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

GUILHERME HOROVITZ LAHMANN

Lei Geral de Proteção de Dados Pessoais para agentes de tratamento de dados de pequeno porte: análise em consultórios de psicologia.

Brasília – DF
2023

Guilherme Horovitz Lahmann

Lei Geral de Proteção de Dados Pessoais para agentes de tratamento de dados de pequeno porte: análise em consultórios de psicologia.

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

Professor Orientador:

Professor Doutor Rafael Rabelo Nunes

Brasília – DF

2023

Guilherme Horovitz Lahmann

Lei Geral de Proteção de Dados Pessoais para agentes de tratamento de dados de pequeno porte: análise em consultórios de psicologia.

A Comissão Examinadora, abaixo identificada, aprova o Trabalho de Conclusão do Curso de Administração da Universidade de Brasília do (a) aluno (a)

Guilherme Horovitz Lahmann

Prof. Dr. Rafael Rabelo Nunes
Professor-Orientador

Prof. Aldery Silveira Júnior
Professor-Examinador

Prof.Virgínia M. Dantas Trinks
Professor-Examinador

Brasília, 17 de setembro de 2024

Dedico este trabalho à minha amada família, em especial, minha mãe e meus saudosos avós, que por tanto tempo me deram todo o suporte para que eu pudesse chegar até aqui.

AGRADECIMENTOS

Sou muito grato às pessoas que me colocaram em contato com os profissionais entrevistados. Sem elas, este trabalho não seria possível.

Aos profissionais entrevistados, gostaria de registrar meus mais profundos e sinceros agradecimentos. Sua generosidade ao compartilhar conhecimento, tempo e experiência contribuiu imensamente para o sucesso deste trabalho.

Agradeço muito à Universidade de Brasília (UnB), pelo aprendizado, suporte e experiências proporcionadas durante todo este longo percurso.

Agradeço ainda ao meu orientador, Rafael Rabelo Nunes, por sua orientação.

"Privacidade não é sobre ter algo a esconder, mas sobre ter o direito de controlar o que os outros sabem sobre você." - Edward Snowden

RESUMO

Diante do avanço tecnológico e da crescente importância das informações na sociedade contemporânea, tornou-se imprescindível o manejo seguro e responsável dos dados. Em resposta a esse panorama, diversas legislações foram concebidas globalmente para salvaguardar o direito à privacidade dos indivíduos. No Brasil, a Lei Geral de Proteção de Dados Pessoais (LGPD), instituída pela Lei nº 13.709, de 14 de agosto de 2018, emerge como marco regulatório nesse contexto. No entanto, os agentes de tratamento de dados de menor porte, sejam eles controladores ou operadores, podem enfrentar desafios específicos de conformidade devido às suas dimensões, cabendo à Autoridade Nacional de Proteção de Dados (ANPD) facilitar essa adaptação por meio de adequações normativas. Especial atenção deve ser dedicada à adequação à LGPD por parte das empresas atuantes na área da saúde, dada a natureza sensível e íntima dos dados relacionados à saúde que são manipulados diariamente. Este estudo propõe-se a avaliar o grau de implementação da Lei Geral de Proteção de Dados Pessoais em consultórios de psicologia - representados por profissionais da área - no Distrito Federal. Para alcançar esse objetivo, foram conduzidas entrevistas em profundidade com 10 profissionais, psicólogos, cujas respostas foram analisadas utilizando-se a técnica de análise de conteúdo. Como resultado, foram identificados e categorizados os principais aspectos relativos à conformidade nesse contexto específico: Conhecimento da LGPD; Desenvolvimento de Políticas de Segurança da Informação; Sensibilização e Treinamento Interno; Controle de Acesso; Garantia da Segurança dos Dados Pessoais e Armazenamento; e Aspectos Cotidianos em Consultórios de Psicologia. A análise dessas categorias revelou que, mesmo considerando a natureza sensível da área, há ainda escasso conhecimento sobre a LGPD, sendo que muitos profissionais desconhecem seus aspectos fundamentais. Os resultados obtidos apresentam relevância tanto para os profissionais da psicologia quanto para as autoridades e demais profissionais envolvidos na aplicação da legislação de proteção de dados pessoais no país.

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

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

LGPD – Lei Geral de Proteção de Dados

ANPD – Autoridade Nacional de Proteção de Dados

GDPR – *General Data Protection Regulation*

ISO – *International Organization for Standardization*

CFP – Conselho Federal de Psicologia

SGSI – Sistema de Gestão de Segurança da Informação

MPE – Micro e Pequenas Empresas

TICs – Tecnologias da Informação e Comunicação

CM – Customização em Massa

DPO – *Data Protection Officer*

CA – *Cambridge Analytica*

TCLE – Termo de Consentimento Livre e Esclarecido

E01, E02 – Entrevistado 01, Entrevistado 02

BBC – British Broadcasting Company Ltd

CPF – Cadastro de Pessoa Física

CEP – Código de Endereçamento Postal

CID – Confidencialidade, Integridade e Disponibilidade

ENISA – *The European Union Agency for Cybersecurity*

IEC – *International Electrotechnical Commission*

NBR – Norma Brasileira

SUS – Sistema Único de Saúde

PSI – Política de Segurança da Informação

CEPP – Código de Ética Profissional do Psicólogo

PEP – Prontuário Eletrônico do Paciente

PFP – Prontuário Físico em Papel

SUMÁRIO

1. INTRODUÇÃO

Dado o contexto atual em que a sociedade se encontra, é evidente o crescente destaque das informações e a necessidade de gerenciar dados de maneira segura e responsável. Os avanços em Tecnologia da Informação têm facilitado o processamento e o armazenamento de dados de forma ágil, exigindo que as empresas busquem as melhores opções para garantir a eficiência nesse processamento e armazenamento (Juarez; Alves; Nunes; De Oliveira, 2022).

A sociedade está sendo transformada pela onda da Transformação Digital, caracterizada pelo avanço das tecnologias no cotidiano das pessoas, especialmente nas Tecnologias da Informação e Comunicação (TIC). Estamos na Era dos Dados e da Informação, onde o uso crescente de plataformas digitais aumentou a importância das informações. Esse panorama de avanço tecnológico e ampliação dos bancos de dados trouxe inovações que impactam diretamente na melhoria da qualidade, na produtividade e na redução de custos, elevando o valor dos produtos e serviços oferecidos. Dessa forma, essa nova realidade se tornou essencial no dia a dia e na economia da sociedade contemporânea (De Souza; Alvares; Nunes, 2022).

À medida que os fluxos de informação se intensificam devido ao desenvolvimento tecnológico, novas oportunidades de armazenamento, uso e manipulação de informações pessoais estão surgindo, afetando diretamente o 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).

A Segurança da Informação, assim, passou a ser um elemento crucial para garantir a privacidade e a proteção dos dados pessoais dos indivíduos. Ela engloba as ações realizadas para proteger as informações processadas em um sistema contra acesso não autorizado, uso indevido, divulgação, interrupção, modificação, leitura, inspeção, gravação ou destruição. O modelo mais adotado para guiar a gestão da segurança da informação em uma organização é conhecido como a tríade CID, que inclui a confidencialidade, a integridade e a disponibilidade das informações (União Europeia, 2016).

A privacidade é um direito universal e está diretamente ligado ao direito da personalidade da pessoa humana , de acordo com sua previsão constitucional (art 5º, inciso X), onde é 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". O código civil também protege a privacidade humana, no artigo 21, 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”.

As legislações voltadas para a proteção de dados têm como objetivo assegurar que a pessoa física esteja ciente de quem possui seus dados, quais informações estão sendo mantidas e como essas informações estão sendo utilizadas, visando proteger sua privacidade (Nakamura; Formigoni; IDE, 2020).

No Brasil, a lei que rege a proteção de dados é a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709, de 14 de agosto de 2018). Apesar de formulada em 2018, a LGPD entrou em vigor apenas em 18 de setembro de 2020 e passou a gerar sanções apenas em 2023, visando oferecer tempo para que os prestadores de serviço que lidam com dados se adequassem à lei. A LGPD regulamenta a obtenção e o tratamento de dados pessoais, e sua principal finalidade é proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme estabelecido na Constituição Federal de 1988 (Brasil, 2020).

A criação de uma lei que protege os dados pessoais criou um precedente para a criação de uma 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, além de implementar e fiscalizar o cumprimento da LGPD no Brasil (Brasil, 2020).

Levando em conta esta problemática, a ANPD priorizou o estabelecimento de flexibilizações ao texto da LGPD, visando adequar a regulamentação à realidade de empresas de menor porte. Desse modo, em 28 de janeiro de 2022 foi publicada 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).

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).

Dentre as empresas de micro e pequeno porte, os consultórios de psicologia representam um setor da saúde e devem se atentar à privacidade dos pacientes.

Embora, à primeira vista, não pareça haver uma conexão direta entre a psicologia e o uso de bancos de dados, um consultório de psicologia lida com diversos tipos de dados pessoais e dados pessoais sensíveis de pacientes, e/ou funcionários. Por isso, é importante que os consultórios cumpram as diretrizes estabelecidas pela LGPD. Dessa forma, além de assegurar os direitos fundamentais dos titulares dos dados e manter os padrões éticos da profissão, o terapeuta também evitará problemas relacionados a multas ou processos judiciais relacionados à proteção de dados - ou a falta dela.

1.1. Formulação do problema

Um levantamento feito pela consultoria Alvarez & Marsal, em parceria com a ABNT, apontou que o Brasil não tem a cultura da privacidade para manter seus dados a salvo de possíveis invasões (Ganut, 2021, p. 10).

Proporcionalmente ao crescimento de usuários da Internet e o desenvolvimento dessa tecnologia nas organizações, verificou-se também o crescimento de novos tipos de crimes, denominados crimes cibernéticos. Os crimes cibernéticos dominam as infrações verificadas nesse tipo de conectividade, afetando sobremaneira o processo de troca de informações proporcionada pela Internet, aspecto fundamental na vida e na sobrevivência das organizações (Vozniuk et. al, 2020).

A fiscalização destas práticas, porém, é morosa; de acordo com o Ministério da Economia, em setembro de 2023, haviam mais de 21 milhões de CNPJs ativos. Dessa forma, levanta-se a hipótese que boa parte das organizações não estejam em total conformidade com a LGPD.

Ante o exposto, esta pesquisa busca compreender: dado o risco de vazamento de dados pessoais e dados pessoais sensíveis, com base na hipótese de que a maioria dos profissionais ainda não está em conformidade com a

legislação, em que medida psicólogos e clínicas de psicologia estão adequados às exigências da Lei Geral de Proteção de Dados Pessoais?

1.2. Objetivo Geral

O objetivo geral desta pesquisa é avaliar o nível de aplicação da Lei Geral de Proteção de Dados Pessoais em consultórios de psicologia – representados por profissionais da área – do Distrito Federal.

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 consultórios de psicologia;
b) Entrevistar profissionais da área de psicologia autônomos e/ou que trabalhem em clínicas de pequeno porte.
c) Identificar e qualificar o nível de adequação dos consultórios de psicologia, 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 Consentimento; Controle de Acesso e Treinamento Interno; Segurança de Dados e Armazenamento; Especificações do cotidiano em Psicologia.
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.

1.4. Justificativa

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

Alguns dos dados pessoais coletados pelos consultórios de psicologia são: nome, endereço, CPF, telefone e informações médicas, ou dados de saúde, considerados dados sensíveis. Esses dados são importantes para a prestação de serviços de terapia ou suporte psicológico, mas também podem ser utilizados ou armazenados de forma indevida, expondo os dados dos pacientes a riscos de segurança, o que pode levar a graves consequências.

Por isso, é fulcral que consultórios e profissionais de psicologia sigam as diretrizes da LGPD, assegurando a proteção das informações pessoais de seus pacientes. Além disso, a adoção da LGPD oferece vantagens para os próprios consultórios, que acabam desenvolvendo processos de gestão de dados mais eficientes e seguros.

Ao investigar como os consultórios de psicologia estão se adaptando às exigências da LGPD, a pesquisa busca proporcionar maior compreensão sobre os desafios enfrentados por profissionais e instituições na gestão de dados pessoais, principalmente os dados sensíveis. Essa compreensão é fundamental para desenvolver estratégias eficazes de conformidade e mitigação de riscos em ambientes onde a confidencialidade e a privacidade são primordiais.

Além disso, a pesquisa busca contribuir para o desenvolvimento de competências em gestão de conformidade legal e ética, visando enriquecer o conhecimento geral sobre a LGPD.

Os resultados da pesquisa são relevantes, uma vez que podem contribuir para o aprimoramento da proteção de dados pessoais dos pacientes e para o desenvolvimento de melhores práticas de gestão de dados nos consultórios psicológicos. Além disso, este trabalho pode contribuir para aumentar a conscientização dos profissionais da área sobre a relevância da LGPD, ajudando-os a se adaptarem às mudanças trazidas por essa legislação. De acordo com o site do CFP (Conselho Federal de Psicologia), consultado em 15 de agosto

de 2024, existem mais de 541 mil profissionais inscritos no conselho espalhados pelo país.

2. REFERENCIAL TEÓRICO

Neste capítulo, será feita a introdução teórica de conceitos fundamentais para a melhor compreensão da pesquisa e suas conclusões. Cada uma das ideias centrais do presente trabalho será abordada em detalhes, buscando elucidar a importância de cada uma delas e como seu conhecimento pode influenciar no entendimento final da pesquisa.

2.1. Dado, Informação e Conhecimento

Apesar de serem constantemente confundidos como sinônimos, devido à proximidade de significados, tais termos possuem definições distintas. Para Correia (2009), a diferença entre estes conceitos pode ser explicada da seguinte forma:

- Dado: é um elemento bruto, sem significado quando analisado por si só. Pode ser representado por números, letras, símbolos, etc. É uma matéria prima que foi coletada, porém não foi processada ou interpretada.

  Por exemplo, um conjunto de números como ‘1234567890’ é um dado.

- Informação: é o resultado do processamento dos dados, ou seja, é o dado que foi organizado, relacionado e interpretado para adquirir significado. A informação é capaz de transmitir algum conhecimento ou compreensão.

  Por exemplo, se organizarmos o conjunto de números em uma sequência de telefone, como ‘(12) 3456-7890’, temos uma informação.

- Conhecimento: é o entendimento ou a compreensão que uma pessoa possui sobre determinado assunto, adquirido a partir da interpretação e assimilação de informações. O conhecimento é construído por meio da experiência, do aprendizado e da reflexão; é uma forma de saber aplicável em diferentes situações.

> Por exemplo, se uma pessoa sabe que o número ‘(12) 3456-7890’ é o telefone de uma empresa de telefonia, ela possui o conhecimento necessário para entrar em contato com esta empresa.

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 sociedade industrial representa a coordenação de homens e máquinas para a produção dos bens. Já a sociedade pós industrial organiza-se em torno do conhecimento, a fim de exercer o controle social e a direção das inovações e mudanças; e isto tudo dá origem, por sua vez, a novos relacionamentos sociais e a novas estruturas, as quais têm de ser politicamente dirigidas (Bell, Daniel, 1973, p. 34).

Segundo Werthein (2000), a expressão “sociedade da informação” é utilizada como substituto para o conceito complexo de “sociedade pós-industrial” e como forma de transmitir o conteúdo específico do “novo paradigma técnico-econômico”.

Ainda para Werthein, tais conceitos das ciências sociais procuram expressar mudanças na sociedade que referem-se às transformações técnicas, organizacionais e administrativas que têm como “fator-chave” não mais os insumos baratos de energia e matéria prima – como na sociedade industrial – mas os insumos baratos de informação propiciados pelos avanços tecnológicos na microeletrônica e telecomunicações.

O crescimento exponencial no volume de dados e a alta velocidade com que circulam e são gerados, são característicos de um dos grandes fenômenos do século 21: o Big Data. Segundo o Glossário Gartner (2021), Big Data refere-se a ativos de informação com alto volume, alta velocidade e/ou alta variedade, que exigem métodos inovadores e econômicos de processamento para proporcionar um discernimento mais aprimorado, apoiar a tomada de decisões e automatizar

processos. O Big Data surge, portanto, das ações dos usuários em plataformas e ambientes digitais que geram informações, organizadas e processadas por meio de algoritmos matemáticos (Salgado Leme; Blank, 2020).

Nesse contexto, um grande volume de informação é produzido a cada segundo, especialmente nos ambientes virtuais da internet, onde dados são continuamente gerados a partir de diversas atividades, como o registro de sites visitados, o tempo gasto nesses sites, a coleta de preferências de compra, a identificação da localização do usuário, entre outros exemplos de situações virtuais que geram informações (Carvalho, 2018).

Tal fluxo de informações, quando coletado por organizações empresariais e explorado para fins lucrativos, é conhecido como Economia Informacional ou Monetização de Dados. De acordo com Cohen (2002), observa-se que, nesse novo modelo econômico, voltado para a comercialização de dados, a principal mudança reside na maneira como a informação é utilizada.

Segundo Adjei (2015), a monetização das informações é o processo pelo qual os dados são convertidos em mercadorias, gerando lucro para quem os coleta e/ou processa. Reinaldo Filho (2018) complementa afirmando que, na Economia da Informação, os dados são frequentemente referidos como o “novo petróleo”, ou seja, possuem um elevado valor monetário e são considerados parte integral dos ativos das organizações empresariais.

De acordo com Yamagata (2017), existem duas abordagens para a monetização de dados: a interna e a externa. A abordagem interna envolve a conversão dos dados em conhecimento, que auxilia na tomada de decisões e na melhoria dos resultados da empresa. Por outro lado, a abordagem externa refere-se à transformação dos dados em produtos que interessam a terceiros, o que leva à comercialização dessas informações.

Em adição das empresas com fins lucrativos, os dados também são de fundamental importância para outras entidades. Conforme Finkelstein (2019), há um interesse público na coleta e utilização dos dados, especialmente para propósitos como segurança pública, investigação criminal e combate a atividades ilícitas, entre outros.

De acordo com Manuel Castells (2001), na era da informação, "a geração, processamento e transmissão de informação torna-se a principal fonte de produtividade e poder".

Portanto, percebe-se que a Sociedade da Informação é definida não apenas pelo uso das tecnologias de informação e comunicação, mas também pela maneira como essas tecnologias transformam a sociedade, influenciando o comportamento das pessoas e moldando os contextos social, político e econômico em escala global.

Em seu livro "A Sociedade em Rede" (2001), Manuel Castells introduz o conceito de "capitalismo informacional" como uma nova forma de organização econômica baseada na lógica da informação e do conhecimento. Ele descreve o capitalismo informacional como um sistema econômico em que a produção, distribuição e acumulação de riqueza dependem cada vez mais da capacidade de processamento de informações e consequente geração de conhecimento.

Para Castells (2001), o capitalismo informacional é caracterizado por três elementos principais:

1. Tecnologias da Informação e Comunicação (TICs): O desenvolvimento e a disseminação das tecnologias da informação e comunicação, como a internet, computadores e redes digitais, desempenham um papel central na economia e na sociedade. Essas tecnologias possibilitam a rápida circulação e processamento de informações em uma escala global.

2. Globalização Econômica: O capitalismo informacional é globalizado, com a interconexão econômica e financeira entre países e regiões. As redes globais de produção, distribuição e consumo são facilitadas pelas TICs, permitindo que as empresas operem em escala internacional.

