2019).

Com relação ao tempo de armazenamento dos dados pessoais, as seguintes respostas foram coletadas e organizadas na Tabela 3.

Tabela 3: Relação entrevistado x Tempo de armazenamento de dados

Entrevistado	Tempo de armazenamento dos dados pessoais
E01	10 anos
E02	20 anos
E03	10 anos
E04	10 anos
E05	Não descarta
E06	2 anos
E07	20 anos
E08	10 anos
E09	Não descarta
E10	2 anos

(Fonte: dados da entrevista)

Como pode se observar nas respostas dadas pelos entrevistados, não há um consenso com relação ao tempo de armazenamento dos prontuários odontológicos. Isto porque essa informação pode ser baseada em três fontes diversas. A primeira e maior entre elas (20 anos) provém da Lei 13.787/18, que disciplina a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuários de pacientes.

O Conselho Federal de Odontologia (CFO), por meio do parecer nº 125/92, também aborda a temática, afirmando que a posse do prontuário é do paciente e sua guarda é do profissional devendo ser arquivado, por no mínimo, 10 anos após o último comparecimento do paciente. E por fim, o Código de Defesa do Consumidor (CDC), em seu artigo 27, determina a prescrição em 5 anos de alguma pretensão à reparação de danos causados por fato do produto ou do serviço, iniciando-se a contagem do prazo a partir do conhecimento do dano e de sua autoria (SARAIVA, 2011).

4.6. ESPECIFICAÇÕES DO COTIDIANO EM CLÍNICAS ODONTOLÓGICAS

Nesta categoria são abordados pontos de aplicação das diretrizes da lei direcionadas ao cotidiano de uma clínica odontológica.

4.6.1 Política de Privacidade

Com o surgimento da LGPD, muitas empresas e organizações estão tendo de criar ou revisar suas políticas de privacidade, de forma que torne explícita a forma de

tratamento dos dados pessoais dos clientes. A política de privacidade deve divulgar os aspectos nos quais as informações são tratadas; os tipos de dados que são coletados; de que forma são coletados, a justificativa da atividade de coleta, além de deixar explícito a finalidade de sua realização. Também se os dados coletados serão compartilhados ou não com parceiros ou terceiros, pois o titular dos dados deve ter autonomia no tocante à disponibilização e compartilhamento de suas informações à terceiros (SIEBRA; XAVIER, 2020).

Neste sentido, foi questionado aos entrevistados se, antes da vinculação do paciente com a clínica ou antes da marcação de consulta, os pacientes são informados quanto a Política de Privacidade vigente na clínica. As respostas foram no sentido de haver um termo para assinatura dos pacientes para permitir o uso dos dados existentes no cadastro das informações pessoais e do prontuário, realizada no momento e assinatura do contrato, conforme os trechos abaixo:

> *Não. É porque na ficha, no final da ficha, tem uma autorização, né, que está por escrito e o paciente, respondeu às perguntas e tudo que ele concorda com o diagnóstico e tudo, e ele assina e data. Entrevistado 04*

> *Não antes de marcar a consulta, né? Mas antes da consulta propriamente dita. Porque assim vamos supor, você liga para mim, liga na clínica, aí a gente marca, aí você vai na sua consulta, aí antes do dentista te atender, você vai receber um prontuário, você responde a anamnese e coloca seus dados e no final dessa anamnese tem esse termo. Então você já lê ele também e já assina. Mas, sinceramente, né como a maioria das pessoas fazem, né? Nem lê direito e já assina. Entrevistado 07*

Outro momento destacado pelos entrevistados, no qual é solicitado a permissão dos pacientes para uso de dados, é quanto ao uso de imagens, seja para fins acadêmicos ou para divulgação em alguma rede social:

> *Olha, não, porque nunca ninguém me perguntou você acredita? Nunca foi agora, assim como às vezes eu dou aula e tal [...] se eu precisar de ter que disponibilizar alguma imagem do paciente, aí, sim, aí eu peço autorização e é assinado por ele e assim a gente não mostra a face toda do paciente, né? Sempre com tarjas e tal, para que não seja reconhecido e quando eu estou dando aula, eu sempre peço ao aluno para não fotografar, para não ser reconhecido. Entrevistado 08*

> *Sim, na primeira consulta, na verdade, antes não, mas na primeira consulta, quando a gente conversa com o paciente, a gente fecha ali o tratamento. Eu explico para ele como funciona e tem a parte do contrato também ali que diz. Aí vai depender de como é que ele vai permitir, por exemplo, [...] se pode ser*

> *usado ou não a imagem do paciente. Se o paciente concordar, beleza. Tem lá onde ele assina e tem alguns pacientes também, não concordam. [...] E aí eu explico pra ele [...] tem segurança e isso só quem tem acesso sou eu. [...] se acontecer de alguém entrar e roubar, tem como apagar. [...] Então ele assina pra poder fazer o tratamento, eu preciso. Então é uma coisa que ele meio que não tem escolha. Mas se ele não quiser que use, está lá, a imagem não será usada de jeito nenhum, só vai estar lá no prontuário dele, diante de todas essas leis e tudo mais, de proteção. Mas é repassado na primeira consulta, quando ele fecha o tratamento eu já explico como é que vai ser essa política de uso, né, dos dados? Entrevistado 09*

> *Bom, então eu trabalho com disfunção. Então alguns casos eu converso com o paciente para ele autorizar a divulgação dele no meio acadêmico. Então, se for um caso interessante, porque como eu dou aula, eu às vezes tenho um caso assim mais interessante que outro. Aí eu pergunto pro paciente, mas isso é ao final da do atendimento. Por que aí eu também tenho que avaliar se o caso é passível de ser divulgado ou não, mas sempre no meio acadêmico. Tá? Então é em palestra em seminário em aula, mas nunca em rede social, nada assim. Eu nunca fiz essa divulgação em rede social não. E é sempre pedido a autorização ao paciente. E também eu peço por escrito pra ele assinar que está liberando o uso de imagem. Entrevistado 10*

O Entrevistado 09 pontuou também que o registro e uso de imagens também é uma forma de resguardo tanto para o paciente, quanto para o dentista, visto que evita qualquer tipo de desentendimento do tratamento ou fraude. Este ponto pode ser observado no relato abaixo:

> *Hoje eu já uso o antes e o depois, mesmo que não seja, é postado. [...] Ele não quer que poste, mas ele quer ver o resultado e é importante às vezes, a imagem. Da câmera intra oral mesmo, querendo ou não, você tem armazenamento. Então eu explico para o paciente que é importante que o que eu esteja falando aqui, mostrando para você, uma cárie, não seja eu que esteja vendo, mas que você esteja vendo o que eu estou vendo também para você detectar, até por questão de fraude. O paciente se sente mais seguro quando você está mostrando para ele a necessidade daquele tratamento, não só porque o dentista está falando, eu estou mostrando. Então, querendo ou não, aquela imagem fica registrada no prontuário dele. Entrevistado 09*

Segundo Vanrell (2002), os documentos odontológicos são um conjunto de declarações firmadas pelo profissional e paciente, no ambiente clínico, que podem ser utilizados como prova, no âmbito jurídico. O prontuário é composto de anamnese, consentimento livre e informado, evolução clínica do tratamento, fotografias e radiografias do paciente, cópias de receitas e atestados.

4.6.2 Uso dos dados pessoais para objetivos diversos

Os dados coletados em clínicas odontológicas podem ser utilizados para fins clínicos, ou seja, com finalidade de agregar no decorrer do tratamento; ou para fins secundários, como pesquisas ou outros fins, como por exemplo, *marketing* ou fins acadêmicos (FAVARETTO *et al.*, 2020).

Alguns dos entrevistados informaram que utilizam os dados pessoais dos pacientes para fins comerciais e de *marketing,* para captar clientes e recuperar clientes antigos. Também foi mencionado por outros entrevistados a utilização de dados de paciente para fins acadêmicos, visto que alguns dos entrevistados são professores e mestrandos. Observa-se esta questão nos relatos abaixo:

> *Outra coisa também que a gente usa os dados né para a gente entender qual é o nosso cliente né tipo assim, faixa etária, profissão, gênero, etc., Mas eu acredito que o próprio software já faz a edição e já fica lá, sabe? A gente não tem esse controle além do software. ” Entrevistado 07*

> *Nunca foi agora, assim como às vezes eu dou aula e tal [...] se eu precisar de ter que disponibilizar alguma imagem do paciente, aí, sim, aí eu peço autorização e é assinado por ele e assim a gente não mostra a face toda do paciente, né? Sempre com tarjas e tal, para que não seja reconhecido e quando eu estou dando aula, eu sempre peço ao aluno para não fotografar, para não ser reconhecido. Entrevistado 08*

> *Oh, eu não utilizava, mas há pouco tempo eu fiz um curso de gestão, né? Aí a gente acaba utilizando isso aí para a gente ter ideia mais menos realmente do público alvo para o perfil e na questão de marketing, não, não seria nem de marketing, mas de captação de pacientes. [...] Então assim a gente acaba utilizando na captação daquele mesmo paciente que a gente já tinha feito um tratamento. Então, utilizo dessa forma também." Entrevistado 09*

4.6.3 Prontuários

Segundo Telles *et al.* (2021), o prontuário médico é um documento elaborado pelo profissional de saúde no qual devem constar em sua totalidade os dados relativos ao paciente. No prontuário os itens obrigatórios são: identificação do paciente, anamnese, exame físico, hipóteses diagnósticas, diagnóstico definitivo e tratamento efetuado. Todos os dados devem estar apresentados de forma concisa e organizada.

Neste sentido, foi questionado aos entrevistados quais eram as informações coletadas no prontuário de suas respectivas clínicas. As respostas de todos os entrevistados seguiram um padrão, sendo mencionado os dados cadastrais,

anamnese, dados de saúde geral e bucal e os procedimentos feitos na clínica. Além dos dados relacionados diretamente à identificação e saúde do paciente, alguns entrevistados também mencionaram que dados de pagamento também eram anexados ao prontuário.

As respostas podem ser observadas nos trechos abaixo:

> *Se fuma, se bebe né, a parte da saúde, as doenças que têm, os medicamentos que tem, as alergias que tem. É um prontuário longo. Se para nós da odontologia, eu pergunto se rói unha, que tipo de alimentação né, vai para a parte da nutrição; sono com bruxismo; inflamação gengival, então é são muitas perguntas da saúde geral do paciente. Pressão. É doenças que já teve, né? Medicação que toma, então é bem extensa para saber da vida, do paciente, dos hábitos. E aí depois é que a gente vai fazer o exame clínico na cadeira. [...] No cabeçalho que começa a idade, às vezes que atendo criança, pai, mãe é né o responsável, endereço, CPF, se tem e-mail. Entrevistado 04*

> *Eu pego os dados básicos, né? Então assim o nome, CPF, endereço, telefone, a indicação, da onde vem, estado civil. E aí eu, essa primeira parte inicial e depois eu entro pra parte de saúde mesmo, né? Então pra eu ver, ter um panorama geral da saúde, se tem alguma doença, se está fazendo algum acompanhamento médico, se está tomando alguma medicação, se tem alergia a algum medicamento ou anestesia. E depois eu entro para a parte de saúde bucal específica assim. Quantas vezes escova o dente? Como que está a higiene bucal de forma geral? Então eu divido assim, primeiro os dados pessoais, depois o estado de saúde geral e depois focado na saúde bucal. Entrevistado 05*

> *É, eu faço primeiro as anotações de dados pessoais, daí eu faço uma anamnese com relação ao estado geral de saúde do paciente, se tem alguma alergia, se se é diabético, hipertensos, essas doenças que geralmente são doenças crônicas, mas que tem alguma relevância no tratamento odontológico. [...] e pergunto, também se faz uso de contínuo de algum medicamento. Porque isso tem relevância no tratamento. Antidepressivos, anti-hipertensivos e afins. Então isso eu tenho tudo anotado no prontuário do paciente, que é quando eu faço a coleta de dados, de observações clínicas, então tudo isso está dentro, está no prontuário dele. Entrevistado 06*