3. Poder da Informação e do Conhecimento: No capitalismo informacional, o poder econômico está cada vez mais relacionado ao controle e à utilização da informação e do conhecimento. As empresas que dominam a produção e o fluxo de informações têm uma vantagem competitiva significativa, podendo influenciar mercados, tomar decisões estratégicas e moldar a opinião pública.

Em resumo, para Castells, o capitalismo informacional é um estágio avançado do capitalismo, no qual a informação e o conhecimento desempenham um papel crucial na produção e na organização social.

Stanley Davis (1990) cunhou uma expressão aparentemente contraditória mas em consonância com as atuais tendências: “personalização em massa”. Sua definição está relacionada basicamente a dois fatores principais: fornecimento de produtos customizados aos clientes e preços não tão altos resultantes dessa customização. A ideia de Davis era de que as novas tecnologias de informação e fabricação haviam tornado possível a customização de produtos para cada comprador individual.

Machado e Moraes (2008) dizem se tratar de uma estratégia que reside em técnicas e artifícios de manufatura para que seus produtos sofram pequenas e baratas alterações, criando a aura de item customizado, para que atinjam o maior número possível de leads e permitindo também aumentos de preço, gerando o maior lucro possível.

De acordo com Nascimento (2018), a capacidade de medir a satisfação dos clientes pela analítica preditiva, o poder de atendê-lo torna-se mais viável, criando produtos que possam suprir suas exatas necessidades.

A transição das sociedades industriais para a era da informação redefiniu o papel da tecnologia e do conhecimento na economia global, transformando dados em um recurso central para o poder e a inovação. À medida que avançamos para um ambiente onde a vigilância informacional e a personalização em massa se tornam cada vez mais comuns, é importante compreender como essas mudanças impactam o mercado e a vida cotidiana.

2.3. Sociedade de Vigilância

Apesar de não ter cunhado o termo, um dos principais teóricos sobre o tema é Michel Foucault. Para Foucault (1978), a vigilância na sociedade atua como um componente essencial do exercício de poder e controle. Sua obra explora como as instituições sociais utilizam mecanismos de vigilância para regular o comportamento das pessoas e manter a conformidade com as normas estabelecidas.

Foucault desenvolveu duas principais teorias relacionadas à vigilância: o poder disciplinar e a biopolítica.

Poder Disciplinar: Foucault descreveu o poder disciplinar como um sistema de controle que opera através da observação, normatização e vigilância constante das

atividades das pessoas. Instituições como prisões, escolas e fábricas aplicam essa forma de poder, dividindo as pessoas em espaços vigiados, regulando seus corpos e comportamentos. A vigilância nesse contexto não apenas mantém a ordem, mas também molda identidades e subjetividades, produzindo indivíduos alinhados com as normas sociais estabelecidas.

Biopolítica: atua não somente sobre indivíduos isolados, mas sobre populações inteiras. Para Foucault, na sociedade moderna, o poder passou a ser exercido não apenas para punir e disciplinar, mas também para regular a vida e a saúde das populações, envolvendo não apenas aspectos socioeconômicos, mas também aspectos biológicos.

Em ambas as teorias, a vigilância desempenha um papel central como mecanismo de poder que opera de maneira sutil e constante. A observação contínua cria uma sensação de visibilidade constante, o que leva as pessoas a internalizar as normas e se autorregular. Foucault estava interessado nas dinâmicas de poder que moldam as sociedades e como esses processos de vigilância influenciam a subjetividade e a conformidade. A vigilância não apenas monitora o comportamento das pessoas, mas também molda suas identidades e influencia suas ações, contribuindo para a manutenção da ordem social e o controle das populações.

De acordo com Stefáno Rodotà (2008), em uma sociedade de vigilância questiona-se o fim da privacidade dos indivíduos, em virtude das exigências dos mercados contemporâneos e da montagem dos robustos bancos de dados pessoais. O autor observa que, após o atentado de 11 de setembro, as dimensões jurídicas acerca da privacidade foram afrouxadas mundo a fora, com a redução de garantias fundamentais por meio de diplomas legais como o *Patriot Act* nos Estados Unidos e até mesmo pelas decisões na Europa de liberação de dados de passageiros de linhas aéreas para os Estados Unidos. O mercado se aproveita desse processo de diminuição de garantias, sendo as novas oportunidades tecnológicas mecanismos eficientes para a classificação, seleção, triagem e controle de indivíduos por meio da coleta de seus dados pessoais (Rodotà, 2008, p. 14).

Um conceito mais recente introduzido por Shoshana Zuboff (2020) é o capitalismo de vigilância. O termo refere-se à nova ordem econômica que reivindica a experiência humana como matéria-prima de práticas comerciais de extração, previsão e venda de comportamento. Para a autora, o capitalismo de

vigilância é uma ameaça tão significativa para a natureza humana no século XXI quanto foi o capitalismo industrial para o mundo natural nos séculos XIX e XX. O trecho a seguir foi retirado de sua obra “A era do capitalismo de Vigilância”, com o objetivo de ilustrar o conceito e algumas de suas influências na dinâmica social.

> O capitalismo de vigilância reivindica a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais. Embora alguns desses dados sejam aplicados para o aprimoramento de produtos e serviços, o restante é declarado como superávit comportamental do proprietário, alimentando processos conhecidos como “inteligência de máquina” e manufaturado em produtos de predição que antecipam o que um determinado indivíduo faria agora, daqui a pouco e mais tarde. Por fim, esses produtos de predições são comercializados num novo tipo de mercado para predições comportamentais que chamo de mercados de comportamentos futuros. [...] a dinâmica competitiva desses novos mercados leva os capitalistas de vigilância a adquirir fontes cada vez mais preditivas de superávit comportamental: nossas vozes, personalidades e emoções. Os capitalistas de vigilância descobriram que os dados comportamentais mais preditivos provêm da intervenção no jogo de modo a incentivar, persuadir, sintonizar e arrebanhar comportamento em busca de resultados lucrativos. Pressões de natureza competitiva provocaram a mudança, na qual processos de máquina automatizados não só conhecem nosso comportamento, como também moldam nosso comportamento em escala (Zuboff, Shoshana, 2020, p. 22).

O capitalismo de vigilância é uma mutação do capitalismo da informação, que nos coloca diante de um desafio civilizacional. As Big Techs – seguidas por outras organizações, laboratórios e governos – usam tecnologias da informação e comunicação (TIC) para expropriar a experiência humana, que se torna matéria-prima processada e mercantilizada como dados comportamentais. O usuário cede gratuitamente as suas informações ao concordar com termos de uso, utilizar serviços gratuitos ou, simplesmente, circular em espaços onde as máquinas estão presentes. (Koerner, Andrei, 2020).

Para Shoshana (2019), assim como o capitalismo industrial foi levado à intensificação contínua dos meios de produção, os capitalistas de vigilância e seus *players* no mercado estão agora travados na intensificação contínua dos meios de modificação comportamental, indo na direção oposta à do sonho digital dos primeiros tempos, relegando o ‘*Aware Home’* a dias longínquos. A conexão digital é agora um meio para fins comerciais de terceiros.

Com o entendimento destes conceitos desenvolvido, espera-se criar a compreensão de que dados de nossas subjetividades, preferências, particularidades

e hábitos são valiosos em diversos sentidos, além de amplamente cobiçados e disputados por diferentes entes da sociedade. Estes dados obtidos por meio da vigilância sistêmica podem ser fundamentais para organizações criminosas ou indivíduos mal intencionados, organizações privadas que buscam lucro ou entidades em busca de algum grau de controle social.

2.4. Segurança da Informação

A informação é um ativo de extrema importância para as organizações e grandes corporações, principalmente quando se encontra em um ambiente complexo de extrema criticidade e desafios constantes. Isso faz com que as organizações necessitem cuidar cada vez mais desses ativos, visando garantir a integridade, disponibilidade e confidencialidade dessas informações (Mohyeddin e Gharaee, 2014).

Segundo Ziraba e Okolo (2018), a informação é vista como a base para obter vantagens competitivas na economia atual. No entanto, possuir informações de terceiros pode representar um risco significativo para as organizações, pois pode levar à violação da privacidade de seus clientes e funcionários.

A Segurança da Informação torna-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
>
> (Associação Brasileira de Normas Técnicas, 2013).

O modelo mais adotado para guiar a gestão da segurança da informação em uma organização é conhecido como a tríade CID: confidencialidade, integridade e disponibilidade da informação (União Europeia, 2016), conforme ilustrado na Figura 1, p. 26.

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).

Em recente publicação sobre resiliência cibernética, Ramirez (2021) discorre que o termo resiliência teria sua origem em uma tática do exército romano denominada resilio, que consistia em recuar diante de ataque do inimigo e logo depois avançar em contra-ataque, mas mudando de posição. Ainda segundo o autor, o termo foi mais tarde incorporado pela Física, para denominar “a propriedade de alguns materiais de retornar à sua forma original após tê-la perdido por alguma razão, ou ainda a capacidade de deformar-se sem romper-se”, sendo depois apropriado por outras áreas do conhecimento humano (Ramirez, 2021, p. 97).

A resiliência cibernética se caracteriza pela proteção efetiva com resposta adequada às ameaças no espaço cibernético, a preservação e a continuidade das atividades e serviços fundamentais, sempre que possível, e a recuperação imediata das operações (Sharkov, 2016).

A ciber-resiliência passa a ser um ponto a ser alcançado para as infraestruturas críticas, possibilitando, de forma holística, o alinhamento entre a infraestrutura e o negócio da organização, trazendo confiança ao sistema, permitindo a prevenção, absorção, recuperação e adaptação após emergências (Bejarano et al., 2021).

2.5. ISO 27000

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

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).

Em essência, a confidencialidade assegura que apenas pessoas autorizadas tenham acesso às informações armazenadas ou transmitidas por algum meio. Manter esse princípio é vital para evitar que indivíduos não autorizados, seja de forma acidental ou intencional, obtenham acesso a essas informações (Caiçara, 2007).

A confidencialidade é um de três pilares da Segurança da informação. Estes três pilares são conhecidos como a tríade CID, que pode ser vista abaixo, na figura 1.

Figura 1: Tríade CID

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

De acordo com Whitman e Mattord (2012), a confidencialidade das informações é primordial para proteger os dados pessoais de funcionários e consumidores, e a falha em preservar essas informações pode comprometer a reputação de uma empresa, além de expô-la a litígios e ao pagamento de multas regulatórias.

Para proteger a confidencialidade das informações, podem ser tomadas algumas medidas, como por exemplo:

Classificação da informação;

Armazenamento seguro de documentos;

Aplicação de políticas gerais de segurança;

Treinamento dos guardiões da informação e usuários finais;

Criptografia das informações.

Integridade:

A Integridade é definida como a “propriedade de precisão e completude” (Associação Brasileira de Normas Técnicas, 2016).

Whitman e Mattord (2012) definem o princípio da Integridade como “a qualidade de ser inteiro, completo e incorrupto”. De acordo com os autores, a integridade de um ativo é ameaçada quando ele está sujeito a corrupção, dano, destruição ou qualquer outra interferência em seu estado original. Além disso, qualquer ativo se torna suscetível à corrupção ao passar por processamentos rotineiros, como a inserção, o armazenamento ou a transmissão de dados.

Para proteger a integridade das informações, são utilizados métodos de detecção de falhas na integridade de um sistema de arquivos, especialmente em caso de um ataque de vírus. O principal método envolve a busca por alterações no estado dos arquivos, seja pelo seu tamanho ou, em sistemas operacionais mais avançados, por meio do valor de hash ou da soma de verificação dos arquivos (Whitman; Mattord, 2012).

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).

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 formato utilizável. Os princípios da Integridade e da Confidencialidade da informação devem ser protegidos, diminuindo a vulnerabilidade e as ameaças de ataques. A Disponibilidade, entretanto, não implica na acessibilidade da informação a qualquer usuário, mas sim, que o dado estará disponível para os usuários autorizados quando for necessário.

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).

Na visão de Lyra (2015), atualmente, o bem mais valioso das organizações

são seus bancos de dados, o que traz o entendimento da importância de aplicação de práticas relacionadas à Segurança da Informação (SI) para as organizações, tanto públicas quanto privadas, visando reduzir os riscos relacionados ao tráfego de informações em formato digital.

Da mesma forma, para 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.

Assim, 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).

Criada pela *International Organization for Standardization*, a série de normas ISO 27000 é um conjunto robusto de padrões internacionais voltados para a gestão da segurança da informação nas organizações. Ela fornece diretrizes e melhores práticas para ajudar as empresas a proteger seus ativos de informação, mitigar riscos de segurança cibernética e garantir a confidencialidade, integridade e disponibilidade dos dados.

A série 27000 conta com as seguintes normas:

> ISO 27000 - Vocabulário da segurança da informação
>
> ISO 27001 - Gestão de segurança da informação
>
> ISO 27002 - Controles para a segurança da Informação
>
> ISO 27003 - Implantação de um SGSI
>
> ISO 27004 - Gerenciamento de Métricas e Relatórios para um SGSI
>
> ISO 27005 - Gestão de Riscos de Segurança da Informação
>
> ISO 27006 - Requisitos para auditorias externas em um SGSI
>
> ISO 27007 - Referências para auditorias em um SGSI
>
> ISO 27008 - Auditoria nos controles de um SGSI
>
> ISO 27010 - Gestão de Segurança da Informação para Comunicações Inter Empresariais
>
> ISO 27011 - Gestão de Segurança da Informação para empresa de Telecomunicações baseada na ISO 27002
>
> (ABNT NBR ISO/IEC, [sd]).

A série de normas ISO 27000 se tornou essencial para as organizações na atualidade devido ao crescente cenário de ameaças cibernéticas e à importância crítica da segurança da informação. Essas normas fornecem um conjunto abrangente de diretrizes e melhores práticas que ajudam as empresas a proteger seus ativos de informação, mitigar riscos de segurança cibernética e garantir a confidencialidade, integridade e disponibilidade dos dados.

A implementação das normas da série ISO 27000 oferece uma abordagem estruturada e holística para lidar com esses desafios, abrangendo desde a definição de vocabulário e conceitos até a gestão eficaz de riscos e a auditoria dos controles de segurança (Associação Brasileira de Normas Técnicas, 2016).

A implementação das normas ISO 27000 também auxilia na conformidade com regulamentações de segurança de dados, como o GDPR (*General Data Protection Regulation)* na União Europeia e a LGPD no Brasil, garantindo que as organizações estejam alinhadas com as exigências legais e evitem potenciais penalidades.

Em suma, a ISO 27000 desempenha um papel fundamental na garantia de que as organizações possuam uma abordagem estruturada e eficaz para lidar com os desafios cada vez maiores da segurança cibernética na atualidade. Ao seguir as diretrizes e controles estabelecidos por essas normas, as organizações podem fortalecer sua postura de segurança e proteger seus ativos de informação de maneira mais eficaz, contribuindo para um ambiente empresarial mais seguro e confiável.

2.6. Origem LGPD

A Lei Geral de Proteção de Dados surgiu para assegurar a segurança dos dados pessoais na sociedade da informação, tendo como base legislações já existentes em outros países. A regulamentação internacional estimulou o Brasil a criar também o seu dispositivo legal específico para este assunto.

2.6.1. Contexto Internacional

GDPR (*General Data Protection Regulation)*

Hoje, o principal marco regulatório estrangeiro sobre proteção de dados é a GDPR (*General Data Protection Regulation*), em português, “Regulamento Geral para 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.

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.

Em substituição à Diretiva de Proteção de Dados de 1995 (Diretiva 95/46/EC), 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. Na regulamentação antiga, 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, criando uma desarmonia entre as regulamentações dos países europeus (União Europeia, 1995)

Para a norma europeia, juntamente com a criação da GDPR, foi criado um Comitê Europeu para Proteção de Dados como organismo da União, que é composto por um diretor da autoridade de controle de cada Estado-membro (Vilela, 2021, p. 38).

Conforme ressaltam Finkelstein *et al.* (2019), apesar de expansivas, 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).

A norma regula o tratamento de qualquer dado pessoal ou informação que esteja vinculada a um indivíduo identificado ou identificável. A implementação da lei visa proteger, além do dado e de seu valor econômico, a privacidade de forma ampla, prevenindo comportamentos discriminatórios e exposições indesejadas da vida privada do titular (Rochfeld, 2018).

Assim, 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).

Cambridge Analytica

A empresa acusada, Cambridge Analytica, consiste em uma empresa inglesa de marketing cuja especialidade é analisar grandes quantidades de dados para construir estratégias supostamente mais eficazes a serem empregadas em campanhas publicitárias de várias ordens, de índole meramente comercial ou de caráter político. Ao que se sabe, essas análises implicavam na combinação de elementos da ciência comportamental com tecnologia de anúncios orientados pelo prévio exame dos dados. (Martins, Tateoki, 2019).

De acordo com Silas Martí (2019), tudo começou em junho de 2014, quando o professor Aleksandr Kogan, da Universidade Cambridge, no Reino Unido, criou um teste de personalidade no Facebook com o pretexto de conduzir um estudo psicológico de usuários.

Em março de 2018, órgãos da imprensa internacional noticiaram que a Cambridge Analytica teve acesso a dados pessoais de mais de 50 milhões de

usuários do Facebook, os tendo utilizado em 2016 para conduzir e influenciar as eleições presidenciais norte-americanas que resultaram na vitória do candidato republicano Donald Trump. Os dados do Facebook foram colhidos por meio do aplicativo *thisisyourdigitallife*, que, ao ser utilizado, os usuários concordavam em ceder dados e informações pessoais. (Martins, Tateoki, 2019).

Mesmo que só 270 mil pessoas tenham feito o teste de Kogan, o sistema permitiu que sua equipe visse o perfil de 50 milhões de usuários, pois também captava as informações de todos os amigos delas. No ano seguinte, Kogan repassou essa informação à Cambridge Analytica, que então contratou outros especialistas, entre eles Christopher Wylie, que acabou revelando o esquema ao jornal britânico *The Observer* (a versão dominical do Guardian).

Descobriu-se assim, com a divulgação feita por Christopher Wylie, que a Cambridge se utilizou de conhecimentos teóricos das ciências comportamentais para identificar parâmetros de personalidade existentes na imensa base de dados colhidos e, com isso, elaborou uma campanha publicitária específica para cada tipo de usuário. Uma das bases para a ação foi o mapeamento de “curtidas” deixadas pelos usuários do Facebook, bem como pesquisas aparentemente inocentes, tais como: ‘que animal mais combina com você?’. Desse modo, Trump e sua equipe eleitoral conseguiram montar perfis de personalidade dos eleitores potenciais de maneira mais eficiente que seus concorrentes.

Fornasier (2020) mostrou que o *modus operandi* da CA era dividido em três frentes de ataque: o primeiro era responsável pela coleta, armazenamento e tratamento de dados pessoais no Facebook, incluindo, a título meramente exemplificativo, fotos pessoais, posts insignificantes do cotidiano, lista de amigos, lista de pessoas bloqueadas, grupos que as pessoas ingressaram e grupos que participam ativamente. Essa tarefa de análise ou tratamento de um colossal banco de dados (big data) e sua categorização era realizada utilizando um software proprietário da CA chamado O.C.E.A.N. Um indivíduo, por intermédio de uma pesquisa dentro do Facebook, não apenas respondia questões como “Eu estou sempre preparado” ou “Eu geralmente me sinto cabisbaixo”, em uma gradação que varia entre inexato, neutro e exato. O resultado final indicava que tipo de comportamento você possui diante de diferentes cenários e hipóteses (Fornasier, 2020).