> *Dados cadastrais, né? [...] Endereço, gênero, idade, contato, né? Como eu posso me comunicar com a pessoa? Se a pessoa tem convênio, se não. Dados de saúde geral, dados de saúde bucal e alguns dados, também mais como a pessoas se sente numa vertente estética, né? Tem uma parte nosso prontuário que fala mais com uma pessoa, vê o sorriso, se ela gosta, se ela está satisfeita com o sorriso dela, né? E aí, por exemplo, se ela está satisfeita, então a gente não vai oferecer nenhum procedimento estético, mas aí se ela coloca que não está satisfeita aí embaixo, tem as opções: mudaria a cor, mudaria sei lá o quê, e aí já consegue designar a consulta melhor assim. E aí é isso. Aí depois no prontuário tem o termo, tem as anotações do que observei no exame clínico. E é isso. Antigamente a gente tinha uma parte de pagamento né. Por exemplo, a paciente foi lá hoje, fez a limpeza e foi tanto. Ai a gente já anotava isso no pagamento. Mas esse controle financeiro hoje*

> *em dia a gente faz pelo software também, né? Já não entra no prontuário. Entrevistado 07*

> *Nome completo, RG, telefone, e-mail e a gente faz anamnese, né? Ali do paciente que é o exame clínico, exame físico. É, eu faço a coleta de imagens quando eu usar a Câmera intraoral. Basicamente, é isso. E autorização né, assinatura de contrato mais autorização. Entrevistado 09*

> *O básico. Queixa principal, histórico médico, histórico odontológico é descrição da doença atual. É, a gente faz também um exame físico para avaliar o que que a gente encontra na hora no paciente, exame físico, exame clínico, tudo o básico mesmo. Ai, com relação aos dados do paciente, nome, telefone, endereço, forma de contato, se por e-mail e tal, essas coisas. Entrevistado 10*

4.6.4 Utilização de dispositivo móveis e redes sociais

Um dos pontos que merece destaque quando se trata de digitalização dos consultórios é o uso do WhatsApp e de outros aplicativos de troca de mensagens por profissionais da saúde. Segundo Atheniense (2019), uma mensagem contendo dados clínicos sensíveis de um paciente ao ser enviada equivocadamente a terceiros, sem prévia autorização ou meios de proteção, é ilegal. Nos casos de clonagem de contas, um eventual vazamento também é de responsabilidade do profissional ou clínica, pois são considerados controladores dos dados pessoais dos pacientes, o que resulta na responsabilidade legal por eventuais falhas de segurança dos aplicativos e no risco de penalidades (ATHENIENSE, 2021).

Nesse sentido, foi questionado aos entrevistados quanto ao uso do WhatsApp pelas clínicas e pelos dentistas e sua finalidade. As respostas foram principalmente no sentido de utilização para marcações e outras questões administrativas. Além de ser utilizado para realização do contato direto entre dentista e paciente após um pós-operatório, por exemplo. Algumas das respostas podem ser observadas abaixo:

> *A gente tem WhatsApp somente para a clínica. E os dentistas não têm acesso a eles, né? Somente nós da equipe. A finalidade é somente agendamento e no máximo uma informação ou outra que o paciente pergunte. Mas qualquer outra informação mais detalhada não é passada pelo WhatsApp. Entrevistado 01*

> *Sim, é o que a gente usa mais é marcação e retorno. Entrevistado 02*

Esse WhatsApp fico no telefone só para confirmação de consulta, desmarcar, né? De toda a conversa, a paciente paga e manda o comprovante de pagamento pra questão do WhatsApp. Então, assim eu, o fixo, ficou quase que inutilizado. A gente usa muito o WhatsApp pra conversar com o paciente. Entrevistado 04

É uso o WhatsApp para marcar as consultas, né? E pra passar algumas informações, por exemplo, um paciente que nunca foi. E aí ele perguntou qual o valor da primeira consulta? Aí eu passo pelo WhatsApp, pega os dados básicos. Assim, o nome só, o nome completo. E faço a marcação de consulta, e aí depois que eu atender o paciente, né? Aí eu passo o valor, tudo mais, eu uso o WhatsApp e fazer esse controle das consultas só. E algumas vezes, passo o orçamento também. É, eu geralmente passo na consulta, presencial, mas tem vezes que também eu mando pelo WhatsApp e também o número de quando eu não consigo falar ou sei lá por alguma razão. Eu não falo pessoalmente ou então assim a pessoa pede para mandar pelo WhatsApp, eu mando os dados bancários, né? Se for fazer um Pix, alguma coisa assim. Entrevistado 05

O WhatsApp é para é marcar consulta, cancelar consulta. É, e eu passo as vezes para o paciente pelo WhatsApp, ou às vezes por e-mail. O planejamento do caso dele. Entrevistado 06

Bom, o WhatsApp, ele é bem utilizado lá na clínica, né? A gente possui 2 números de WhatsApp, um que fica com a secretária, então é utilizado para a marcação de consultas. É pegar esses dados cadastrais, né? Às vezes, previamente, a pessoa chegar de fato a clínica, né? A gente já pega convênio, essas coisas, o motivo da consulta também. E, eventualmente, uma comunicação, assim, mais direta, né? E também como envio de materiais, por exemplo, se você foi à clínica hoje e você tem um implante e ninguém tinha te orientado até hoje sobre como tem que ser realizada essa higienização do implante. Aí a gente faz, né? Tipo um documento, né? Explicando como tem que ser bonitinho e a gente dá a opção pro paciente, se ele quer esse material físico ou se envia pelo WhatsApp. A maioria prefere pelo WhatsApp, então a gente já envia. É, às vezes passagem de orçamentos também, né? A gente tem. E quem tem acesso a esse da secretária, sinceramente, só ela, a gerente, que é a dona da clínica, e eventualmente, eu assim, sabe, mas no meu caso é mais para uma comunicação pós-operatória, sabe? Diretamente com o paciente, tanto para não usar meu número pessoal, né? E também, se caso a secretária esteja ocupada, então eu já pego o celular e mando como foi, se melhorou a dor? Então está tudo certo, mais assim. E aí tem um segundo número de WhatsApp, da gerente, né? E aí, é meio que tudo assim, para a captação de pacientes, resolver às vezes um feedback que que foi passado, às vezes também para essa questão de fluxograma entre a equipe mesmo, mais pra isso. Entrevistado 07