A BBC (2018) informou que o algoritmo criado pela CA para analisar os dados dos usuários com as curtidas poderia ser bastante preciso: com algumas dezenas de inputs seria possível revelar aspectos da personalidade de alguém com

elevadíssima precisão. A partir disso, a publicidade eleitoral, dentro do próprio Facebook, foi dirigida para cada tipo de pessoa. Estima-se que foram distribuídos cerca de 35 a 45 mil tipos de anúncios diferentes, dependendo das características do destinatário.

Esta situação gera um problema de identificação dos personagens, já que a massa eleitoral foi manipulada, ao receber conteúdo customizado, com o uso indevido de seus dados pessoais, oferecendo um candidato que representasse a forma ideal de agradar determinado eleitor, ofertando exatamente o que indivíduo em questão pensava e/ou acreditava. Dessa forma, a qualidade do voto, como exercício da cidadania, foi prejudicada.

Naquele momento, no Brasil, apesar de a proteção de dados pessoais já ser um princípio do marco civil da internet, ela não estava totalmente regulada por esta lei, e fazia-se necessária a criação de uma nova lei específica, voltada unicamente à proteção de dados pessoais.

2.6.2. Contexto Nacional

Antes da LGPD, a proteção de dados era tratada indiretamente por meio de outros dispositivos legais, como o Código de Defesa do Consumidor, a Lei do Cadastro Positivo (Lei nº 12.414/2011) e o Marco Civil da Internet. Uma regulamentação específica sobre o assunto 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).

Em 1990, o Código de Defesa do Consumidor, em seu artigo 43, já expunha proteção ao titular de dados frente bancos 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.

Já em 2011, a “Lei do Cadastro Positivo” (Lei nº 12.414/2011), regulamentou os 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.

No mesmo ano, surgiram 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 públicas.

No ano de 2012, um caso ganhou notoriedade nacional, quando a atriz Carolina Dieckmann teve sua intimidade violada após um grupo de técnicos de informática invadir seu computador pessoal, que havia sido enviado para manutenção, e subtrair sem autorização 36 imagens, que foram publicadas em redes sociais, mediante ameaças e extorsões para evitar a exposição. Com a envergadura que o caso ganhou, a justiça, em estado de emergência, deu sua resposta em menos de um ano; a lei Nº 12.737/2012, que criou o amparo legal para a punição de criminosos praticantes deste delito, que foi tipificado como “Invasão de dispositivo informático” (Art. 154-A do Código Penal) com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Para além da invasão de dispositivos pessoais, a atuação dos brasileiros na internet, mesmo com a formulação da lei Carolina Dieckmann (lei nº 12.737/2012), ainda não possuía princípios, garantias, ou deveres estabelecidos legalmente para o uso da rede; situação que foi devidamente normatizada no ano de 2014, pela lei nº 12.965/2014, o Marco Civil da Internet. Essa lei teve grande importância estrutural, pois trouxe ao meio da rede fundamentos constitucionais que já eram vigentes previamente à interação on-line, como o respeito à liberdade de expressão, aos direitos humanos, à pluralidade e à diversidade, livre iniciativa, livre concorrência e a defesa do consumidor. Esta lei trouxe ainda princípios constitucionais para a realidade da rede, como a proteção da privacidade, proteção dos dados pessoais, preservação e garantia da neutralidade da rede, responsabilização dos agentes de acordo com suas atividades e liberdade dos modelos de negócio promovidos na internet. Além dos fundamentos e princípios constitucionais terem sido inseridos por esta lei, foram delimitados também direitos e garantias dos usuários, como inviolabilidade da intimidade e vida privada com indenização prevista pelo dano material ou moral decorrentes de sua violação,

inviolabilidade e sigilo dos fluxos de informação e comunicações privadas pela internet e não suspensão da conexão à internet, salvo por débitos decorrentes de sua utilização e o não fornecimento de dados pessoais salvo mediante consentimento livre, expresso e informado (Brasil, 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 tendo surgido anos antes da LGPD, o Marco Civil da Internet (Lei nº 12.965/2014) já trouxe formalizações sobre a isonomia da rede e seus usuários, estabelecendo limites para a atuação do responsável por determinada transmissão de dados. O artigo que normatiza tais limites é o Art. 9º, que além do exposto, também versa sobre a proteção dos usuários, conforme o trecho destacado abaixo.

> Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.
>
> § 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
>
> I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
>
> II - priorização de serviços de emergência.
>
> § 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º , o responsável mencionado no caput deve:
>
> I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;
>
> II - agir com proporcionalidade, transparência e isonomia;

> III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
>
> IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
>
> § 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo (Brasil, 2014).

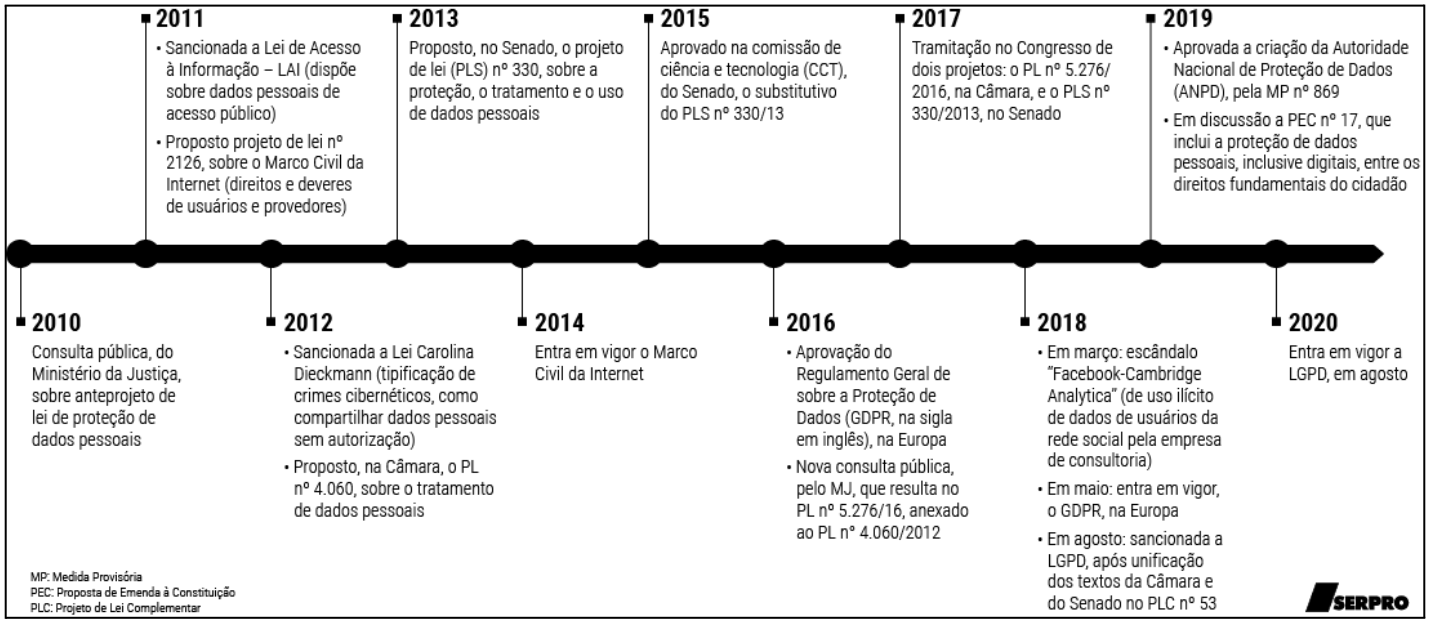
Apesar do Marco Civil da Internet, o Brasil ainda precisava de uma legislação mais detalhada sobre proteção de dados, tanto digitais quanto não digitais. Além disso, a GDPR, ao exigir em seu artigo 46 a existência de legislação específica e a adequação de outros países aos regulamentos de proteção de dados, incentivou o Brasil a desenvolver 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.

No ano de 2020, os dados de mais de 200 milhões de brasileiros que utilizavam o SUS (Sistema Único de Saúde) e até aquelas que não utilizavam tal mecanismo, ficaram expostos na rede por alguns meses devido a uma falha de segurança no sistema do Ministério da Saúde. Dados como nome completo, CPF, endereço e telefone foram vazados, certificando novamente a relevância do comprometimento com a Lei Geral de Proteção (Galvão *et al*, 2024).

Para Finkelstein *et al.* (2019), a disseminação de casos com possíveis implicações no controle dos processos eleitorais democráticos e o escândalo da *Cambridge Analytica*, 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, 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 no Brasil



(Fonte: SERPRO, disponível na *internet*)

2.7. Lei Geral de Proteção de Dados Pessoais (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD), promulgada pela Lei nº 13.709 em 14 de agosto de 2018, representa um divisor de águas na legislação brasileira em relação à proteção de informações pessoais. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece uma estrutura abrangente para o tratamento de dados pessoais, com o objetivo de garantir a privacidade, a segurança e a transparência no manuseio dessas informações.

A definição de dados pessoais na LGPD abrange qualquer informação relacionada a uma pessoa natural identificada ou identificável. Isso inclui desde dados básicos, como nome e endereço, até informações sensíveis, como dados de saúde, orientação sexual, origem étnica, opinião política e filiação a sindicatos ou a organização de caráter religioso, filosófico ou político. A ampla abrangência da definição visa proteger os direitos fundamentais dos indivíduos em relação à sua privacidade e autonomia.

2.7.1. Fundamentos da LGPD

A palavra ‘fundamento’, do latim *fundamentum* - que significa “base” - possui algumas definições, literais e figurativas, mas duas delas traduzem melhor o sentido desejado. De acordo como o dicionário Michaelis (2024), são elas;

1. “Conjunto de princípios básicos que regem a organização e o funcionamento de uma atividade, uma instituição etc., exprimindo circunstâncias, quer jurídicas, quer de fato, em que se firmam coisas ou em que se sancionam as ações.”

2. “Aquilo que confere a alguma coisa a sua existência ou a sua razão de ser.”

Desta forma, a LGPD define seus fundamentos para que seja de conhecimento público o seu conjunto de preceitos, que servirá de base para a compreensão de conceitos posteriores. A Lei nº 13.709, de 14 de agosto de 2018, estabelece para a disciplina da proteção de dados os seguintes fundamentos:

> I - o respeito à privacidade;
>
> II - a autodeterminação informativa;
>
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
>
> IV - a inviolabilidade da intimidade, da honra e da imagem;
>
> V - o desenvolvimento econômico e tecnológico e a inovação
>
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor;
>
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.
>
> (Brasil, 2020)

2.7.2. Princípios da LGPD

A LGPD determina que as atividades de tratamento de dados pessoais deverão observar a boa fé, mas também define critérios claros para o trabalho com dados. É o Art. 6º que define os seguintes princípios:

> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: 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;
>
> IV - livre acesso: 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;
>
> V - qualidade dos dados: 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;
>
> VI - transparência: 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;
>
> VII - segurança: 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;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - 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, 2020)

2.7.3. Tratamento de dados pessoais

O conceito de dado pessoal é definido pelo art. 5º da LGPD, que formaliza conceitos que podem ser nebulosos para muitos. De acordo com este fragmento da lei, dado pessoal pode ser descrito como “informação relacionada a pessoa natural identificada ou identificável” (Brasil, 2020). A definição descrita em lei encontra-se destacada abaixo.

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).

Ademais, conforme apresentado pelo Governo Federal, através do 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.

Em se tratando da LGPD, o tratamento de dados pessoais é regido pelo seu Art. 7º, e diz que tal tratamento somente pode ocorrer nas seguintes hipóteses:

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular;

II - para o cumprimento de obrigação legal ou regulatória pelo controlador;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; (Redação dada pela Lei nº 13.853, de 2019)

IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente. (Brasil, 2020).

2.7.4. Tratamento de dados pessoais sensíveis

Da mesma forma que a LGPD define as circunstâncias obrigatórias para que se possa tratar dados pessoais comuns, existe uma seção específica na lei formalizando os requisitos que devem ser cumpridos ao tratar dados pessoais sensíveis.

Os dados pessoais sensíveis são definidos também pela LGPD, em seu art. 5º, inciso II, que diz:

> Art. 5º - Para os fins desta Lei, considera-se:
>
> II - dado pessoal sensível: 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;

Os dados pessoais sensíveis, definidos no Art. 5º da LGPD acima, exigem um tratamento especial. Nesse sentido, o Art. 11 estabelece as hipóteses específicas em que o tratamento desses dados é permitido, como com o consentimento explícito do titular ou em casos excepcionais, como cumprimento de obrigação legal, tutela da saúde, ou proteção à vida:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
>
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais. (Brasil, 2020).

Conforme identificado acima, o Art. 11º da Lei Geral de Proteção de Dados Pessoais (LGPD) trata das condições em que o tratamento de dados pessoais sensíveis pode ser realizado. Esses dados, por sua natureza, exigem maior proteção, uma vez que envolvem informações como saúde, genética, orientação sexual, entre outros, que são considerados vulneráveis.

O ponto central deste artigo é que, de forma geral, o tratamento desses dados deve ocorrer mediante consentimento específico do titular (inciso I). No entanto, o artigo também lista exceções em que o tratamento pode ocorrer sem consentimento, desde que justificado por circunstâncias específicas.

A alínea f, do inciso II, destaca a tutela da saúde, autorizando o tratamento de dados sensíveis, como os dados de saúde, exclusivamente por profissionais ou serviços de saúde, sem a necessidade de consentimento do titular, desde que seja para fins de procedimentos relacionados à saúde. No contexto dos consultórios de psicologia, isso significa que os psicólogos podem lidar com informações sensíveis dos pacientes sem necessidade de consentimento explícito para cada procedimento, desde que essas informações sejam necessárias para o tratamento ou prestação de serviços. Isso reforça a importância de garantir que esses dados sejam manipulados com cuidado, uma vez que envolvem a privacidade e confidencialidade dos pacientes.

Tal trecho da lei ressalta o papel do psicólogo não apenas como prestador de serviço, mas também como guardião dos dados sensíveis, devendo adotar medidas de proteção para evitar a exposição indevida dessas informações. O cuidado no manejo dessas informações fortalece a confiança na relação terapeuta-paciente e assegura a conformidade com a LGPD.

2.7.5. Tratamento de dados pessoais de crianças e de adolescentes

O Art. 14º da Lei Geral de Proteção de Dados (LGPD) estabelece diretrizes específicas para o tratamento de dados pessoais de crianças e adolescentes, com foco no melhor interesse do menor, em conformidade com a legislação vigente. O tratamento de dados de crianças só pode ocorrer mediante consentimento específico e destacado de, no mínimo, um dos pais ou responsável legal. Essa exigência garante que os responsáveis estejam cientes e autorizem de forma clara a coleta e o uso de informações pessoais dos seus filhos. Além disso, os controladores dos dados devem manter informações públicas sobre os tipos de dados coletados, a forma de utilização e os procedimentos para que os responsáveis possam exercer seus direitos, como previsto no art. 18º da LGPD.

Há, no entanto, exceções em que os dados de crianças podem ser coletados sem consentimento prévio, como nos casos em que a coleta for necessária para contatar os pais ou responsáveis, desde que seja uma coleta única, sem armazenamento, ou para garantir a proteção da criança. Em tais casos, os dados não poderão ser repassados a terceiros sem a devida autorização. A lei também impede que controladores condicionem a participação de crianças em atividades como jogos e aplicativos ao fornecimento de informações pessoais que não sejam estritamente necessárias para a execução da atividade. O Art. 14º é destacado abaixo, buscando trazer o entendimento completo sobre o tema:

> Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente.
>
> § 1º O tratamento de dados pessoais de crianças deverá ser realizado com o consentimento específico e em destaque dado por pelo menos um dos pais ou pelo responsável legal.
>
> § 2º No tratamento de dados de que trata o § 1º deste artigo, os controladores deverão manter pública a informação sobre os tipos de dados coletados, a forma de sua utilização e os procedimentos para o exercício dos direitos a que se refere o art. 18 desta Lei.
>
> § 3º Poderão ser coletados dados pessoais de crianças sem o consentimento a que se refere o § 1º deste artigo quando a coleta for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento de que trata o § 1º deste artigo.

> § 4º Os controladores não deverão condicionar a participação dos titulares de que trata o § 1º deste artigo em jogos, aplicações de internet ou outras atividades ao fornecimento de informações pessoais além das estritamente necessárias à atividade.
>
> § 5º O controlador deve realizar todos os esforços razoáveis para verificar que o consentimento a que se refere o § 1º deste artigo foi dado pelo responsável pela criança, consideradas as tecnologias disponíveis.
>
> § 6º As informações sobre o tratamento de dados referidas neste artigo deverão ser fornecidas de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (Brasil, 2020).

Vale notar a exigência de que os controladores façam esforços razoáveis para garantir que o consentimento tenha sido realmente dado por um dos pais ou responsáveis legais, levando em consideração as tecnologias disponíveis para essa verificação. Além disso, as informações sobre o tratamento de dados devem ser comunicadas de forma clara, simples e acessível, levando em conta as capacidades físico-motoras e cognitivas da criança. O uso de recursos audiovisuais, quando adequado, é encorajado para facilitar a compreensão tanto pelos responsáveis quanto pelas crianças.

Esse conjunto de normas reflete o compromisso da LGPD em assegurar a proteção dos dados pessoais de menores de idade, promovendo o uso responsável e transparente dessas informações. Para profissionais que lidam com dados sensíveis de crianças, como psicólogos, essas diretrizes são essenciais para garantir que o tratamento das informações ocorra de maneira segura e ética, reforçando a importância da privacidade e da proteção de dados no ambiente clínico.

2.7.6. Garantias e responsabilidades

Por ser uma extensão dos direitos à privacidade, a LGPD traz aos titulares uma série de garantias, incluindo o acesso aos seus dados pessoais, como a correção de informações incorretas, a exclusão de dados desnecessários ou excessivos e a portabilidade dos dados para outros provedores de serviços. (Brasil, 2018). O compartilhamento de dados sensíveis possui atenção especial na lei, que veda a comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica, exceto nas hipóteses relativas a prestação de serviços de saúde, de assistência farmacêutica e de assistência à saúde, incluídos os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares dos dados (Brasil, 2020).

De acordo com a lei, consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. Isso significa que as organizações só podem coletar, armazenar, processar e compartilhar dados pessoais mediante autorização expressa e informada do titular. Além disso, a lei estabelece que o consentimento deve ser revogável a qualquer momento, garantindo o controle dos indivíduos sobre suas informações. Todos esses direitos empoderam os indivíduos e visam garantir que eles tenham controle sobre suas informações em todos os estágios do tratamento.

Para as organizações, a LGPD impõe uma série de obrigações e responsabilidades. Isso inclui a implementação de medidas de segurança adequadas para proteger os dados pessoais contra acessos não autorizados, vazamentos, perdas ou qualquer forma de tratamento indevido. As empresas também devem nomear um encarregado de proteção de dados (DPO - *Data Protection Officer*) e adotar políticas e procedimentos internos para garantir a conformidade com a lei.

Em caso de não conformidade, a LGPD prevê sanções administrativas significativas. As penalidades podem incluir advertências, multas de até 2% do faturamento da empresa, limitadas a R$ 50 milhões por infração, além de outras medidas corretivas determinadas pela Autoridade Nacional de Proteção de Dados (ANPD), órgão responsável pela fiscalização e aplicação da lei.

Em síntese, a LGPD representa um marco importante na proteção da

privacidade e dos direitos dos indivíduos, dando-lhes mais controle sobre suas informações pessoais. Ao estabelecer regras claras e rigorosas para o tratamento de informações pessoais, a lei busca promover uma cultura de respeito à privacidade e à segurança dos dados, fortalecendo a confiança dos cidadãos nas instituições que lidam com suas informações pessoais.

2.7.7. Adequação de MPEs à LGPD

Segundo Pinheiro (2018) atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de compliance digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura.

A adoção destas medidas tende a deixar a organização mais segura e confiável, com uma atuação mais responsável e resiliente. Este entendimento pode aprimorar a imagem pública da empresa, melhorando sua reputação.

Davies, Chun e Silva (2001) ressaltam que “reputação corporativa é um fenômeno complexo”. Na década de 60, o principal ponto de vista abordado era o do consumidor. Apenas na década de 70 surgiram estudos sobre o ponto de vista dos empregados. Esses autores definem a reputação como “um termo coletivo que se refere às visões de todos stakeholders sobre a reputação corporativa, incluindo identidade e imagem”, onde a identidade representa a percepção dos empregados da empresa e a imagem, a percepção dos agentes externos à empresa. (Vance; Ângelo, 2007).

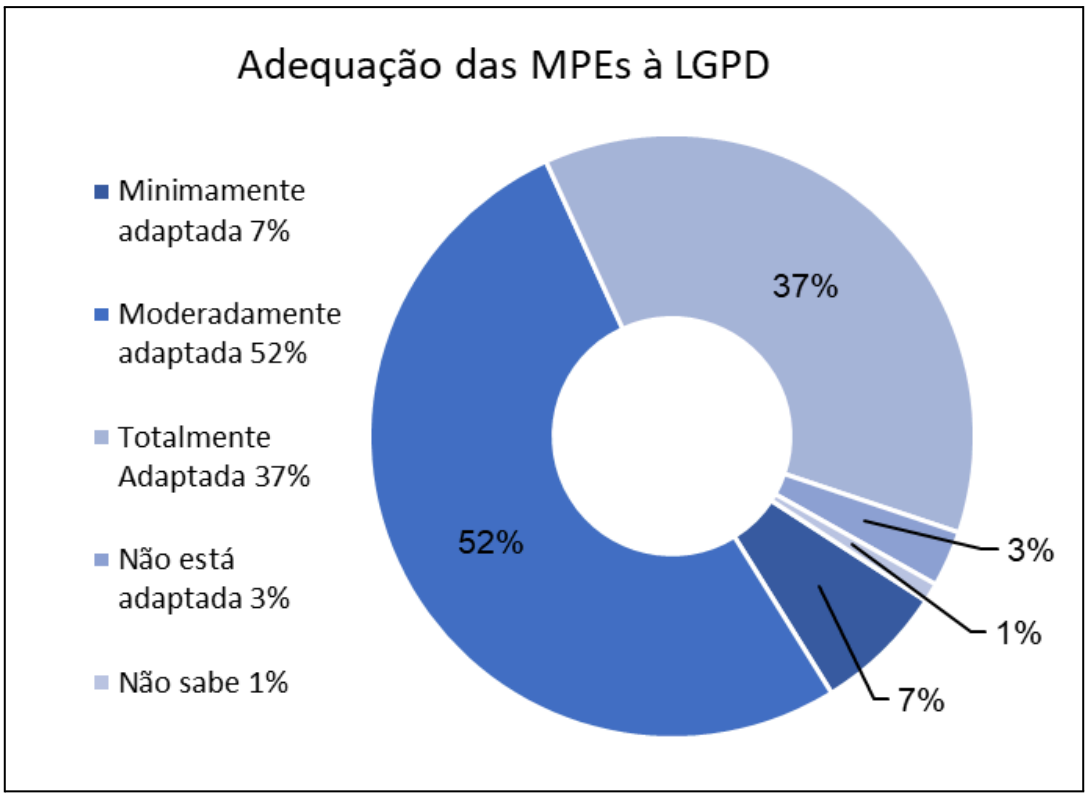
Essas definições variam de acordo com o autor. Dowling (2001) e Argenti e Forman (2002) definem a identidade como o conjunto de nomes, marcas, símbolos e outras manifestações visuais e concretas da realidade da empresa, e a imagem como a percepção das diferentes partes que integram a empresa (empregados) ou interagem com ela (investidores, consumidores e comunidade).

O panorama geral demonstra que as empresas estão progredindo lentamente no processo de implementação e adequação às diretrizes da LGPD. Elas têm dificuldade em formular políticas de proteção de dados e também

enfrentam falta de investimento em um profissional conhecido como Data Protection Officer (DPO), responsável por fiscalizar a aplicação efetiva da lei. Além disso, as empresas não dispõem de recursos suficientes para investir em novos processos tecnológicos e carecem de profissionais especializados para orientar a implementação das políticas de proteção, o que dificulta a adaptação à legislação e contribui para a lentidão no processo de conformidade (Galvão *et al*, 2024).

Já 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 pôde ser observada na pesquisa feita pela empresa de *software* Capterra, entre os dias 16 e 23 de junho de 2021, quase 1 ano após a lei ter entrado em vigor. Nesta pesquisa foi mensurado que somente 3 a cada 10 MPEs no Brasil se adequaram à LGPD. Ou seja, apenas 37%, das 305 empresas questionadas, disseram estar totalmente adequadas à legislação (GAVA, 2021). Na Figura 3, está representado um gráfico com o resultado da pesquisa.

Figura 3: A adequação das MPEs à LGPD.



(Fonte: adaptado de GAVA, 2021)

As estratégias modernas de linguística computacional oferecem ferramentas e técnicas, e numerosos recursos estão disponíveis, mas há pouca orientação para os psicólogos sobre por onde começar. (Harlow and Oswald, 2016).

2.7.8. Resolução CD/ANPD nº 2

Levando em conta os desafios enfrentados pelas pequenas e microempresas na adequação à lei, a ANPD deu prioridade em sua agenda à criação de flexibilizações no texto da LGPD, com o objetivo de ajustar a regulamentação à realidade das empresas de menor porte.

Assim, no dia 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). Esta primeira resolução já trouxe uma série de flexibilizações, tratando da adequação das normas à realidade das empresas de menor porte que vêm enfrentando dificuldades em entrar em conformidade com os requisitos da 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 Art. 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;
>
> III- 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 II da Lei Complementar nº 182, de 1º de junho de 2021; e
>
> IV - zonas acessíveis ao público: espaços abertos ao público, como praças, centros comerciais.

Para além disso, o Art. 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 ainda 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:

> 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;
>
> II - 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 (Brasil, 2022).

As principais flexibilizações trazidas pela Resolução nº 2 da ANPD (Brasil, 2022) estão condensadas no Quadro 1:

Quadro 1: Principais Flexibilizações da Resolução nº 2 da ANPD.

Tema	Resolução
Das obrigações relacionadas aos direitos do titular	"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	"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	"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	"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	"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	"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)

2.7.9. LGPD em consultórios de psicologia

O papel dos Conselhos

Os conselhos (regionais e federais) são considerados instâncias de representação máxima dos profissionais da área (Holanda, 1997), aos quais cabem as funções de orientar, disciplinar, fiscalizar e zelar pelo cumprimento das práticas éticas na profissão. Por ser o órgão fiscalizador da profissão, o Conselho Federal de Psicologia (CFP) tem, dentre suas atribuições, a responsabilidade de garantir a qualidade técnica e ética dos serviços prestados pelos psicólogos (Anache; Corrêa, 2010). Sua atuação, no entanto, não se limita, ainda de acordo com as autoras, à fiscalização. Ele consiste em uma instância, cujo objetivo maior é o de promover o debate e construir diretrizes que orientem as práticas dos psicólogos, dentro de um diálogo constante com a sociedade sobre o trabalho do profissional dessa área.

Assim, um papel fundamental dos Conselhos relaciona-se à fiscalização e ao zelo pelo cumprimento integral das práticas éticas. Para isso, o Código de Ética Profissional, o qual postula os princípios éticos a serem adotados pelos profissionais de cada área, surgiu como parâmetro para regular o conjunto de condutas profissionais e para proteger os interesses das pessoas. Por conta das mudanças ocorridas nos diferentes períodos da história do país e da própria Psicologia, diante da necessidade de responder às transformações da sociedade brasileira, a Psicologia encontra-se em seu quarto código, os quais foram publicados, respectivamente, em 1975, 1979, 1987, 2005, ainda em vigor (Anache, & Reppold, 2010).

Código de Ética Profissional do Psicólogo e Fundamentos da LGPD

Toda profissão define-se a partir de um corpo de práticas que busca atender demandas sociais, norteado por elevados padrões técnicos e pela existência de normas éticas que garantam a adequada relação de cada profissional com seus pares e com a sociedade como um todo. Um Código de Ética profissional, ao estabelecer padrões esperados quanto às práticas referendadas pela respectiva categoria profissional e pela sociedade, procura fomentar a auto-reflexão exigida de cada indivíduo acerca da sua práxis, de modo a responsabilizá-lo, pessoal e

coletivamente, por ações e suas consequências no exercício profissional (CFP, 2005).

De acordo com a resolução CFP nº 010/2005, a missão primordial de um código de ética profissional não é de normatizar a natureza técnica do trabalho, e, sim, a de assegurar, dentro de valores relevantes para a sociedade e para as práticas desenvolvidas, um padrão de conduta que fortaleça o reconhecimento social daquela categoria. Códigos de Ética expressam sempre uma concepção de homem e de sociedade que determina a direção das relações entre os indivíduos. Traduzem-se em princípios e normas que devem se pautar pelo respeito ao sujeito humano e seus direitos fundamentais (CFP, 2005).

Por constituir a expressão de valores universais, tais como os constantes na Declaração Universal dos Direitos Humanos; sócio-culturais, que refletem a realidade do país; e de valores que estruturam uma profissão, um código de ética não pode ser visto como um conjunto fixo de normas e imutável no tempo. As sociedades mudam, as profissões transformam-se e isso exige, também, uma reflexão contínua sobre o próprio código de ética que nos orienta. Mesmo assim, é interessante notar que mesmo tendo sido elaborado em 2005, o Código de Ética Profissional do Psicólogo (CEPP) apresenta diversas diretrizes já alinhadas com a LGPD, lei que entraria em vigor apenas em 2020. Abaixo, são listadas as confluências entre os documentos. Vale lembrar que os trechos da LGPD que definem seus fundamentos e princípios estão dispostos nas páginas 37 e 38 deste trabalho.

O princípio da privacidade é refletido no dever do psicólogo de resguardar as informações confidenciais dos atendidos. O Conselho Federal de Psicologia demonstra obrigações do profissional ao tratar dados: “Zelar para que a comercialização, aquisição, doação, empréstimo, guarda e forma de divulgação do material privativo do psicólogo sejam feitas conforme os princípios deste Código” (CFP, Resolução 010/05, p. 08, Art. 1º). Tanto a LGPD quanto o Código de Ética destacam a proteção à privacidade como central no tratamento de dados ou informações; ‘autodeterminação informativa’ (LGPD, Art. 2º, Fundamento II, 2020).

O Código afirma que o psicólogo deve garantir que “o psicólogo baseará o seu trabalho no respeito e na promoção da liberdade, da dignidade, da igualdade e da integridade do ser humano, apoiado nos valores que embasam a Declaração Universal dos Direitos Humanos.” (CFP, Resolução 010, 2005, p. 7). Nota-se também ênfase no texto da LGPD sobre este tema, quando é enfatizado o direito

da pessoa de controlar suas próprias informações e estar informada sobre o uso destas; Inviolabilidade da intimidade, da honra e da imagem (LGPD, Art 2º, Fundamento IV). A inviolabilidade da intimidade é um princípio fundamental para a prática da psicologia, que exige do psicólogo “respeitar o sigilo profissional a fim de proteger, por meio da confidencialidade, a intimidade das pessoas, grupos ou organizações, a que tenha acesso no exercício profissional.” (CFP, Resolução 010, 2005, p. 13, Art. 9º). Tanto a LGPD quanto o CEPP tratam da proteção à intimidade e confidencialidade das informações; “direitos humanos, dignidade e exercício da cidadania" (LGPD, Art. 2º, Fundamento VII).

É interessante observar como a orientação do artigo 9º do CFP mostra-se em acordo com a previsão constitucional (art 5º, inciso X), citada na introdução deste trabalho, onde é 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" Brasil [Constituição (1988)]. Além disso, o nono artigo também coincide com o código civil, artigo 21, também citado na introdução deste trabalho.

Vale salientar que para além da consonância com os dispositivos legais já mencionados, este artigo está em perfeita harmonia com os fundamentos da LGPD, definidos no Artigo 2º, números 1 e 4: “Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; [...] IV - a inviolabilidade da intimidade, da honra e da imagem;” (Brasil, 2020).

Artigo 10º (CFP, Resolução 010, 2005, p. 13): Em situações de conflito entre o sigilo e os princípios fundamentais, o psicólogo poderá decidir pela quebra de sigilo, sempre baseando sua decisão no critério de menor prejuízo possível. O parágrafo único deste artigo determina que, nesses casos, o profissional deve "restringir-se a prestar as informações estritamente necessárias" (CFP, Resolução 010, 2005).

Artigo 12º (CFP, Resolução 010, 2005, p. 13): Ao participar de equipes multiprofissionais, o psicólogo deverá registrar “apenas as informações necessárias para o cumprimento dos objetivos do trabalho”. Esse ponto ressalta a necessidade de compartilhar apenas o mínimo indispensável de informações, mantendo o caráter confidencial.

Artigo 15º (CFP, Resolução 010, 2005, p. 14): Em casos de interrupção do trabalho, como demissão ou extinção do serviço, este artigo impõe ao psicólogo o dever de zelar pelo destino dos arquivos confidenciais, repassando-os ou

lacrando-os para o próximo responsável. Isso assegura que informações sigilosas continuem protegidas mesmo após o término do atendimento.

Artigo 16º (CFP, Resolução 010, 2005, p. 14), alínea "c": Neste item, é requerida a garantia a anonimização das pessoas, grupos ou organizações envolvidas em pesquisas e estudos, salvo interesse manifesto destes. Aqui percebe-se grande semelhança com a LGPD, Art. 7º, que permite o tratamento de dados apenas em determinadas situações, sendo uma delas descrita no inciso IV: “para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;” (Brasil, 2020)

O psicólogo deve “Estabelecer acordos de prestação de serviços que respeitem os direitos do usuário ou beneficiário de serviços de Psicologia.” (CFP, Resolução 010, 2005, p. 08, Art. 1º). Este tema se relaciona ao fundamento VII da LGPD; “os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais” (Brasil, 2020).

Código de Ética Profissional do Psicólogo e Princípios da LGPD

Finalidade (Art. 6º, Princípio I da LGPD)

“O psicólogo atuará com responsabilidade social, analisando crítica e historicamente a realidade política, econômica, social e cultural.” (CFP, Resolução 010, 2005, p. 7). A similaridade se dá no reforço da necessidade de comunicar com clareza as finalidades do uso de dados ou das intervenções, conforme Art 6º, princípio I da LGPD.

Adequação (Art. 6º, Princípio II da LGPD)

“O psicólogo, para ingressar, associar-se ou permanecer em uma organização, considerará a missão, a filosofia, as políticas, as normas e as práticas nela vigentes e sua compatibilidade com os princípios e regras deste Código.” (CFP, Resolução 010, 2005, p. 11, Art. 3º). A adequação do tratamento de dados ou da intervenção deve estar em sintonia com as finalidades e o contexto, tanto na LGPD quanto no Código.

Necessidade (Art. 6º, Princípio III da LGPD)

“Nos documentos que embasam as atividades em equipe multiprofissional, o psicólogo registrará apenas as informações necessárias para o cumprimento dos objetivos do trabalho.” (CFP, Resolução 010, 2005, p. 13, Art. 12º). A LGPD também restringe o uso de dados ou informações ao mínimo necessário para o cumprimento de suas finalidades.

Transparência (Art. 6º, Princípio VI da LGPD)

“Nas situações em que se configure conflito entre as exigências decorrentes do disposto no Art. 9º e as afirmações dos princípios fundamentais deste Código, excetuando-se os casos previstos em lei, o psicólogo poderá decidir pela quebra de sigilo, baseando sua decisão na busca do menor prejuízo.” (CFP, Resolução 010, 2005, p. 13, Art. 10º). Tanto a LGPD quanto o Código de Ética exigem que as informações sejam claras, precisas e acessíveis ao titular ou paciente.

Segurança (Art. 6º, Princípio VII da LGPD)

O Código orienta que “É dever do psicólogo respeitar o sigilo profissional a fim de proteger, por meio da confidencialidade, a intimidade das pessoas, grupos ou organizações, a que tenha acesso no exercício profissional.” (CFP, Resolução 010, 2005, p. 13, Art. 9º). A proteção contra o uso indevido ou não autorizado de informações é uma prioridade compartilhada.

Prevenção (Art. 6º, Princípio VIII da LGPD)

O psicólogo deve adotar medidas para prevenir riscos que possam afetar a confidencialidade e segurança dos dados de seus pacientes. “Compartilhará somente informações relevantes para qualificar o serviço prestado, resguardando o caráter confidencial das comunicações, assinalando a responsabilidade, de quem as receber, de preservar o sigilo.” (CFP, Resolução 010, 2005, p. 12, Art. 6º). A prevenção de danos relacionados ao tratamento de dados é um princípio compartilhado por ambas as normativas.

Não Discriminação (Art. 6º, Princípio IX da LGPD)

“O psicólogo trabalhará visando promover a saúde e a qualidade de vida das pessoas e das coletividades e contribuirá para a eliminação de quaisquer formas de negligência, discriminação, exploração, violência, crueldade e opressão.” (CFP, Resolução 010, 2005, p. 7). O combate à discriminação, seja no tratamento de dados ou no exercício profissional, é um princípio comum.

A LGPD e o Código de Ética do Psicólogo possuem um grande alinhamento, já que ambos visam proteger a dignidade, a privacidade, e os direitos humanos, promovendo o uso ético e responsável das informações. Desta forma, espera-se encontrar algum grau de semelhança na análise das entrevistas.

Outras Resoluções importantes

Resolução CFP nº 06/2019

A Resolução CFP nº 6, de 29 de março de 2019, institui regras para a elaboração de documentos escritos por psicólogas(os) no exercício de sua profissão. Essa normativa define diretrizes para a produção de documentos como laudos, relatórios, pareceres e atestados psicológicos, garantindo que eles sejam elaborados de forma clara, precisa e ética, respeitando o sigilo e a proteção das informações dos pacientes. A resolução também revoga as anteriores Resolução CFP nº 15/1996, Resolução CFP nº 07/2003 e Resolução CFP nº 04/2019, consolidando as orientações e atualizando os procedimentos para a produção desses documentos.