Ó, a gente usa bastante WhatsApp. O WhatsApp, pra mim serve tanto por eu ter contato com o paciente e alguns pacientes tem inclusive o meu WhatsApp pessoal, a depender do tratamento, eu preciso ter, né? Esse contato direto com o paciente. Eu utilizo nessa função questão de clínica né saber como é que está o meu paciente após um procedimento, então eu, como dentista, eu utilizo lá dessa forma. Minha secretária, ela parte de agendamento, ela utiliza para poder fazer agendamento. Hoje em dia é muito difícil o paciente ligar, gente é raridade eu atender o telefone, a secretária, atender telefone. Geralmente está tudo ali no WhatsApp, no telefone da clínica. E aí a gente utiliza também para a remarcação, agendamento, contato do paciente. E

> *também para a questão de marketing e captação de pacientes. Como te falei, alguns dados, a gente usa, "deixa eu ver aqui esse paciente tem não sei quanto tempo, vamos mandar mensagem". Às vezes a gente faz algumas campanhas no consultório. Esse mês é o mesmo clareamento. Eu sei quem, então a gente tem ali, através daqueles dados, um perfil de pacientes que a gente sabe que a gente pode mandar mensagem para ver se aquele paciente, se ele retorna para clínica. [...] primeiro contato pelo WhatsApp, ligação é só se o paciente não responder as mensagens. Entrevistado 09*

> *Utilizamos para Marcação de pacientes, confirmação, tudo isso. [...] às vezes manda nota fiscal pro pelo WhatsApp também essas coisas. Entrevistado10*

Durante a pandemia do Covid-19, o Conselho Federal de Odontologia (CFO), através da Resolução 226/2020 apresentou algumas modalidades de teleodontologia, incluindo: o telemonitoramento no intervalo entre consultas – acompanhamento a distância dos pacientes que estejam em tratamento –, com registro obrigatório em prontuário de toda e qualquer atuação realizada nestes termos; bem como a teleorientação realizada por Cirurgião-Dentista com o objetivo único e exclusivo de identificar, por meio de questionário pré-clínico, o melhor momento para a realização do atendimento presencial. (CONSELHO FEDERAL DE ODONTOLOGIA, 2020).

Neste quesito, de atendimento à distância, parte dos entrevistados responderam que não realizam foram negativas ou no sentido de ser realizadas apenas consultas orientativas e de urgência, conforme é observado nos relatos abaixo:

> *É, nós não costumamos fazer isso. Na odontologia. É muito difícil a gente conseguir algum diagnóstico por meio da tecnologia. Enfim, mas alguns casos, para diagnóstico é rápido, a gente utiliza.. Entrevistado 01*

> *Sim, já, porque às vezes manda uma foto, não é? Quebrou um dente. "O que que eu faço?" Às vezes a gente dá uma orientação, a medicação, um analgésico, uma coisa que eu preciso tomar às vezes, né? É Que dentista é difícil se resolver pelo WhatsApp, mas a uma orientação, né? Onde procurar? No fim de semana, uma emergência, essas coisas. Às vezes até no nosso próprio pessoal, tem paciente que procura. Entrevistado 04*

> *Não, eu não realizo atendimento a distância, nunca realizei, porque a Odonto assim é muito prático, né? Muito assim, tem que ter a prática. Sempre tem que fazer algum procedimento, alguma coisa assim. Então eu nunca fiz atendimento à distância. Entrevistado 05*

> *Já fiz muito pouco. Por exemplo, eu tenho paciente diplomata que mora no exterior. Aí ele, se ele tem alguma dúvida, alguma intercorrência que está do*

> *outro lado do mundo, aí eu vou orientando o meu paciente. Até que ele possa ter um atendimento, que geralmente eles esperam, quando não é uma urgência, para vir ao Brasil, né? Mas eu faço esse atendimento nesse sentido de orientação. Entrevistado 06*

> *Olha, não é um padrão e sinceramente, eu acho que nunca ocorreu de precisar fazer uma com uma tele consulta assim. [...] Como eu trabalho na área de DTM, eventualmente, eu ainda faço umas tele consultas, mas não é nada vinculado a uma clínica e, sinceramente, geralmente é mais como um auxílio a outro profissional, né? Sei lá, às vezes um amigo meu está tendendo alguém e a mandíbula está travada, e aí não tem como eu estar no consultório, ele está precisando de ajuda e a gente faz essa tele consulta, sabe? É uma coisa bem rara, mesmo de acontecer. Entrevistado 07*

> *Não faço não, eu posso assim responder, por exemplo, se o paciente começou a desencadear alguma dor, alguma coisa e ele entrar em contato comigo, eu oriento. Entrevistado 08*

> *Olha, assim, atendimento em si a distância eu nunca consegui fazer. É, eu já atendi assim. Eu já tive algumas urgências, pacientes que já me mandou mensagem é com alguma dúvida, se ia ao consultório, se ia ao hospital, alguma urgência assim, nesse caso, sabe? De perguntar e aí eu ter que ou algum paciente que fez alguma estripulia após alguma cirurgia e eu não tô. Mas basicamente é muito difícil né na odontologia a gente conseguir fazer algum atendimento. [...] porque a gente é muito manual mesmo. A gente precisa botar a mão na massa para poder fazer. Não dá para fazer por. Entrevistado 09*

> *Então eu já realizei mais fora do âmbito do consultório. Então, durante a pandemia, alguns pacientes disfunção, eu atendi online. Mas foi uma coisa muito pontual. Depois da pandemia, daquele processo todo, eu nunca mais fiz, né? Entrevistado 10*

Por fim, com relação ao uso do Instagram, a maior parte dos entrevistados informaram não utilizar para fins profissionais e aqueles que disseram utilizar, o fazem apenas como meio informativo, conforme apresentado no Quadro 6.