Resolução CFM nº 2.309/2022

A Resolução CFM nº 2.309/2022 estabelece regras para a publicização e o compartilhamento de dados de médicos inscritos, em conformidade com a Lei Geral de Proteção de Dados (LGPD). Ela equilibra a proteção da privacidade dos profissionais com o interesse público e as atribuições legais do Conselho Médico. Essa norma visa garantir que o tratamento desses dados seja realizado de maneira responsável e transparente, respeitando tanto os direitos dos médicos quanto a necessidade de acesso a informações relevantes por parte da sociedade.

Resolução CFM nº 2.314/2022

A Resolução CFM nº 2.314/2022 define e regulamenta a telemedicina, estabelecendo a prestação de serviços médicos mediados por tecnologias de comunicação. Essa normativa formaliza o uso da telemedicina no Brasil, detalhando os critérios, condições e responsabilidades para que médicos realizem consultas, diagnósticos e tratamentos à distância, garantindo que sejam respeitadas as normas éticas e de qualidade no atendimento, além de proteger a privacidade e segurança dos dados dos pacientes.

Resolução CFM nº 2.309/2022

A Resolução CFM nº 2.309/2022 regulamenta o compartilhamento e a publicização de dados de médicos inscritos, buscando adequar-se à nova legislação brasileira. Essa norma unifica e sistematiza as regras referentes ao tratamento e divulgação das informações dos profissionais de medicina, promovendo maior transparência e proteção dos dados. Ela estabelece diretrizes sobre como os dados podem ser acessados e utilizados, garantindo que os direitos dos médicos e dos pacientes sejam respeitados. Estabelece também que, em atendimentos por telemedicina, o paciente ou seu representante legal deve dar consentimento explícito para o compartilhamento de suas informações pessoais.

Instrução Normativa CFM nº 003/2021

A Instrução Normativa CFM nº 003/2021 institui a Política de Privacidade dos Dados das Pessoas Físicas dentro do Conselho Federal e nos Conselhos Regionais de Medicina. Essa normativa estabelece diretrizes para o tratamento de dados pessoais, visando proteger a privacidade dos cidadãos e assegurar que as informações sejam manipuladas de forma ética e em conformidade com a Lei Geral de Proteção de Dados (LGPD). Ela enfatiza a importância da transparência no tratamento dos dados, a necessidade de consentimento dos titulares para o uso de suas informações e a responsabilidade dos conselhos em garantir a segurança e a confidencialidade dos dados pessoais que gerenciam.

Instrução Normativa CFM nº 003/2019

A Instrução Normativa CFM nº 003/2019 regulamenta os procedimentos para o acesso e tratamento de informações e documentos no âmbito do Conselho Federal de Medicina (CFM). Essa normativa estabelece diretrizes sobre como as informações devem ser manejadas, garantindo que o tratamento de dados pessoais e documentos respeite a legislação vigente, incluindo a Lei Geral de Proteção de Dados Pessoais (LGPD). Além de definir responsabilidades e processos, a instrução enfatiza a importância da transparência e da segurança na gestão das informações, assegurando que os direitos dos titulares sejam respeitados.

Prontuários

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.

No Brasil, a temática relativa ao Prontuário eletrônico do paciente (PEP) ganhou força no meio universitário em meados da década de 1990, culminando em algumas iniciativas isoladas. Em 1999, por ação do Ministério da Saúde, um conjunto mínimo de informações que devem constar no prontuário eletrônico é proposto, visando permitir a integração dos diversos sistemas e fortalecer sua implementação. Alguns anos mais tarde, em 2002, o Conselho Federal de Medicina reconheceu o prontuário eletrônico, na Resolução CFM 1639/2002, como uma forma legítima de armazenamento de dados relativos aos pacientes. Além disso, a Resolução CFP nº 006/2019 do Conselho Federal de Psicologia (CFP) estabelece as regras para a elaboração de documentos escritos produzidos por psicólogos no exercício profissional.

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.

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).

Segundo Carvalho, Leandro e Liarte (2018) o prontuário, seja ele físico ou eletrônico, é o principal documento do sistema de informação hospitalar, essencial em seus aspectos assistenciais e administrativos. Constitui também o registro completo da assistência prestada ao paciente durante sua doença e, portanto, tem significado como documento jurídico. O prontuário clínico é um documento legal que armazena informações, imagens e sinais relativos aos serviços prestados ao paciente em todas as áreas do sistema de saúde, possibilitando a comunicação entre os diversos profissionais da equipe e a continuidade do atendimento ao cidadão (Monaghan et al., 2020).

De acordo com pesquisa elaborada por Casanova (2019), quando abordado qual seria o prontuário mais seguro para manter os dados dos pacientes em sigilo, apenas 33% dos entrevistados afirmaram ser o PFP (Prontuário Físico em Papel) o mais seguro para evitar vazamento de informações dos pacientes (Casanova et al, 2019).

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 MPEs que tratam dados sensíveis, optou-se pela aplicação do estudo especificamente no nicho de consultórios de psicologia, por haver o manejo de dados sensíveis referentes à tutela de saúde, que é um Direito Fundamental previsto pela Constituição Federal de 1988.

Para investigar este tema, foi realizada uma pesquisa do tipo exploratória e de abordagem qualitativa, buscando coletar informações sobre o assunto, para a posterior 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, pelo alinhamento de objetivos, a pesquisa exploratória mostrou-se alinhada e compatível com o presente trabalho, que aborda um tema relativamente recente e não muito estudado em discussões acadêmicas.

Segundo Pádua (2019), a pesquisa baseia-se em dois tipos de procedimentos metodológicos, sendo eles: bibliográfico e de campo. Assim, inicialmente, foi desenvolvida uma revisão da literatura sobre dados, segurança cibernética, proteção e privacidade de dados. Neste momento também foram abordados a origem e as inspirações 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, especialmente, em consultórios de psicologia, 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), organiza-se previamente um conjunto de questões (roteiro) sobre o tema que está sendo estudado, mas permite, e às vezes até incentiva, que o entrevistado fale livremente sobre assuntos que vão surgindo como desdobramentos do tema principal. As entrevistas semiestruturadas não possuem uma estrutura rígida, de forma que idealmente seja 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 psicólogos sobre o impacto da LGPD no contexto da área, bem como questões da aplicabilidade da lei no cotidiano de um consultório de psicologia. O questionário de entrevista semiestruturado utilizado nesta pesquisa pode ser conferido no Apêndice A.

3.2. Caracterização do objeto de estudo

O presente estudo tem como objeto a adequação dos psicólogos e das clínicas de psicologia à LGPD no Brasil. A pesquisa investiga o nível de conformidade desses profissionais e instituições com as exigências legais de proteção de dados pessoais e sensíveis dos pacientes, considerando a importância de garantir a privacidade e a segurança dessas informações no contexto clínico.

Nos consultórios de psicologia, os dados coletados possuem peculiaridades que demandam cuidados especiais. Além de informações pessoais comuns, os psicólogos lidam com dados sensíveis, que podem incluir histórico de saúde mental, relatórios terapêuticos, diagnósticos, informações sobre questões emocionais e comportamentais dos pacientes, entre outros. Esses dados, quando expostos ou mal geridos, podem causar danos significativos à privacidade e bem-estar dos indivíduos, tornando sua proteção ainda mais crucial.

A conformidade com a LGPD exige que esses dados sejam tratados com maior cautela, garantindo segurança no armazenamento e no acesso, além de garantir o consentimento informado do paciente em relação ao uso de suas informações. Como esses dados são frequentemente utilizados tanto em formato

físico quanto digital, o risco de vazamento ou uso indevido aumenta, tornando a adequação às normas da LGPD essencial para evitar violações e sanções legais. Além disso, a pesquisa também busca compreender como os consultórios de psicologia foram afetados pela lei, analisando a percepção dos profissionais sobre a aplicação da regulamentação em suas rotinas de trabalho e as estratégias adotadas para proteger as informações dos pacientes.

3.3. Participantes da pesquisa

Para que se obtivesse a profundidade necessária, foram selecionados os profissionais de psicologia que lidam com a coleta e/ou com o tratamento dos dados de seus pacientes, e que atuam como terapeutas e/ou analistas em clínicas e consultórios de psicologia. Portanto, a escolha dos participantes 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 de psicologia, permitindo a obtenção das informações necessárias.

Durante a escolha dos entrevistados, alguns critérios foram utilizados para a seleção, como ser um profissional da área de psicologia que exerça a profissão de terapeuta em consultórios de psicologia, sendo excluídos estudantes ainda em graduação, profissionais aposentados e terapeutas que não possuíssem formação acadêmica na área. Não houve restrição sobre a natureza dos atendimentos, ou seja, foram consideradas como equivalentes as modalidades de terapia presencial e on-line.

Foram realizadas 10 entrevistas com indivíduos que atuam 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 pela anonimização das respostas, onde foi designada uma numeração de 1 a 10 para realizar a identificação de cada entrevistado, incluindo também siglas como, por exemplo, *E01, E02* em diante.

3.4. Caracterização e descrição dos instrumentos de pesquisa

O instrumento de pesquisa utilizado foi a entrevista semiestruturada, modelo de entrevista que combina perguntas abertas e fechadas, e que permite que o entrevistador e o entrevistado façam perguntas fora do roteiro prévio

O entrevistador permite ao entrevistado falar livremente sobre o assunto. Este tipo de entrevista é bastante empregado em situações onde há o objetivo de explorar a fundo alguma experiência vivida em condições precisas (Gil, 1987).

A entrevista semiestruturada tem como objetivo explorar as perspectivas e experiências dos entrevistados de maneira mais aberta e abrangente. Permite uma exploração profunda dos temas, adaptando-se às respostas do entrevistado.

Embora o entrevistador tenha um roteiro, há uma grande flexibilidade para seguir novos caminhos que emergem durante a entrevista, baseando-se nas respostas do entrevistado, permitindo um diálogo mais profundo e pessoal, adaptando-se às respostas do entrevistado para explorar novas áreas que podem surgir durante a conversa.

É comum em pesquisas sociais, psicológicas e educacionais onde o entendimento profundo dos pensamentos, sentimentos e comportamentos dos entrevistados é necessário.

Em levantamento bibliográfico sobre o uso de entrevistas na pesquisa em educação, a pesquisadora Ana Cláudia Sacramento nos esclarece que de uma forma ampla a entrevista é um instrumento de pesquisa que visa obter informações de interesse a uma investigação. O pesquisador formula perguntas orientadas, com um objetivo definido, para identificar diferentes variáveis e suas relações, comprovar hipóteses, orientar outras fases da pesquisa, coleta de dados para uma pesquisa preliminar.

3.5. Procedimentos de coleta e de 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 (2016). 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 Consentimento;

Controle de Acesso e Treinamento Interno;

Segurança de Dados Pessoais e Armazenamento;

Especificações do cotidiano em consultórios de psicologia.

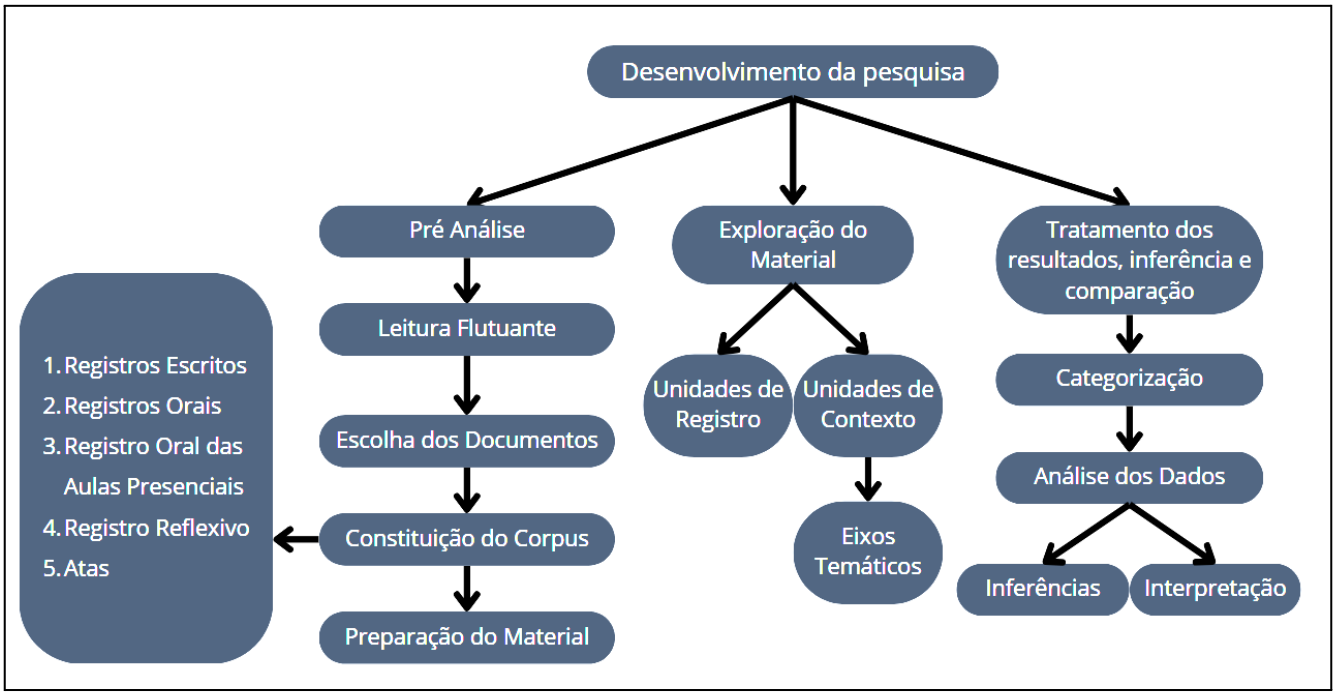
Inicialmente, o roteiro continha em sua totalidade 16 perguntas, que ao longo das entrevistas poderiam ser adaptadas de acordo com a progressão das respostas de cada entrevistado. Dessa forma, possibilitando o aprofundamento e entendimento de questões específicas de cada entrevistado.

As entrevistas foram realizadas individualmente e de forma online, através da plataforma de reunião virtual, entre abril e agosto de 2024, e tiveram, 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 (1977), uma técnica de análise de dados qualitativos que consiste em 3 (três) etapas principais:

- Pré-análise: etapa na qual o pesquisador define o objetivo do estudo e seleciona o material a ser analisado;
- Exploração do material, Categorização ou Codificação: etapa na qual o pesquisador lê o material de forma não sistemática para ter uma compreensão geral;
- Tratamento dos resultados, Inferências e Interpretação: etapa na qual o pesquisador analisa os dados coletados e elabora as conclusões.

Figura 4: Desenvolvimento de Pesquisa de Acordo com o método de Bardin.



(Fonte: Baseado em Bardin (1977, p. 102))

A etapa de pré-análise, conforme ilustrada na figura 4, se deu na transcrição das entrevistas, buscando organizar as informações coletadas e prepará-las para posterior análise e exploração. 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 construído um documento de análise das informações compartilhadas pelos entrevistados, dividindo as respostas coletadas entre as categorias pré-estabelecidas 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.

Ainda na segunda etapa, os trechos destacados anteriormente também foram agrupados, facilitando a visualização e a comparação das respostas obtidas.

3.6. Categorias Analisadas

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

Quadro 2: Categorias de Análise de Conteúdo da Pesquisa

Categoria	Descrição
Conhecimento da LGPD	Análise do nível de conhecimento e aplicação da lei.
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.
Conscientização e Consentimento	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 da LGPD e em normas editadas pela ANPD.
Controle de Acesso e Treinamento Interno	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.
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.
Especificações do cotidiano em consultórios de psicologia	Pontos de aplicação das diretrizes da lei direcionadas ao cotidiano de um consultório de psicologia.

(Fonte: adaptado de Brasil, 2021; ENISA, 2016).

4. RESULTADOS E DISCUSSÕES

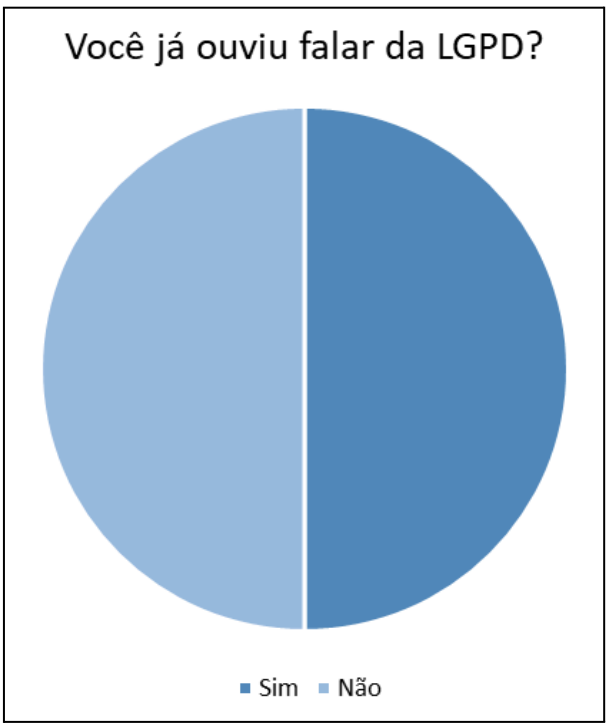
Com o objetivo de compreender as principais percepções e aspectos relacionados às categorias pré-definidas neste estudo, cada uma delas será analisada individualmente. Essa análise levará em conta sua base teórica e a aplicação prática no cotidiano, por meio da avaliação das informações obtidas nas entrevistas realizadas com os profissionais da área de psicologia.

4.1. Conhecimento da LGPD

A categoria inicial examinada nas entrevistas focou no entendimento da Lei Geral de Proteção de Dados no âmbito da psicologia. O propósito era medir o grau de familiaridade e a implementação dessa lei nas clínicas onde os entrevistados trabalhavam.

Percebeu-se que as respostas foram equilibradas; metade dos entrevistados possuía pouco ou nenhum conhecimento sobre a lei e seu propósito, enquanto a outra metade afirmou já ter algum contato, como ilustrado abaixo na Figura 5.

Figura 5: Ciência dos entrevistados sobre a LGPD



(Fonte: Elaboração Própria)

Conforme demonstra o gráfico, as respostas relacionadas a este tópico foram objetivas e, em geral, revelaram um conhecimento superficial da lei por parte dos entrevistados, como demonstrado em alguns dos trechos destacados a seguir:

> *Eu acho que já ouvi falar, assim, lendo artigos, sabe? Especificamente sobre essa lei, acho que só em artigos de aplicação, de pesquisa. Entrevistado 04*

> *Eu já trabalhei um coworking onde teve uma palestra sobre LGPD, nessa palestra foi quando eu descobri que existia isso. Entrevistado 05*

> *Já ouviu falar. Eu estudava para concurso há muito tempo atrás e aí tinha uma matéria lá que envolvia a LGPD, mas no curso de psicologia não. Entrevistado 10*

Cinco dos entrevistados afirmaram conhecer a lei, mesmo que superficialmente. Destes, três tomaram conhecimento desta em contextos diferentes de sua atividade-fim; lendo artigos, estudando para concursos ou assistindo palestras.

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

> *Não tinha ouvido falar, não assim, dentro desses termos, né? Entrevistado 09*

Em levantamento feito pela consultoria Alvarez & Marsal, em parceria com a ABNT, notou-se que para as empresas de médio e pequeno portes, a adequação não é uma prioridade, visto o alto custo. De acordo com o levantamento, cerca de 60% delas nem começaram a pensar sobre este assunto e como irão se adequar (Ganut, 2021, p. 5).