Quadro 6: Relação Entrevistado x Utilização de Instagram

Entrevistado	Utilização de Instagram?
E01	Sim
E02	Não
E03	Não
E04	Não
E05	Sim (informativo)
E06	Não
E07	Sim (informativo)
E08	Não

E09	Não
E10	Não

(Fonte: Dados entrevistas)

5 CONCLUSÃO

Na Sociedade da Informação, contexto atual em que a sociedade está imersa, no qual há um constante crescimento na relevância das informações no dia a dia das pessoas, é ampliado a importância do correto gerenciamento dos dados, de forma segura e responsável. As inovações na área da Tecnologia da Informação, têm contribuído para que dados e informações sejam processados e armazenados com agilidade, sendo necessário às empresas buscarem as melhores alternativas para viabilizar o processamento e o armazenamento desses dados e informações (JUAREZ; ALVES; NUNES; DE OLIVEIRA, 2022)

As clínicas odontológicas devem executar de forma segura o processamento e armazenamento de dados de pacientes, principalmente pela natureza do setor, envolvendo dados de saúde, estes classificados pela LGPD como dados sensíveis. A conformidade com os termos inseridos na LGPD, portanto, além de garantir os direitos fundamentais dos titulares dos dados e exercer a manutenção de questões éticas intrínsecas à profissão, o cirurgião-dentista também evitará qualquer implicação de multas ou processos judiciais relativos à questão da proteção de dados.

Visto a importância de aplicação da LGPD neste nicho de clínicas odontológicas, que geralmente são empresas de porte micro ou pequeno ou constituído por profissionais autônomos, optou-se pela realização da pesquisa nesta área, a fim de avaliar e compreender o nível de aplicação da Lei Geral de Proteção de Dados (Lei nº 13.709 de 2018) no cotidiano.

Para avaliar o tema proposto, foi realizada uma pesquisa do tipo exploratória e de abordagem qualitativa, visando a coleta de informações sobre o assunto, para posteriormente realizar uma análise mais detalhada dos dados coletados. Foram selecionados 10 profissionais, cirurgiões-dentistas, que atuam profissionalmente, em clínicas e consultórios odontológicos. O roteiro foi elaborado tendo como base documentos de orientação para conformidade da LGPD em pequenas e microempresas, disponibilizados pela ANPD (BRASIL, 2021) e pela ENISA (ENISA, 2016), além do estudo sobre o impacto e aplicação da LGPD em clínicas odontológicas (FRANCO, 2021).

O questionário foi segmentado em grupos temáticos pré-definidos, tendo como referência o ‘Checklist de Medidas de Segurança para Agentes de Tratamento de

Pequeno Porte', também disponibilizado pela ANPD (BRASIL, 2021). As categorias pré-estabelecidas foram: Conhecimento da LGPD; Políticas de Segurança da Informação; Conscientização e Treinamento Interno; Controle de Acesso; Segurança de Dados Pessoais e Armazenamento; Especificações do cotidiano em clínicas odontológicas.

Quanto ao conhecimento da LGPD, observou-se, à princípio que a grande maioria dos entrevistados detinha nenhum ou pouco conhecimento quanto à lei e sua finalidade. 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, os entrevistados responderam de forma unânime no sentido de desconhecimento total desta resolução. Mesmo quando explicado aos entrevistados sobre o assunto tratado pela resolução, foi observado que os entrevistados ainda assim não tinham conhecimento da existência de flexibilizações da LGPD para empresas de pequeno porte, demonstrando a pouca divulgação desta matéria.

Ao analisar as respostas acerca das razões para o conhecimento da LGPD ainda ser limitado na área da odontologia, umas das principais razões mencionadas foi pela ainda vasta utilização de prontuários físicos (em papel) e utilização limitada de softwares e tecnologia nos respectivos consultórios. Observou-se que grande parte das clínicas, principalmente as de menor porte, ainda organizam os documentos em formato físico ou estão no começo da transição para a utilização de documentos digitais e *softwares*. E observou-se também que os profissionais da área possuem uma equivocada visão de que a LGPD é aplicada apenas no tratamento de dados digitais.

Entretanto, a razão mais apontada pelos entrevistados foi o fato de não ser um tema ensinado e apresentado aos profissionais da área, sobretudo, nas universidades e nos cursos de pós-graduação e especialização. Alguns dos entrevistados inclusive eram mestres em suas respectivas especializações e apontaram o desconhecimento da lei e a omissão dos cursos em informar a importância da LGPD.

A ausência de um responsável pelo tratamento de dados nas clínicas também foi observada a partir da análise das entrevistas realizadas. 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.

Ainda de acordo com Telles *et al.* (2021), não se deve facilitar o manuseio e conhecimento dos prontuários médicos sujeitas ao segredo profissional, por pessoas não obrigadas ao mesmo compromisso, fato que é observado no cotidiano dos entrevistados.

Quanto a conscientização e treinamento dos funcionários das clínicas quanto a importância de manutenção do sigilo dos dados pessoais dos pacientes, a grande maioria dos entrevistados relataram que em há a preocupação de realizar essa conscientização dos funcionários, entretanto, não há nenhuma formalidade com relação a isso. Através da análise dos pontos abordados na entrevista, acredita-se que a razão da preocupação dos dentistas neste ponto, mesmo desconhecendo a LGPD e suas formalidades, está relacionado ao regimento de ética profissional da área odontológica que aborda o tema do sigilo profissional.

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).

Entretanto, na prática foi observado que os entrevistados afirmaram não haver, em suas respectivas clínicas, tratamento especial ou diferente para estes dados em específico. Algumas das razões identificadas para os dados sensíveis serem tratados da mesma forma que os dados não-sensíveis é o fato de estarem todos contidos em um único documento, o prontuário, físico ou digital, sendo um documento essencial e de fácil acesso pelos funcionários do consultório.

Com relação às políticas de privacidade, as respostas foram no sentido de haver um termo para assinatura dos pacientes para permitir o uso dos dados existentes no cadastro das informações pessoais e do prontuário, realizada no momento e assinatura do contrato,

Os dados coletados em clínicas odontológicas podem ser utilizados para fins clínicos, ou seja, com finalidade de agregar no decorrer do tratamento; ou para fins

secundários, como pesquisas ou outros fins, como por exemplo, marketing ou fins acadêmicos (FAVARETTO *et al*., 2020).

Alguns dos entrevistados informaram que utilizam os dados pessoais dos pacientes para fins comerciais e de *marketing*, para captar clientes e recuperar clientes antigos. Também foi mencionado por outros entrevistados a utilização de dados de paciente para fins acadêmicos, visto que alguns dos entrevistados são professores e mestrandos.

Por fim, quanto ao uso do WhatsApp e das teleconsultas pelos entrevistados, as respostas foram principalmente no sentido de utilização para marcações e outras questões administrativas para o WhatsApp e uso principalmente para orientação e atendimentos de urgências para as teleconsultas.

De modo geral, através da análise completa da base teórica, da legislação e dos dados coletados na presente pesquisa, observou-se que a transformação digital vem sendo realizada nas clínicas odontológicas, sobretudo, após a pandemia do Covid-19. Entretanto, os profissionais da área ainda se veem perdidos quanto à aplicação da Lei Geral de Proteção de Dados no cotidiano das clínicas. Observou-se que o sigilo dos dados é mantido tendo como base principal o Código de Ética da área odontológica, não havendo muita influência da LGPD e de suas sanções que, de modo geral, são desconhecidas pelos profissionais.

Os resultados da presente pesquisa contribuem para o aprimoramento da proteção de dados pessoais dos pacientes e para o desenvolvimento de melhores práticas de gestão de dados nas clínicas odontológicas. Além disso, a pesquisa também pode auxiliar na conscientização dos profissionais da área sobre a importância da LGPD e em sua adaptação às mudanças na legislação.

Além dos profissionais da área odontológicas, os profissionais que trabalham com a implementação da LGPD em empresas, sejam eles advogados, administradores ou profissionais de segurança cibernética, também podem ser beneficiados com as análises desta pesquisa, tendo em vista a descoberta de alguns vácuos na implementação desta lei.

No âmbito acadêmico, sugere-se o aprofundamento de algumas questões tratadas de forma mais superficial nesta pesquisa, sendo possível a investigação e estudo mais aprofundado de questões levantadas pelos entrevistados.

REFERÊNCIAS

ADJEI, Joseph K. **Monetization of Personal Identity Information: Technological and Regulatory Framework**. IEEE Computer Society Washington, Washington DC/EUA, 14 dez. 2015. Disponível em: https://www.researchgate.net/profile/Joseph_Adjei3/publication/325142873_Monetization_of_personal_digital_identity_information_Technological_and_regulatory_framework/links/5be99f48a6fdcc3a8dd1b2a1/Monetization-of-personal-digital-identity-informationTechnological-and-regulatory-framework.pdf. Acesso em: 02 dez. 2022.

ALMEIDA, Maria José Guedes Gondim; FIGUEIREDO, Bárbara Barros; SALGADO, Akayana Calegaro; TORTURELLA, Igor Moreira. **Discussão ética sobre o prontuário eletrônico do paciente.** Revista Brasileira de Educação Médica, v. 40, n. 3, jul./set. 2016. https://doi.org/10.1590/1981-52712015v40n3e01372015. Disponível em: https://www.scielo.br/j/rbem/a/JgjRCsnkb9qwjdg7JJZxVyq/abstract/?lang=pt. Acesso em: 30 ago. 2021.

ANDRADE, Diego de Calasans Melo; MOURA, Plínio Rebouças de. **O direito de consentimento prévio do titular para o tratamento de dados pessoais no ciberespaço**. Revista de Direito, Governança e Novas Tecnologias, Goiânia,v.5, n.1, p.110-133, Jan/Jun de 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. ISO/IEC 27000. **Informação Tecnológica. Segurança da Informação. Técnicas e metodologias**. São Paulo, 2016.

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://www.alexandreatheniense.com.br/lgpd-e-o-setor-de-saude-orientacoes-para-medicos-hospitais-e-clinicas/. Acesso em: 25 mar. 2023.

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

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

BIONI, Bruno Ricardo; SILVA, Paula Guedes Fernandes da; MARTINS, Pedro Bastos Lobo. **Intersecções e relações entre a Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação (LAI): análise contextual pela lente do direito de acesso**. Coletânea de Artigos da Pós-graduação em Ouvidoria Pública. Cadernos Técnicos da CGU, Brasília, DF, v. 1, n. 1, p. 1-28, 2022. Disponível em: https://revista.cgu.gov.br/Cadernos_CGU/article/view/504/284. Acesso em: 25 jan. 2023.

BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção aos dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP, 2015. Disponível em: http://gomaoficina.com/wp-content/uploads/2016/07/XEQUE_MATE_INTERATIVO.pdf. Acesso em: 06 mar. 2020

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/l10406compilada.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-e-protecao-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://www.gov.br/anpd/pt-br/documentos-e-publicacoes/arquivos-de-documentos-de-publicacoes/guia-do-consumidor_como-proteger-seus-dados-pessoais-final.pdf. 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: guia-vf.pdf (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/l13709.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/l13787.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://www.gov.br/anpd/pt-br/assuntos/noticias/inclusao-de-arquivos-para-link-nas-noticias/minuta_de_resolucao___aplicacao_da_lgpd_para_agentes_de_tratamento_de_pequeno_porte.pdf. 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/-/resolucao-cd/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.

CARVALHO, Victor M. B. de**. O Direito Fundamental à Privacidade ante a Monetização de Dados Pessoais na Internet: apontamentos legais para uma perspectiva regulatória**. 2018. Dissertação (Mestrado em Direito) – Programa de Pós-Graduação em Direito, Universidade Federal do Rio Grande do Norte, Natal, 2018. Disponível em: https://repositorio.ufrn.br/handle/123456789/26851. Acesso em: 4 fev. 2022.

CASTELLS, Manuel. **Internet Galaxy: Reflections on the Internet, Business, and Society**. 1ª ed. Rio de Janeiro: Editora Zahar, 2003.

CEDERBERG, R.; WALJI, M.; VALENZA, J. **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.