No que diz respeito ao impacto da lei nos consultórios onde os entrevistados atuam, observa-se que, na maioria dos casos, os profissionais reconhecem que a lei pode, de fato, influenciar suas rotinas de trabalho, conforme ilustração da Figura 6.

Figura 6: Impacto da LGPD na atuação dos entrevistados

(Fonte: Elaboração Própria)

Apesar de metade dos entrevistados não ter ouvido falar sobre a LGPD na pergunta anterior, conforme elucidado na Figura 5, nota-se que ao falar de uma possível influência da lei em seu trabalho, existe preocupação por parte dos entrevistados.

Alguns entrevistados afirmam já resguardar o sigilo não só dos dados pessoais de seus pacientes, mas também com anotações de evolução e relatos de sessão, como evidenciado nos trechos a seguir. Nota-se que especialmente o Entrevistado 8 ressaltou já ser cauteloso sobre o sigilo geral de suas sessões, demonstrando que ao início do tratamento busca tranquilizar o paciente sobre o sigilo dos dados trocados durante os atendimentos, conforme as transcrições abaixo.

Sim… Principalmente quando a gente fala de sigilo, né?! Entrevistado 01

De certa forma, acredito que sim.. Entrevistado 05

No contexto clínico dos atendimentos psicológicos, a gente já utiliza o sigilo de uma forma bem ética, e é primordial. É uma das premissas, das primeiras coisas que a gente fala com o paciente, né? Então, de certa forma, é algo

> *que acredito que seja fundamental [...] Tudo é muito sigiloso, de forma que a gente tem que manter ele sempre guardado, de uma forma bem sigilosa. Entrevistado 08.*

> *Com certeza. Não só nos atendimentos presenciais para quem faz, que já não é mais o meu caso, mas principalmente no que diz respeito ao formato online que a gente tem hoje, né? Entrevistado 09*

> *Eu nunca ouvi falar, então eu acredito que não. Entrevistado 03*

> *Acho que não. [...] mas como eu disse, assim, em relação ao sigilo ou à psicologia, eu acho que a gente já... já tem esse cuidado, já tinha esse cuidado. Acho que a gente lida com temas muito delicados. Então, já é meio que de se esperar que um psicólogo tenha muito cuidado com os dados, sabe?. Entrevistado 04*

Apesar do diminuto conhecimento específico da LGPD e suas disposições, os profissionais, de modo geral, se mostraram confiantes sobre a privacidade de seus atendimentos. Quando indagados se acreditavam estar em conformidade com a lei, apenas dois entrevistados (E03 e E06) responderam negativamente. Podemos inferir da resposta do Entrevistado 03 que sua crença em não estar alinhado à lei se deve ao desconhecimento da norma, como mostra o trecho a seguir.

> *Não sei. Acredito que não. Nunca ouvi falar. Entrevistado 03*

Em contrapartida, 80% dos entrevistados afirmaram acreditar estar em conformidade com a lei. Apenas um entrevistado (E05) foi categórico ao afirmar que está de acordo com a lei, enquanto os outros deram respostas afirmativas, porém pouco assertivas, de acordo com os trechos transcritos abaixo.

> *Eu não consigo nem falar de [...] acordo com a lei, mas pensando nessa questão do sigilo, da questão dos dados, das coletas de informação dos pacientes, acho que sim. Entrevistado 08*

> *Sim. Dentro da psicologia a gente responde ao nosso código de ética, e isso é estrutural. Na nossa formação inteira, o sigilo é fundamental. Então acho que antes de ter essa lei, os psicólogos já praticavam isso. E a gente tem a fiscalização do Conselho Federal de Psicologia. E se não cumprir, a gente pode perder nossa licença de atuação. Entrevistado 02*

O Código de Ética Profissional do Psicólogo (CEPP) foi publicado pelo Conselho Federal de Psicologia (CFP) em 2005, por meio da Resolução CFP nº 010, 2005, e estabelece diretrizes fundamentais para a prática da psicologia no

Brasil. O Código é um instrumento que surge para delinear à sociedade as responsabilidades e deveres do psicólogo, assegurando uma atuação ética e responsável, protegendo os direitos e a dignidade dos indivíduos com quem trabalham, além de oferecer diretrizes para a formação do psicólogo e balizar os julgamentos das suas ações, contribuindo para o fortalecimento e ampliação do significado social da profissão.

A privacidade e a confidencialidade além de fundamentais na prática da Psicologia, são abordadas pelo Código de Ética buscando assegurar que os dados e as informações pessoais compartilhadas no contexto terapêutico sejam protegidos e tratados com cautela. Esses valores não são apenas exigências éticas, mas também elementos relevantes para a construção de um ambiente de confiança entre psicólogo e paciente. Este tema é tratado em diversos artigos do CEPP, em maior ou menor intensidade, como exposto a seguir.

Artigo 9º (CFP, Resolução 010, 2005, p. 13): O principal fundamento sobre privacidade e confidencialidade está neste artigo, que estabelece que “é dever do psicólogo respeitar o sigilo profissional a fim de proteger, por meio da confidencialidade, a intimidade das pessoas, grupos ou organizações, a que tenha acesso no exercício profissional.” (CFP, Resolução 010, 2005). É notória a importância dada a resguardar a privacidade dos atendidos, garantindo que informações pessoais e sensíveis não sejam divulgadas.

A Lei Geral de Proteção de Dados alia-se ao dever de sigilo do paciente, previamente presente na área, corroborando com a importância e a necessidade da preservação dos dados pessoais dos pacientes em instituições de saúde (Telles; Maruco; Silva, 2021). Assim, com base na análise das entrevistas, é possível observar que os psicólogos, apesar de desconhecerem a LGPD a fundo, acabam se adequando aos termos da lei, devido à atenção dada à privacidade dos dados de seus pacientes, salientado diversas vezes no código de ética profissional da área.

4.2. Políticas de Segurança da Informação

Nesta categoria, examina-se a presença de políticas de segurança da informação (PSI), ou seja, se existem diretrizes estabelecidas nas clínicas que permitam o planejamento, a implementação e o controle de medidas voltadas à proteção da informação.

Buscando compreender como se dá o processo de obtenção e o grau de digitalização das informações, foi questionado aos entrevistados como é feita a coleta de dados pessoais dos pacientes. É interessante notar que 70% dos entrevistados afirmaram fazer uma anamnese na primeira sessão.

Segundo Porto (2001), Anamnese significa '*Ana'* - trazer de volta, recordar '*mnese'* - memória, e é realizada através da técnica da entrevista. Para isso é imprescindível o levantamento sistematizado dos dados do paciente realizado no primeiro momento (Santos *et al.*, 2010).

> *A gente faz uma anamnese, que é um questionário estruturado e aí ele fica a critério de cada profissional. Eu coleto as informações que eu preciso no primeiro atendimento, e aplico metade do questionário, pra deixar mais aberto, mais flexível. E aquilo que eu vejo que não é tão importante assim para o paciente naquele momento mas que é importante para mim no futuro, vou coletando depois. Entrevistado 01*

> *Depende, se eu estou trabalhando com avaliação psicológica, a gente faz uma anamnese e um registro mais completo [...] Mas se for para a clínica que eu estiver clinicando, o meu contrato é verbal. Os registros da sessão são escritos e as informações que vem surgindo, vão surgindo a partir da escuta mesmo. Entrevistado 02*

> *Olha, na minha atuação, pelo menos, até hoje, [...] eu só atendi sendo conveniada à clínica ou à faculdade. Então, eu sempre criei um formulário de anamnese, que apresentava para o cliente, geralmente, na primeira sessão. [...] é um formulário que a gente pergunta um pouco sobre a vida deles, sobre comorbidades, se faz tratamento de psiquiatria também, questões mais sensíveis de religião, como a pessoa se identifica, coisas gerais, para a gente ter mais um norte para o tratamento, e aí a gente guarda esse formulário de anamnese numa pasta do cliente. [...] e aí a cada sessão que a gente vai fazendo, eu vou fazendo minhas anotações. Entrevistado 03*

> *Bom, normalmente quando eu pego um paciente, a primeira sessão é a sessão de anamnese, coleta de dados. Fora isso, na sessão eu pergunto. Entrevistado 04*

> *Eu tenho inicialmente um formulário de anamnese, que é enviado via forms, no qual só eu tenho acesso também, mas nesse formulário são dados assim, bem básicos, não tem nada que vai expor muito a pessoa, só sobre demanda, informações básicas, contato, dados para emissão de recibo posteriormente, e as anotações prontuárias são todas feitas de forma manuscrita, guardados numa pasta, num local também, na qual só eu tenho acesso. Entrevistado 09*

> *Inicialmente, quando o paciente entra em contato, eu sempre aplico uma pré-anamnese, que é para ele preencher os dados em relação a dados pessoais mesmo, nome, CPF, dados de cadastro, e também alguns dados a respeito do objetivo terapêutico do paciente. Então eu envio essa pré-anamnese, que é através do Google Forms, ali do Google, que já vem diretamente só para mim. Entrevistado 08*

Durante a anamnese. Entrevistado 06

As respostas foram relativamente próximas: a maioria relatou fazer anamnese e coletar informações importantes ao longo dos atendimentos. Porém, alguns entrevistados afirmaram ter rotinas levemente diferentes e aparentemente mais seguras, como o E07, que envia uma ficha cadastral e recolhe a assinatura do paciente. Esta medida é interessante para o profissional, que coleta os dados pessoais e ainda o consentimento do paciente, o que acaba por resguardar legalmente o profissional em possíveis eventos futuros. Alinhado com esta prática, conforme e trecho destacado abaixo, o E10 envia um formulário para seu paciente via *google forms,* que ficam armazenados em seu *google drive* profissional, que apesar de não ser o ideal, ao menos oferece alguns recursos para proteção de dados.

> *Ficha cadastral, que eu envio para o email do paciente, para assinatura digital ou manual, mas escaneada e arquivada no prontuário, com o documento de identificação digitalizado. Entrevistado 07*

> *Quando o paciente está sendo admitido, quando é um paciente que vai começar o processo que a gente faz a ficha cadastral, eu uso o forms do Google. E esse forms, essa ficha, ela vai para uma planilha, todos os dados são jogados em uma planilha e essa planilha é protegida no meu drive. Entrevistado 10*

> *Atualmente minha coleta de dados é feita durante a consulta, e na consulta eu uso o Google Meet. Na minha antiga clínica, era feita via WhatsApp. Entrevistado 05*

Em sua resposta, conforme trecho destacado acima, o E05 afirmou que atualmente faz seus atendimentos por meio do *google meet*, plataforma de videochamadas da *google*, porém, em seu antigo emprego, utilizava o *Whatsapp*. Dentre as opções de redes sociais possíveis para tal, é questionável a escolha do *Whatsapp* para tal. 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.

Sabemos que há implementação de mecanismos de segurança pelo *WhatsApp Messenger,* que tentam garantir a privacidade dos usuários - considerado o primeiro pilar da segurança da informação. Porém, estes

mecanismos não mantêm a segurança dos usuários na sua totalidade. O surgimento da engenharia social é constituído por pessoas mal-intencionadas que utilizam técnicas como o *phishing*, o *spear phishing*, *smishing*, entre outras. Essas técnicas têm por objetivo atrair e induzir usuários a clicar em links maliciosos de fontes desconhecidas. O principal veículo da disseminação de ataques a vítimas pela engenharia social são os aplicativos de mensagens de texto e por e-mails, em especial o *WhatsApp Messenger*, concentrando quase 90% de mensagens de phishing em todo o mundo (Silva, 2021).

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 psicólogo que requisita as informações de seus pacientes é responsável pelo tratamento de dados, e em caso de irregularidades responderá da mesma forma ao ocorrido (Atheniense, 2019).

4.3. Conscientização e Consentimento

Foi abordado durante as entrevistas questões de conscientização dos profissionais das clínicas quanto à importância de manter em sigilo os dados pessoais dos pacientes e a responsabilidade que todos os funcionários possuem ao tratar estes 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 já haver a preocupação e o cuidado com o sigilo, de acordo com o CEPP, entretanto, não há nenhuma formalidade sobre a LGPD especificamente.

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar o uso de terceiros em alguma medida, dos dados de seu titular. Ele promove a personalidade, sendo meio para a construção e delimitação da esfera privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações (Teffé; Viola, 2020). Assim, o consentimento do paciente sobre a

obtenção de seus dados pessoais, deve ser obtido. De acordo com a LGPD, consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada (Brasil, 2020).

Quando perguntados se existe o hábito de obtenção do consentimento de seus pacientes, titulares dos dados, apenas dois entrevistados (E04 e E06) demonstraram não dar muita importância ao tema, conforme pode-se notar na transcrição abaixo.

> *Então, eu não faço contrato assinado com os meus pacientes. Entrevistado 04*

Todos os outros oito entrevistados, entretanto, demonstraram preocupação com o tema. Ou seja, apenas 20% dos profissionais participantes da pesquisa estão em desconformidade com a lei, já que de acordo com o art. 7º, “O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular [...]” (Brasil, 2020).

> *Sim. E se eu for usar eles para alguma pesquisa ou publicação de artigo, eu tenho que conversar com eles antes e eles têm que consentir. Eu tenho TCLE, [...] o termo de consentimento (Termo de Consentimento Livre e Esclarecido). Porque toda pesquisa que a gente faz que tem essas coisas tem que ir para o comitê de ética, e eles têm que assinar. Entrevistado 02*

> *Sim. É sempre uma coisa que eu pergunto logo na primeira assistência. Pergunto os dados e explico o que vai acontecer com eles, eventualmente se precisarem. Até, eu gosto de assegurar que é um direito da pessoa mesmo, sabe? Se ela quiser pegar aquele material um dia para olhar, ser lá. Eu gosto sempre de fazer um contrato no começo, explicar como vai acontecer.. Entrevistado 03*

> *Sim, apesar de nada ser exposto para fora, né, quando eles preenchem ali, eles colocam, não tem nenhuma pergunta que seja obrigatória. Mas de resto, todos eles tem liberdade para escolher se querem responder e como querem responder também. Entrevistado 09*

> *Eu pergunto se eu posso pegar os dados dele, então sim, eu busco obter consentimento. Entrevistado 05*

É interessante observar nas transcrições acima que a grande maioria dos profissionais relatou buscar o consentimento do paciente titular dos dados (oito entrevistados). Este assunto também é tratado no Código de Ética da área. Em

seu Artigo 16, inciso b, fica explícito que o psicólogo deve garantir "o caráter voluntário da participação dos envolvidos, mediante consentimento livre e esclarecido," especialmente em estudos, pesquisas e atividades voltadas à produção de conhecimento. Isso evidencia o compromisso de respeitar a autonomia dos participantes, que devem ser informados sobre os objetivos, procedimentos, riscos e benefícios antes de decidirem participar.

Além disso, o Artigo 14 reforça a importância do consentimento no uso de registros e observações da prática psicológica. Ele determina que "o usuário ou beneficiário, desde o início, seja informado" (CFP, Resolução 010/05) sobre qualquer meio de registro utilizado, seja gravação de áudio, vídeo ou observação, o que garante que as pessoas saibam como suas informações estão sendo capturadas e tenham a oportunidade de consentir ou não com esses registros.

O conceito de autonomia refere-se à perspetiva de que cada ser humano deve ser verdadeiramente livre, dispondo das condições mínimas para se auto realizar. Em consequência, no plano da relação clínica com o paciente, todas as intervenções carecem de consentimento informado, livre e esclarecido, sendo esta condição considerada como um imperativo de ética profissional (Pereira, 2004).

Foi questionado também se o consultório, representado pelo profissional entrevistado, atende menores de idade, e em caso de resposta positiva, como era obtido o consentimento para a coleta destes dados. Metade dos entrevistados relataram não atender menores de idade. Mesmo assim, alguns entrevistados (E08, E04, E03) já fizeram atendimento a menores de idade no passado e relataram ser obrigatório o consentimento dos pais ou responsável legal, como pode ser observado no texto destacado abaixo.

> *Eu atendi poucas vezes crianças, e meu público foco é mais adultos mesmo, entre adolescentes, mas para adolescentes também funciona da mesma forma que é com crianças. Quando uma criança inicia o tratamento, tem que trazer os pais ou o responsável. A primeira sessão é sempre com eles, e aí eu faço esse formulário de anamnese com os pais. Entrevistado 03*

> *Atualmente, a gente não está, acho que, com nenhum paciente que é menor de idade, mas eu já tive e aí eu coleto com os pais. Então, com o responsável que leva para a sessão. E se é online, normalmente é o responsável que me contata para marcar a sessão, né? Então, eu tenho sempre essa comunicação com os dois. Entrevistado 04*

> *Eu não atendo menores de idade. [...] Eu já atendi por pouquíssimo tempo, e tinha consentimento para coleta de dados, eu enviava só pros responsáveis. Entrevistado 08*

> *Atualmente eu não atendo menor de idades, só maior de idade. Entrevistado 05*

A outra metade dos entrevistados afirmou atuar com menores de idade, seja em atendimentos psicológicos individuais ou como psicólogo escolar. Todos afirmaram obter consentimento dos pais. Os trechos abaixo elucidam a abordagem dos profissionais entrevistados sobre o tema com maiores detalhes.

> *Então, eu trabalho em dois empregos [...] eu trabalho para um instituto, e nesse instituto a gente faz atendimento com crianças em situação de vulnerabilidade. Então, nesse instituto que eu trabalho, eu atendo crianças de 5 a 18 anos, porque o objetivo do projeto é atender crianças mesmo, né? E aí, lá, como a gente é um projeto inicial, a gente criou a documentação, e nessa documentação a gente tem o pai da criança, o tutor legal, que assina um documento liberando que essa criança faça os atendimentos, né?*
>
> *E aí o conselho, ele traz uma, ele traz uma obrigatoriedade de quando são crianças, por exemplo, que são separadas ou estão passando por separação judicial, ambas as partes precisam assinar. Entrevistado 01*

> *Eu atendo criança como psicólogo escolar. Que é em uma escola. Na matrícula, os pais, eles assinam com o consentimento liberando o uso da imagem da criança. Então, se tiver a foto, alguma coisa, a escola pode usar. Mas, geralmente, os meus atendimentos são muito pontuais. Porque a psicologia escolar é diferente da psicologia clínica. Os meus atendimentos são sempre feitos com outras pessoas no ambiente. Por exemplo, mediação… Se na semana de prova, a criança está tendo crise de ansiedade, vai para mim. Aí eu faço uma mediação e depois eu informo a equipe da orientação educacional. E a gente comunica aos pais que houve uma intervenção. Mas quando eu apliquei pesquisa com criança, pesquisa de desenvolvimento infantil, os pais tinham que assinar um documento autorizando o uso da imagem da criança. A gente não pode reforçar a criança de nenhuma forma. Então, não pode dar doce, não pode pagar a passagem, não pode dar nada porque é antiético. O Conselho Federal de Psicologia é muito rígido sobre pesquisa com crianças. O uso de imagem, de informação de criança tem proteção total. Então, você não pode tirar fotos. Se tiver foto, é só das mãos. Não pode ter nenhuma forma de reconhecimento da criança. Entrevistado 02*

> *Hoje eu atendo só uma, na verdade, que veio do presencial, e o primeiro atendimento é sempre feito com o responsável, então todo acordo, todo contrato é feito com os responsáveis desse menor.. Entrevistado 09*

> *Eu atendo adolescentes a partir dos 15 anos e para atendimento dos adolescentes eu faço um termo, eu peço autorização dos pais para iniciar o processo e tudo que envolve o processo. Então isso também significa ficha, prontuário, etc. Entrevistado 10*

> *Sim. Preciso do consentimento dos pais ou responsáveis legais. Entrevistado 07*

Nota-se que o Conselho Federal de Psicologia aborda com clareza a questão do atendimento a menores de idade, estabelecendo normas específicas para garantir a proteção e os direitos dessa população.

O Artigo 8º (CFP, Resolução 010, 2005, p. 12) determina que, para realizar o atendimento de crianças, adolescentes ou interditos, o psicólogo deve obter "autorização de ao menos um de seus responsáveis" (CFP, Resolução 010, 2005, art. 8º), em conformidade com a legislação vigente. Esse cuidado visa garantir que o atendimento esteja devidamente autorizado e que a integridade do menor seja respeitada. Caso não haja um responsável legal presente, o atendimento deve ser feito e comunicado às "autoridades competentes" (CFP, Resolução 010/05, §1º do Art. 8º), o que demonstra o compromisso do psicólogo com o bem-estar do menor, mesmo em situações de ausência de um responsável.

Além disso, o Artigo 13º (CFP, Resolução 010, 2005, p. 13) destaca que, ao informar os responsáveis sobre o atendimento, o psicólogo deve comunicar "o estritamente essencial para se promoverem medidas em seu benefício." (CFP, Resolução 010, 2005). Essa diretriz garante que a confidencialidade seja mantida, protegendo a intimidade do menor enquanto se busca seu melhor interesse. A orientação é reforçada pelo cuidado em manter o sigilo, exceto nos casos em que a comunicação é necessária para a segurança e proteção do atendido.

Esses artigos, ao lado de outros dispositivos do Código, garantem que o atendimento psicológico a menores de idade seja conduzido de forma ética, equilibrando o respeito à confidencialidade com a obrigação de zelar pela segurança e proteção do menor.

Artigo 14º (CFP, Resolução 010, 2005, p. 13): Esse artigo regulamenta o uso de “quaisquer meios de registro e observação da prática psicológica”, assegurando que o usuário ou beneficiário seja informado desde o início sobre qualquer registro de suas interações. Aqui, o foco é garantir que o paciente tenha controle sobre o uso de suas informações pessoais.

Vale ressaltar que a LGPD também especifica o

O consentimento representa instrumento de manifestação individual no campo dos direitos da personalidade e tem o papel de legitimar que terceiros utilizem, em alguma medida, os dados de seu titular. Ele promove a personalidade, sendo meio para a construção e delimitação da esfera

privada. Associa-se, portanto, à autodeterminação existencial e informacional do ser humano, mostrando-se imprescindível para a proteção do indivíduo e a circulação de informações (Teffé, Viola, 2020).

4.4. Controle de acesso e Treinamento Interno

As ações de proteção e controle de acesso devem ser ações de nível estratégicas que definam parâmetros gerais para proteger as informações de contra danos (alterações indevidas) e vazamentos não autorizados (Lyra, 2015).

O controle de acesso é um conjunto de medidas que garantem que os dados sejam acessados somente por pessoas autorizadas, por meio 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 (BRASIL, 2021, p. 10).

Com isso em mente, foi questionado aos entrevistados se suas clínicas possuem algum nível de controle de acesso aos dados em posse da clínica ou do profissional, com base nas necessidades de cada função exercida. Apesar de a maioria afirmar que existe cuidado com o acesso e utilizar mecanismos digitais para tal, como o *google drive*, 3 entrevistados afirmaram guardar documentos físicos em um armário protegidos com chave. Abaixo, encontram-se transcrições selecionadas para elucidar com maiores detalhes como é feito o controle dos profissionais entrevistados.

> *Um armário, que como eu divido com o meu colega, [...] e aí a gente anexa os documentos físicos lá, em papel, e [...] ele fica trancado. E lá no instituto é a mesma coisa, só que não fica trancado. Então eu não sei se seria de atrapalhar ou não. Mas, por exemplo, no meu segundo emprego, os documentos ficam de fácil acesso para qualquer pessoa, o que é algo que a gente já trouxe, que seria um problema e tal, mas como é algo que está fora do nosso controle, então a gente não consegue ter muita segurança em relação aos documentos. Entrevistado 01*

> *Armário com chave. Fica nisso e eu tenho o meu arquivo pessoal que fica na minha casa. Entrevistado 02*

> *Nos lugares que eu principalmente atuei, assim, atendendo o clima com dois lugares, foi no centro comunitário da faculdade e no CAPS, nesses dois lugares existe uma sala dos prontuários. Aí elas são divididas pelo nome e*

> *por ordem alfabética, e essas salas só pessoas que são da área da saúde, estagiários ou de outras áreas vão ter acesso. Entrevistado 03*

Vale reforçar que não há prejuízo de segurança simplesmente pelo fato de manter-se um arquivo físico com os documentos e informações dos pacientes, até porque, a própria LGPD regulamenta o tratamento de dados, tanto físicos quanto digitais. Entretanto, o custo de proteção dos documentos físicos costuma ser maior, conforme demonstrado por Andrade (2021);

> Já no armazenamento dos meios físicos, é essencial manter o local, além de trancado e acesso restrito, com câmeras de monitoramento 24h, identificando todas as pessoas que tiveram acesso ao arquivo. Bem como, seria ideal um acesso por biometria instalado na porta, assim, somente aquela pessoa autorizada poderia entrar no local (Andrade, Albuquerque, 2021).

Ainda para este questionamento, outros entrevistados afirmaram manter seus documentos armazenados em ambiente digital, protegido com senha, conforme exposto abaixo nas transcrições das entrevistas realizadas.

> *Eu coloco tudo no Google Drive porque fica até mais prático [...], só eu tenho acesso, eu realmente trabalho sozinha, então não tem ninguém que entre em lugar nenhum das minhas questões aqui de trabalho, principalmente no Google Drive, que é onde estão todas essas informações. Entrevistado 08*

> *Sim, como eu atendo online, né, eu atendo de casa, então tudo que diz respeito ao meu trabalho, nada é compartilhado com outra pessoa porque tudo é de uso pessoal, então ninguém tem acesso ao meu computador, ninguém tem acesso aos meus relatórios, é tudo bem privado. Entrevistado 09*

> *Todos os prontuários, todas as informações dos meus pacientes, ficam salvos nas minhas pastas do drive que são protegidas por senha. Entrevistado 10*

Apesar da maioria das respostas ao questionamento sobre controle de acesso terem sido guiadas pelo zelo com as informações dos pacientes, três entrevistados relataram algumas problemáticas (E04, E05 e E06). O E04, por utilizar um *Whatsapp* compartilhado com seu irmão, automaticamente compartilha todos os documentos com ele e vice-versa, já que dividem uma conta profissional. Este tipo de restrição de acesso pode ser problemático a depender da natureza do dado ou

da informação compartilhada, que pode ser sensível ou sigilosa, além dos riscos envolvendo a atuação de criminosos pelo *Whatsapp*. As respostas podem ser observadas abaixo.

> *Então, não tem muita coisa [...]. Mas atualmente meu consultório sou eu e minha irmã, a gente abriu uma clínica juntas. Então, a gente tem um WhatsApp e web juntas. Então, tudo que eu recebo, ela tem acesso também, e vice-versa. Entrevistado 04*

> *Atualmente eu uso para guardar meus prontuários um Google Drive com um e-mail profissional. [...] A clínica que eu estava trabalhando [...] não tinha nenhum tipo de autenticação de duas etapas ou biometria, mas só quem tinha acesso ao prontuário dos pacientes era o próprio psicólogo. Já a parte de dados pessoais como CPF, RG, CEP, etc. era aberta para que todo mundo que tinha acesso administrativo pudesse ver. Entrevistado 05*

> *Não. Eu tenho consultório privado e não possuo recepcionista. Entrevistado 06*

O E06, ao afirmar não possuir controle de acesso por trabalhar sozinho, chama para si a responsabilidade total pela obtenção, tratamento e armazenamento de dados de seus pacientes. Conforme já explorado anteriormente, por ser um agente de pequeno porte não há obrigação em nomear um profissional específico para este assunto, entretanto, traz novas funções para este profissional, que deve se preocupar com diversas outras questões relacionadas ao controle de acesso e tratamento destes dados, podendo gerar sobrecarga. Já o E05, apesar de afirmar fazer uso de um *google drive* atualmente, relatou que em seu emprego antigo não havia restrição de acesso a dados pessoais dos clientes, o que levanta grande preocupação, já que os mecanismos de engenharia social para obtenção de dados alheios por pessoas mal intencionadas é uma realidade global.

Visando analisar o nível de preparo dos profissionais para lidar com dados, os entrevistados foram indagados sobre já terem recebido alguma espécie de treinamento específico sobre a LGPD. Surpreendentemente, apenas um entrevistado (E07) afirmou já ter feito treinamento EAD. Apenas três respostas foram totalmente negativas (E01, E06 e E04), afirmando não ter recebido qualquer treinamento sobre o tema.

> *Treinamento EAD e preenchimento do termo de sigilo. Entrevistado 07*

Não. Específico assim, não. Entrevistado 04

Os outros entrevistados afirmaram não ter recebido treinamento específico sobre a LGPD, mas demonstraram algum grau de consciência sobre o tema, adquirido, segundo eles, por meio de palestra e também do Código de Ética Profissional do Psicólogo. Pode-se confirmar isso nos trechos das transcrições abaixo.

> *Não. Especificamente não, né? Não, a gente tem… A gente tem só [...] o código de ética, né? Inclusive na faculdade a gente tem disciplinas voltadas para estudar o código de ética do psicólogo. Entrevistado 02*

> *Então, tudo o que eu já escutei até hoje foi mais em relação à importância da gente proteger esses dados, que é sob hipótese nenhuma, levar o prontuário para casa, não deixá-lo espalhado por aí. Até mesmo para deixar na frente do paciente, porque a pessoa vai querer ler, ela vai querer olhar, e às vezes não é uma coisa que vai ajudar, sabe? Só em situações específicas ou em casos de solicitação. Entrevistado 03*

> *Atualmente trabalho sozinho, mas na minha antiga clínica não, isso não aconteceu. [...] o meu único treinamento foi no co-working que eu trabalhei antes, onde tive uma palestra sobre LGPD. Entrevistado 05*

> *Então, na verdade tem a questão do [...] código de ética, que tem todas essas questões em relação a tudo, tanto a questão dos dados, do paciente e tudo, quanto a questão da nossa forma de trabalhar, da ética mesmo. Entrevistado 08*

> *Não, nenhuma. A única coisa que a gente recebe é um caderninho do código de ética do Conselho de Psicologia, e assim, que cada um também interpreta de um jeito, então é comum que as pessoas tenham interpretações diferentes sobre algumas coisas que não estão tão claras dentro do código de ética. Entrevistado 09*

> *Proteção de dados de forma geral sim, por conta do nosso código de ética. Então desde o nosso primeiro semestre a gente já entra em contato com a sensibilidade que é o nosso trabalho, o quanto que a gente precisa resguardar isso. [...] em específico a LGPD não. Entrevistado 10*

4.5. Segurança de Dados Pessoais e Armazenamento

Nesta categoria, o foco está no processamento de dados pessoais, seja em bancos de dados ou outros sistemas relevantes (incluindo a nuvem). A análise também abrange o tratamento de dados pessoais por colaboradores, utilizando dispositivos como celulares.

Aos entrevistados, foi perguntado como se dá o armazenamento dos dados pessoais dos pacientes e quais medidas de segurança são adotadas para protegê-los. Como já discutido anteriormente, a maioria dos entrevistados ainda utiliza documentos físicos em suas rotinas de trabalho. Nesta pergunta, foram 60% os entrevistados que relataram usar papel para armazenar dados de seus pacientes. Os outros 30% usam serviços de nuvem, e um entrevistado possui servidor local, como explicitado abaixo.

> *Não, a gente usa é papel mesmo. Entrevistado 01*

> *São documentos em papel e tem o meu registro pessoal, que é uma agenda que eu tenho. Eu tenho algumas aqui, de clientes. Uhum. Aí eu vou acompanhando e vou fazendo anotações delas. Elas ficam aqui em casa. Entrevistado 02*

> *Olha, foi mais arquivo físico, mas também tem a questão de quando a gente atende também. Todo psicólogo sempre guarda pra si um caderninho com a notícia espacial. E eram sondados também, então a gente tem uma responsabilidade nisso. Mas até hoje, da forma que eu trabalhei, foi arquivo físico mesmo. Entrevistado 03*

> *Eu tenho um prontuário físico, porque eu gosto de coisas físicas. Então, por mais que eu pegue as informações ali no WhatsApp, eu anoto tudo no papel, eu imagino na pasta as informações de todos os pacientes. Então, é físico mesmo. Entrevistado 04*

> *Em prontuário físico. Entrevistado 06*

> *A parte dos prontuários ficam numa pastinha, separados, e os arquivos que eu tenho de anamnese eu gero um PDF também para deixar separado junto com os prontuários. Então fica tudo armazenado num armário, dentro do meu quarto, fechado, antes de ninguém ter acesso. Entrevistado 09*

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).

Vale reforçar que não existe problema em armazenar documentos físicos. Esta prática pode sim estar de acordo com a LGPD; entretanto, costuma ser uma forma mais onerosa; tanto mais trabalhosa, quanto mais cara de se manter a proteção destes dados, o que nos leva para o próximo questionamento.

Quando perguntados se existia alguma espécie de proteção aos dados

coletados, mesmo com o levantamento de exemplos físicos e também digitais (dispostos no Apêndice 1, pergunta 13) buscando ilustrar o que seriam artifícios de proteção, um entrevistado (E02) negou proteger os dados de forma sucinta. Apesar disso, todos os outros entrevistados afirmaram oferecer algum grau de proteção, como podemos ver a seguir.

> *Só o armário que fica trancado dentro do consultório. Entrevistado 01*
>
> *Geralmente é armário com tranca. Entrevistado 03*
>
> *Mantenho isso aqui no meu escritório de casa mesmo. Entrevistado 04*
>
> *A minha proteção seria o Drive. Não sei se isso conta como proteção. Mas atualmente é dessa forma que eu protejo os meus pacientes. E também na antiga clínica a proteção era o próprio sistema. Entrevistado 05*
>
> *Arquivo com chave. Entrevistado 06*
>
> *Sim. Senha forte e eventual verificação, confirmação por duas etapas. Entrevistado 07*
>
> *Só a senha, para entrar no meu Google Drive ali pelo meu Gmail profissional. Entrevistado 08*
>
> *Sim, num quarto trancado. Entrevistado 09*
>
> *Minha senha. Entrevistado 10*

A décima quarta pergunta trata de backup e busca entender melhor como é a abordagem dos participantes sobre esta medida de segurança. Segundo Franch (2008) o backup consiste na replicação idêntica dos dados que integram um documento, esta é uma técnica comum em qualquer contexto tecnológico, que se tornou necessária devido às experiências de perdas em nível mundial. Abaixo estão expostos trechos das entrevistas.

> *Eu, eu sou o backup. [...] Acho que o profissional pode ser uma fonte de backup, né? A psicologia é um pouco mais analógica, eu acho. Entrevistado 02*
>
> *Olha, até onde eu sei, pelo tempo que eu trabalhei assim, não. Foi tudo só físico mesmo. Se perder aquele ali, vai da sua cabeça mesmo. Já teve*

> *casos que eu vi de pessoas que atenderam e porventura perderam a folha do relatório, coisas assim, e teve que refazer com base no que a pessoa sabia. Mas não existe uma cópia ou nada desse tipo. Entrevistado 03*

Outros entrevistados afirmaram guardar folhas de rascunho para casos de perda (E01), enquanto os outros contam confiar totalmente nos serviços de nuvem, conforme fragmentos das transcrições realizadas.

> *Eu tenho minhas folhas de rascunho que ficam comigo. Pra mim, são meu backup, mas se eu perder também, aí acabou. Mas já é uma camada, né? Entrevistado 01*

> *Eu acredito que a própria nuvem seria o backup, mas eu posso estar falando besteira, [...] na minha antiga clínica, que eu trabalhava até agora, tinha um backup interno. Entrevistado 05*

> *Eu não sei se o backup é necessário quando o arquivo está na nuvem. Eu não tenho esse costume, eu não tenho esse costume, nem essa regularidade. Mas acho que na nuvem é uma forma de deixar salvo. Entrevistado 10*

Segundo Neto et al (2012, p.2) o backup pode ser definido como “cópia de segurança dos dados de determinado dispositivo de armazenamento que pode ser espelhado em outro dispositivo de forma a garantir a estabilidade dos arquivos e afastar a possibilidade de surpresas como a perda desses dados.” Ainda de acordo com Neto et al (2012) a prática rotineira de backup é vista como algo trabalhoso para muitos. Por isso muitos gestores de sistemas estão trabalhando na tarefa de simplificar e automatizar a tarefa de realização e backup, para minimizar o tempo gasto.

De acordo com Jesus e Schimiguel (2018, p.23) “para backup de pequeno e médio porte a solução de backup em nuvem apresenta grandes vantagens, devido ao fato de seu tamanho ser pequeno. Além da vantagem de utilização do backup em nuvem, que permite a inexistência de um local para armazenamento, e a escalabilidade, aumentando gradualmente o tamanho do backup de acordo com a necessidade, não requer um custo inicial”.

Ao levantar o tema de política de retenção de dados, a maioria demonstrou um certo alinhamento, ao afirmar que mantém os dados por 5 anos, de acordo com as transcrições das entrevistas realizadas.

> *A gente é obrigado a manter o prontuário de cada paciente durante cinco anos. Eu não posso fazer o descarte desses prontuários ou desses documentos antes disso. Entrevistado*

> *Tem que ficar cinco anos no arquivo guardado de relato de sessão, porque pode ser pedido para uso judicial. Para várias coisas, e até pra comprovar que você atendeu aquela pessoa, mas vai virar arquivo morto, né? [...] Acabou o tratamento. Entrevistado 02*

> *Na minha antiga clínica, se não me engano, os dados [...] eram apagados depois de 5 anos. Entrevistado 05*

> *A gente pode permanecer guardando os dados por 5 anos, após isso pode descartar de forma segura. Entrevistado 08*

> *Os dados ficam arquivados e aí, conforme as normas do Conselho, a gente pode, depois de cinco anos, entrar em contato com o Conselho para solicitar uma autorização para que a gente destrua esses registros. Entrevistado 09*

> *Sim, a gente tem uma legislação do CRP para isso. Então documentos psicológicos e prontuários a gente precisa manter por até 5 anos. Entrevistado 10*

A comparação das respostas obtidas revela um leve desacordo na política de retenção adotada pelos profissionais, conforme demonstrado abaixo.