COHEN, Max E. **Alguns aspectos do uso da informação na economia da informação**. Ciência da Informação, vol. 31, n. 3, 2002. Disponível em: http://www.scielo.br/scielo.php?pid=S0100-19652002000300003&script=sci_abstract&tlng=pt. Acesso em: 4 fev. 2023.

CONSELHO FEDERAL DE MEDICINA**. Resolucão nº 1.638, de 18 de iulho 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%83O/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.puc-rio.br/14038/14038_4.PDF. Acesso em: 4 fev. 2023.

DE SOUZA, F. L.; ALVARES, L. M. A. de R.; NUNES, R. R. **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

DONEDA, Danilo. **A Proteção de Dados Pessoais nas Relações de Consumo: para Além das Informações Creditícias.** Caderno de Investigações Científicas. v. 2. Brasília, 2010. **Disponível em:** manual-de-protecao-de-dados-pessoais.pdf (www.gov.br). Acesso: 25 mar. 2023.

DONEDA, Danilo. **O Direito Fundamental à proteção de dados**. In: MARTINS Guilherme Magalhães. Direito Privado e Internet. São Paulo: Atlas, 2014

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-security-of-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.

FIUZA, César**. Direito civil: curso completo**. 13. ed. rev. e atual. Belo Horizonte: Del Rey, 2009.

FLORES, Paulo Roberto Moglia Thompson. **Direito Civil: Parte Geral: Das Pessoas, Dos Bens e Dos Fatos Jurídicos**. 1. ed. Brasília, DF: Gazeta Jurídica, 2013.

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://22478337.fs1.hubspotusercontent-na1.net/hubfs/22478337/1623247301ebook-_Dental_Office_LGPD_na_Odontologia_V02_1.pdf_1.pdf?utm_medium=email&_hsmi=230723372&_hsenc=p2ANqtz--7xUjWIysI-ALBwth1CvHTT4rJYgkq1kTnVYHAi8yAR9sVN2TplocOWJUjBawJUuA5RowlwCcoVzmMxQo9YtK35njumA&utm_content=230723372&utm_source=hs_automation. Acesso em: 06 mar. 2023.

GANUT, Marcos. **Pesquisa LGPD no Mercado Brasileiro**. [S.l.]: Alvarez e Marsal, 2021. Disponível em: https://www.alvarezandmarsal.com/sites/default/files/2021-11/E-book%20LGPD%20no%20Mercado%20Brasileiro.pdf. Acesso em: 04 fev. 2023.

GARRITANO, Célia Regina de Oliveira; JUNQUEIRA, Felipe Holanda; LOROSA, Ely Felyppy Soares; FUGIMOTO, Mavara Sanae; MARTINS, Wallace Hostalacio Avelar. **Avaliacão 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.

GARTNER IT GLOSSARY. Disponível em: <<https://www.gartner.com/en/information-technology/glossary/big-data>> Acesso em 20 dez. 2022

GAVA, Marcela. **LGPD para PME: minoria está totalmente adequada à legislação**. Capterra, 13 ago. 2021. Disponível em: https://www.capterra.com.br/blog/2153/lgpd-pme. Acesso em: 04 fev. 2023.

GERHARDT, T. E.; SILVEIRA, D. T. **Métodos de Pesquisa**. Porto Alegre: Universidade Federal do Rio Grande do Sul, 2009.

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

HOFFMAN, S. **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.

IRAMINA, Aline. **GDPR v. GDPL: Strategic Adoption of the responsiveness approach in the elaboration of Brazil´s General Data Protection Law and the EU General Data Protection Regulation.** Law, State and Telecommunications Review, [S. l.], v. 12, n. 2, p. 91–117, 2020. Disponível em: https://periodicos.unb.br/index.php/RDET/article/view/34692. Acesso em: 25 jan. 2023.

JUAREZ, D. ; ALVES, C. A. de M. ; NUNES, R. R ; DE OLIVEIRA, R. M. **. Benefícios e Riscos do Uso da Computação em Nuvem no Setor Público: Uma análise baseada em artigos disponibilizados em bases dados acadêmicas 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, Vicosa, 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

MARINO, Tiago**. Dado x Informação x Conhecimento**. 2020. Disponível em: https://tiagomarino.com/classes/EXTRAS/material/5%20%20Dado%20x%20Informa%C3%A7%C3%A3o%20x%20Conhecimento.pdf. Acesso em: 25 mar. 2023.

MATTORD, Hebert J.; WHITMAN, Michael E. **Roadmap for Information Security for IT and Infosec Managers**. 2012. Disponível em: https://books.google.com.br/books?hl=pt-BR&lr=&id=zYMKAAAAQBAJ&oi=fnd&pg=PR3&dq=(WHITMAN%3B+MATTORD,+2012).&ots=13iV1flJMe&sig=jOdvVYpCtzEMX19LABeM6ic4xOA#v=onepage&q&f=false. Acesso em: 04 fev. 2023.

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

MENDES, Rosana Maria; MISKULIN, Rosana Giaretta Sguerra. **Análise de Conteúdo como uma Metodologia**. Cadernos de Pesquisa, São Paulo, v. 47, n. 165, 2017. Disponível em: https://doi.org/10.1590/198053143988. Acesso em: 04 fev. 2023.

MITTELSTADT, B.D.; FLORIDI, L. **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.

MUHLEN, Élen Andreia Von; SCHNEIDER, Eliete Vanessa. **O Direito a Privacidade à Luz da Lei Geral de Proteção de Dados Pessoais (LGPD)**. Salão do Conhecimento UNIJUÍ, v. 6, n. 6, 2020. Disponível em: https://publicacoeseventos.unijui.edu.br/index.php/salaoconhecimento/article/view/18153.

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, Eliana de; ENS, Romilda Teodora; FREIRE ANDRADE, Daniela B. S.; MUSSIS, Carlo Ralph de. **ANÁLISE DE CONTEÚDO E PESQUISA NA ÁREA DA EDUCAÇÃO**. Revista Diálogo Educacional, Curitiba, v.4, n.9, p.11-27, maio/ago. 2003. Disponível em: https://www.redalyc.org/articulo.oa?id=189118067002. Acesso em: 8 fev. 2023

OLIVEIRA, D. L. de; YARID, S. D. **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, S.R**. 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.

ROCHFELD, J. **Como qualificar os dados pessoais? Uma perspectiva teórica da União Europeia em face dos gigantes da Internet**. Revista de Direito, Estado e Telecomunicações, Brasília, DF, v. 10, n. 1, p. 61-84, 2018.

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/opiniao-lgpd-saude-importancia-lei-1378718. Acesso em: 25 mar. 2023.mar-21/opiniao-lgpd-saude-importancia-lei-1378718

SALGADO LEME, R.; BLANK, M. **Lei Geral de Proteção de Dados e segurança da informação na área da saúde.** Cadernos Ibero-Americanos de Direito Sanitário, *[S. l.]*, v. 9, n. 3, p. 210–224, 2020. DOI: 10.17566/ciads.v9i3.690. Disponível em: https://www.cadernos.prodisa.fiocruz.br/index.php/cadernos/article/view/690. Acesso em: 25 mar. 2023.

SARAIVA, A. S. **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.

SERPRO - SERVIÇO FEDERAL DE PROCESSAMENTO DE DADOS. **Linha do tempo da proteção de dados pessoais e da Lei Geral de Proteção de Dados Pessoais, no Brasil.** Disponível em: https://www.serpro.gov.br/lgpd/menu/arquivos/linha-do-tempo-1/view. Acesso em: 9 fev. 2023.

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

SIEBRA, S. de A.; XAVIER, G. A. C. **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, V. de M. D. ; ALBUQUERQUE, R. O. ; NUNES, R. R ; MOTA, G. A. . **Strategic Assessment of Cyber Security Contenders to the Brazilian Agribusiness in the Beef Sector**. INFORMATION , v. 13, p. 1-19, 2022.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (Regulamento Geral sobre a Protecão de Dados, RGPD**). Jornal Oficial da União Europeia, L 119/1, 4 mai 2016. Disponível em: https://gdpr-info.eu. Acesso em: 25 jan. 2023

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://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex:31995L0046. Acesso em: 06 abr. 2023.

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

VIANA DA SILVA, Marcos; 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. Disponível em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/18. Acesso em: 09 fev 2023.

VITAL, Antonio. **Protecão de dados: informacões pessoais movimentam nova economia digital mundial** – Bloco 4. Rádio Câmara, Câmara dos Deputados, Brasília, 05 mar. 2018. Disponível em: https://www2.camara.leg.br/camaranoticias/radio/materias/REPORTAGEMESPECIAL/554146-PROTECAO-DE-DADOS-INFORMACOES-PESSOAISMOVIMENTAM-NOVA-ECONOMIA-DIGITAL-MUNDIAL-BLOCO-4.html. Acesso em: 02 dez. 2022.

YAMAGATA, Nicolas. **Monetizando você e seus dados com a função de inteligência**. Intelligence Hub, 05 nov. 2017. Disponível em: https://www.intelligencehub.com.br/monetizando-voce-e-seus-dados-com-funcao-de-inteligencia/. Acesso em: 10 jan. 2023.

ZIRABA, A. & OKOLO, C. **The impact of information technology (IT) policies and strategies to organization's competitive advantage**. Munich, Germany: GRIN Verlag, 2018. Disponível em: https://dl.acm.org/citation.cfm?id=3239838. Acesso em: 15 jan. 2023.

APÊNDICES

Apêndice 1: Questionário de Entrevista

LGPD: Geral

1. Você conhece a Lei Geral de Proteção de Dados e tem entendimento da finalidade da lei?

2. Você conhece as consequências da inobservância da LGPD?

3. A clínica em que você trabalha está em conformidade com a LGPD? Você sabe a importância das clínicas odontológicas estarem em conformidade com a LGPD?

4. Quais são as maiores dificuldades no processo de adequação à lei? E caso desconheça, porque você acha que é pouco difundido no meio?

5. Você tem conhecimento da Resolução nº2 da ANPD/2022, que trata da aplicação flexibilizada das diretrizes da LGPD para pequenas e microempresas?

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

6. Em sua clínica é utilizado algum tipo de software que assegure a segurança dos dados pessoais?

7. Existe alguém responsável pelo tratamento de dados da empresa?

8. Realizam o registro de tratamento de dados?

CONSCIENTIZAÇÃO E TREINAMENTO

9. Em sua clínica há a preocupação de conscientizar os funcionários, via treinamentos, sobre as suas obrigações e responsabilidades relacionadas ao tratamento de dados pessoais, conforme disposto na LGPD?

10. Nesse sentido, quais são os principais direcionamentos?

CONTROLE DE ACESSO

11. Há o uso de algum sistema de controle de acesso aplicável a todos os usuários, com níveis de permissão na proporção da necessidade de acesso de cada um a cada tipo de dado pessoal?

12. Com relação aos dados sensíveis (de saúde) há algum tratamento diferente?

SEGURANÇA DOS DADOS PESSOAIS ARMAZENADOS

13. Como são armazenados os dados? Quais são as medidas de segurança utilizadas para protegê-los?

ESPECÍFICOS DA ÁREA DE ODONTOLOGIA

14. Antes da marcação de uma consulta, os pacientes são informados quanto a política de privacidade da clínica?

15. Além de utilizar os dados dos pacientes para realização de cadastros e para o tratamento em si, na sua clínica vocês utilizam os dados para algum outro propósito? Por exemplo, mapeamento do perfil dos pacientes ou algo nesse sentido.

16. Quais informações são coletadas no prontuário do paciente?

17. Os prontuários dos pacientes são físicos (em papel) ou é utilizado algum software administrativo para clínicas odontológicas?

18. Que medidas são tomadas para preservar a privacidade do prontuário dos pacientes?

19. Por quanto tempo a clínica armazena os dados dos pacientes?

20. O *Whatsapp* é utilizado pela clínica e pelos dentistas? Para qual finalidade? Que tipo de dado normalmente é compartilhado nesta plataforma?

21. Há atendimentos a distância? Se sim, como são realizados?

22. Utilizam Instagram em sua clínica? Em caso positivo, informam ao paciente quando vão publicar algum tipo de dado, como por exemplo, imagens.