> *Então, nos dois lugares que eu atuei, a retenção de dados funcionava assim; a gente mantinha os prontuários por até dez anos. E aí, passado esse tempo, e caso não tenha sido feito nada, o material geralmente é destruído. Entrevistado 03*

> *A gente não construiu essa política ainda, mas eu acho interessante, acho importante isso. Se não tá mais fazendo terapia há seis meses aqui, a gente apaga os dados e se ele quiser voltar a gente pega de novo. Entrevistado 04*

A tabela 1 foi elaborada com o objetivo de simplificar o entendimento geral da atuação destes profissionais quanto à retenção de dados que aplicam em suas rotinas, bem como a visualização e comparação destas práticas.

Tabela 1: Relação entrevistado x Tempo de retenção de dados

Entrevistado	Retenção dos dados
E01	5 anos
E02	5 anos
E03	10 anos
E04	Ainda não formulou esta política
E05	5 anos
E06	Não descarta
E07	Não descarta
E08	5 anos
E09	5 anos
E10	5 anos

(Fonte: dados da entrevista)

É possível observar nas respostas dadas pelos entrevistados que não há um consenso com relação ao tempo de armazenamento dos prontuários. 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 Psicologia (CFP), por meio da resolução CFP nº 007/2003, institui que o manual de elaboração de documentos escritos, determina que esses materiais (impressos e digitalizados) devem ser guardados pelo prazo mínimo de 5 anos, observando-se a responsabilidade por eles tanto do psicólogo quanto da instituição em que ocorreu a avaliação psicológica. Esse prazo poderá ser ampliado nos casos previstos em lei, por determinação judicial, ou ainda em casos específicos em que seja necessária a manutenção da guarda por maior tempo. Em caso de extinção de serviço psicológico, o destino dos documentos deverá seguir as orientações definidas no Código de Ética Profissional do Psicólogo. Após o prazo determinado de guarda, é preciso que o psicólogo destrua completamente o material, de forma que não seja possível a leitura ou visualização. Durante as entrevistas, alguns profissionais relataram não descartar os documentos, o que não é uma boa prática e pode gerar riscos.

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. Cotidiano em consultórios de psicologia

Nesta categoria são abordados pontos de aplicação das diretrizes da lei direcionadas ao cotidiano de um consultório de psicologia.

Política de privacidade

Com a implementação da LGPD, diversas empresas e organizações estão sendo obrigadas a criar ou revisar suas políticas de privacidade, tornando claro o tratamento dado às informações pessoais dos clientes. A política de privacidade deve detalhar como os dados são processados, quais tipos de informações são coletadas, de que maneira isso ocorre, a justificativa para a coleta, além de explicar claramente a finalidade dessa atividade. Também deve especificar se os dados serão ou não compartilhados com parceiros ou terceiros, já que o titular dos dados precisa ter controle sobre o uso e o compartilhamento de suas informações (Siebra; Xavier, 2020). De modo geral, os entrevistados informam seus pacientes sobre a política de privacidade exercida na clínica, com poucas exceções, conforme demonstram as respostas abaixo.

> *Esse contrato de sessão é porque assim, se você é psicólogo e trabalha numa clínica e se recebe pelo plano, a gente precisa ter o contrato escrito. Para abater do plano. Mas se for particular, o contrato é só verbal. Então eu, por exemplo, com meus clientes particulares, eu não mando documento nem nada. A gente conversa na sessão, na primeira sessão. E aí eu falo as regras da sessão. Tipo, por exemplo, se for ter falta, tem que avisar com 24 horas de antecedência, senão é cobrada a falta. Paga no final da sessão, por transferência bancária. Enfim, a gente conversa tudo isso verbalmente. A pessoa concorda ou não. Igual reajuste de valor, tudo isso. Mudança de horário. Se for numa clínica com plano de saúde, aí tudo tem que ser mais registrado. Mas se for no particular, é verbal. Mas a palavra na psicologia, de novo, tem um peso muito grande, até maior do que o escrito. O contrato oral é muito importante. Entrevistado 02*

> *Tem certas coisas que eu vou contar e certas coisas que eu não vou contar, sabe? [...] então eu acredito que esteja mais no sentido de explicar para a pessoa de que consiste o tratamento, o que vai ser feito com o que ela está me falando, sabe? Entrevistado 03*

> *Não do consultório. Normalmente é uma conversa na primeira sessão sobre o sigilo dos dados na sessão, mas não em relação, por exemplo, a outros psicólogos do consultório. Entrevistado 04*

> *Uma das primeiras coisas que eu faço com os pacientes é informar que ele está em um ambiente sigiloso. [...] Então eu não chego a falar sobre a política de privacidade de dados dos pacientes. Entrevistado 05*

> *Eu informo sempre no início, quando o paciente está iniciando o processo terapêutico, tem um contrato terapêutico também que eu envio, então lá está falando sobre a questão ética, sobre a questão do sigilo. Entrevistado 08*

> *Sim. Sempre que a gente dá início ao tratamento é informado sobre a questão do sigilo, de que acontece no site terapêutico. Mesmo que on-line é garantido o sigilo do paciente, isso também é colocado para ele como uma coisa importante para que ele esteja num lugar em que os dados, a privacidade dele também seja respeitada. Entrevistado 09*

> *Todas as vezes que eu vou iniciar um processo terapêutico, eu sempre falo que eles são protegidos por um sigilo e de que uma das únicas possibilidades de eu ter que quebrar esse sigilo é em caso de risco para a própria integridade física do paciente ou de pessoas próximas. Caso contrário, eu não tenho esse direito, então sim, eu informo. Entrevistado 10*

Prontuário

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.

Já para o CFP, conforme Resolução 005/2007, o prontuário é definido como documento único e individual, constituído de um conjunto de informações geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada. Tem caráter legal e sigiloso, possibilitando a comunicação entre os integrantes da equipe e o registro de suas considerações técnicas, sendo preenchido e compartilhado por todos os técnicos da instituição.

Neste sentido, foi questionado aos entrevistados quais eram as informações coletadas no prontuário de suas respectivas clínicas.

As respostas podem ser observadas nos trechos abaixo:

> *Então é prontuário mesmo, aí dentro tem; formulário de análise, dados iniciais, contato de terapia, que a gente sempre faz, explicar como vai*

> *funcionar, programas de alimentação de dados, que vai ficar até 10 anos, tudo guardadinho, caso a pessoa for me pedir, é um direito dela de ver aquilo para entender o material do psicólogo. Entrevistado 03*
>
> *Os arquivos deles? Em pasta. [...] fica no arquivo. [...] toda a documentação daquele cliente vai naquela pasta. Então, se ele me trouxe um desenho, eu vou tirar uma xerox e colocar naquela pasta. Se ele me trouxe fotos da família, eu vou tirar uma xerox e colocar naquela pasta. [...] aí tem a pasta dele com tudo. E olha só, eu já trabalhei em várias áreas da psicologia, aqui eu falei pra você, com avaliação psicológica de adulto e criança, psicologia escolar, psicologia clínica, trabalhei no SUS, no CAPS, e é tudo papel, tá? Tipo assim, tudo papel. No CAPS, eu que trabalhei no CAPS do Paranoá, eles têm uma sala gigante, assim, se pegar fogo acabou, não existe… Mas é tudo papel.[...] eu acho bem ruim. Mas eu acho muito difícil a gente conseguir adaptar isso, porque foi como eu te falei, é um trabalho muito manual. Entrevistado 02*
>
> *É, eu tenho um prontuário de cada paciente e normalmente o que eu faço, porque eu sei também que varia muito de profissional para profissional, né? Anotar por sessão, tipo um relatório de sessão. Eu anoto normalmente palavras-chave do que foi dito naquela sessão e mantenho no prontuário do paciente. Então esse é o armazenamento eu acho que de histórico de sessões. Entrevistado 04*
>
> *Os prontuários ficam ali, como eu falei, em cada pastinha tem um documento específico com o prontuário, as datas, a data de cada sessão, o que foi realizado em cada sessão, o que foi trabalhado, e nesses prontuários também é algo até que também envolve essa questão da ética, a gente não coloca todas as informações, até porque é impossível colocar tanta informação ali sempre do que as pessoas falam, mas a gente não coloca todas as informações detalhadamente com questões até bem sensíveis, bem profundas, a gente coloca ali o que foi trabalhado, assuntos importantes, intervenções que foram utilizadas, planos de ação ali, o que a pessoa vai fazer durante a semana até a próxima sessão, algo ali para ser memorizado ali, para ser verificado do que foi trabalhado na sessão. Essas questões bem mais pessoais e profundas realmente ficam entre eu e o paciente sempre. Entrevistado 08*
>
> *Sim, eu trabalho com os prontuários. Cada paciente tem seu prontuário individual, [...] sem nada que seja explícito, apenas alguns tópicos do que foi trabalhado em sessão para acompanhamento e quando necessário anotações pessoais que são separadas, mas que não vem informando nenhum dado pessoal. É mais para estudo de caso, registro de alguma demanda que precisa aprofundar mais. Entrevistado 09*
>
> *Sim, existe. Todo paciente, explicar mais ou menos assim. Todo paciente eu [...] crio uma pasta no drive. Dentro dessa pasta eu coloco a evolução do caso, formulação de caso e o planejamento de sessão, que são coisas muito diferentes.]...] tudo que eu vou produzindo eu vou guardando nessa pasta. Entrevistado 10*

Conforme estabelece a Resolução CRP-PR 005/2007, as informações devem ser registradas no Prontuário de forma sequencial, sem espaço entre elas, sendo que cada informação deverá ser datada, assinada e carimbada, constando o nome completo da(o) profissional e número de registro no CRP.

5. CONCLUSÃO

Na Sociedade da Informação, em que há um crescente destaque para o papel das informações no cotidiano, a necessidade de um gerenciamento seguro e responsável dos dados torna-se fundamental. As inovações tecnológicas têm acelerado o processamento e o armazenamento de dados, o que exige das empresas a busca por soluções eficazes para lidar com essas informações (Juarez *et al*, 2022).

As clínicas de psicologia, devido à natureza dos dados que coletam, especialmente dados sensíveis de saúde, precisam realizar o processamento e armazenamento dessas informações de forma segura, conforme a LGPD. A conformidade com essa legislação não só protege os direitos fundamentais dos titulares dos dados, mas também evita riscos legais e multas para os profissionais.

Diante da relevância da LGPD para clínicas de psicologia, que geralmente são micro ou pequenas empresas, optou-se por realizar esta pesquisa a fim de avaliar e compreender o nível de aplicação da LGPD (Lei nº 13.709 de 2018) no cotidiano destas organizações.

Foi realizada uma pesquisa exploratória com abordagem qualitativa, entrevistando 10 psicólogos atuantes em clínicas e consultórios. O roteiro foi elaborado com base em documentos orientadores da ANPD (Brasil, 2021) e da ENISA (ENISA, 2016), além de estudos diversos sobre os impactos da LGPD no contexto nacional.

O roteiro de entrevista 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 foram: Conhecimento da LGPD; Políticas de Segurança da Informação; Conscientização e Consentimento; Controle de Acesso e Treinamento Interno; Segurança de Dados Pessoais e Armazenamento; Especificações do cotidiano dos profissionais de psicologia.

Quanto ao conhecimento da LGPD, observou-se que a grande maioria dos entrevistados detinha pouco ou nenhum 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*.

Ao analisar as respostas sobre as razões para o conhecimento da LGPD ainda ser limitado na área da psicologia, uma das principais justificativas mencionadas foi o uso predominante de prontuários físicos (em papel) e a utilização limitada de softwares e tecnologia nos consultórios. Observou-se que grande parte das clínicas, especialmente as de menor porte, ainda organiza os documentos em formato físico ou está no início da transição para o uso de documentos digitais e softwares. Além disso, notou-se que muitos profissionais têm uma visão equivocada de que a LGPD se aplica apenas ao tratamento de dados digitais.

Um achado relevante da pesquisa destaca que, embora os psicólogos reconheçam a importância da proteção de dados de seus pacientes, muitos ainda armazenam essas informações em contas pessoais do *Google Drive*, e-mails e até mesmo *Whatsapp*. Essa prática apresenta riscos significativos em termos de segurança e conformidade legal, especialmente sob as diretrizes da LGPD. O uso de plataformas não especializadas e contas pessoais para o armazenamento de dados sensíveis pode expor as informações a violações de segurança, perda de dados e acesso não autorizado. Além disso, essa abordagem pode não garantir a observância das normas de consentimento, acesso, retificação e exclusão de dados, como exigido pela LGPD. É crucial que os profissionais da psicologia implementem soluções de armazenamento que sejam seguras, criptografadas e que ofereçam garantias adequadas de proteção de dados. Isso não apenas fortalece a confiança do paciente mas também assegura a conformidade com as leis de proteção de dados, minimizando riscos legais e melhorando a gestão de informações sensíveis.

Outro aspecto crítico revelado pela pesquisa é a lacuna no conhecimento dos psicólogos sobre procedimentos básicos de tratamento de informações no ambiente virtual. A falta de familiaridade com práticas seguras de gestão de dados evidencia uma urgente necessidade de treinamentos específicos na área. É imperativo que os profissionais de psicologia sejam capacitados não apenas em aspectos terapêuticos de sua profissão, mas também em competências tecnológicas que garantam a segurança e a privacidade dos dados de seus pacientes. Treinamentos regulares e a disseminação de boas práticas sobre o uso

seguro de tecnologias podem ajudar a mitigar riscos de vazamentos e violações de dados. Além disso, essas iniciativas contribuiriam significativamente para que os psicólogos pudessem não apenas compreender, mas também implementar de maneira efetiva as normas estabelecidas pela LGPD, promovendo um ambiente de atendimento que respeita e protege as informações sensíveis dos pacientes.

Outro ponto relevante foi o desconhecimento sobre a Resolução nº 2 da ANPD, que oferece condições especiais de adequação para pequenas empresas. Apesar de a maioria dos entrevistados já possuir preocupações éticas relacionadas ao sigilo de dados devido ao Código de Ética Profissional, poucos estavam conscientes das formalidades exigidas pela LGPD. Isso demonstra a necessidade de maior divulgação e treinamento sobre a lei, especialmente nas universidades e cursos de especialização.

Quanto à conscientização e treinamento dos funcionários das clínicas sobre a importância de manter o sigilo dos dados pessoais dos pacientes, a maioria dos entrevistados relatou que não recebeu treinamento específico, sendo que alguns nunca tinham ouvido falar sobre a lei.

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 *et al*, 2021).

Na prática, foi observado que os entrevistados afirmaram não haver, em suas respectivas clínicas, um tratamento especial ou diferenciado para os dados sensíveis. Uma das razões identificadas para que esses dados sejam tratados da mesma forma que os dados não-sensíveis é o fato de estarem todos contidos em um único documento, o prontuário, seja ele físico ou digital, o que o torna um documento essencial e de fácil acesso pelos funcionários do consultório.

Com relação às políticas de privacidade, as respostas indicaram que há um termo para assinatura dos pacientes ou um contrato verbal, permitindo o uso dos dados constantes no cadastro de informações pessoais e no prontuário.

De modo geral, a análise completa da base teórica, da legislação e dos dados coletados na presente pesquisa revelou que a transformação digital tem sido implementada nas clínicas de psicologia, especialmente após a pandemia do Covid-19. No entanto, os profissionais da área ainda demonstram incertezas e/ou

desconhecimento quanto à aplicação da LGPD no cotidiano de suas clínicas. O sigilo das informações continua sendo mantido, principalmente com base no Código de Ética Profissional do Psicólogo, com pouca influência da LGPD e um desconhecimento generalizado sobre suas possíveis sanções.

Esta pesquisa e seus resultados, contribuem para o aprimoramento da proteção de dados pessoais dos pacientes e para o desenvolvimento de melhores práticas de gestão de dados na área da saúde. Além disso, a pesquisa também pode auxiliar na conscientização de profissionais da área sobre a importância da LGPD e em sua adaptação às mudanças impostas pela legislação.

Além dos psicólogos, outros profissionais que trabalham com a implementação da LGPD, também podem ser beneficiados com as análises desta pesquisa, tendo em vista a descoberta de possíveis vácuos e pontos de atenção na implementação desta lei, além de promover a conscientização sobre os desafios legais e éticos que envolvem essa prática.

Por fim, observou-se que a transformação digital nas clínicas de psicologia ainda está em progresso, e a adaptação à LGPD está sendo feita de maneira gradual e limitada. A pesquisa destaca a importância de melhorar a conscientização sobre a LGPD e promover a adoção de boas práticas na gestão de dados sensíveis nas clínicas de psicologia.

A presente pesquisa abre oportunidades para estudos futuros, especialmente no aprofundamento das limitações identificadas, que foram abordadas superficialmente. Além disso, seria interessante explorar mais detalhadamente a transição do uso de prontuários físicos para digitais e o impacto de soluções tecnológicas específicas no cumprimento da LGPD e proteção dos dados dos pacientes. Outra temática que pode ser averiguada é a investigação do papel das associações e conselhos de psicologia na promoção de boas práticas de proteção de dados e sua influência na conscientização dos profissionais sobre a legislação.

REFERÊNCIAS

ABNT- Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação**. Rio de Janeiro: ABNT, 2013.

ABNT - 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.

Adjei, Joseph K. ***Monetization of Personal Identity Information: Technological and Regulatory Framework***. *Washington DC/EUA: IEEE Computer Society Washington*, 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: 04 set. 2024.

Almeida, Maria José Guedes Gondim; Figueiredo, Bárbara Barros; Salgado, Hakayna Calegaro; Torturella, Igor Moreira. **Discussão Ética sobre o Prontuário Eletrônico do Paciente**. Minas Gerais, 2016. DOI: http://dx.doi.org/10.1590/1981-52712015v40n3e01372015.

Andrade, Lorrayne Damazio; Albuquerque, Francisco Jovando Rebelo de. **O Impacto Da Lei Geral De Proteção De Dados Pessoais Nº 13.709/2018 Nas Empresas**. Teresópolis: Revista Cadernos De Negócios, v. 2, n. 1, 2021.

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: 05 set. 2024.

Bardin, Laurence. **Análise de conteúdo**. Lisboa: Edições 70, 1977.

BBC. **O escândalo que fez o Facebook perder US$ 35 bilhões em horas**. [s.l.], 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43466255. Acesso em 04 set.2024.

Bell, Daniel. **O Advento da Sociedade Pós-Industrial**. São Paulo: Cultrix, 1974

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: 04 set. 2024.

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: 04 set. 2024.

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: 13 mai. 2024.

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 mai. 2024.

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: 5 set. 2024.

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 set. 2024.

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: 15 mar. 2024.

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: 05 set. 2024.

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

Cardoso Neto, Celso Et Al. **Backup**. Revista De Trabalhos Acadêmicos, 2014.

Carvalho, Victor M. B. de. **O Direito Fundamental à Privacidade ante a Monetização de Dados Pessoais na Internet: apontamentos legais para uma perspectiva regulatória**. Natal, UFRN, 2018. Disponível em: https://repositorio.ufrn.br/handle/123456789/26851. Acesso em: 4 set. 2024.

Castells, Manuel. **A sociedade em rede**. São Paulo: Paz e Terra, 2001.

Cohen, Max F. **Alguns aspectos do uso da informação na economia da informação**. Ci. Inf., Brasília, v. 31, n. 3, p. 26-36, set./dez. 2002. DOI: https://doi.org/10.1590/S0100-19652002000300003.

Conselho Federal de Psicologia. **A Psicologia brasileira apresentada em números**. https://www2.cfp.org.br/infografico/quantos-somos/. Acesso em 04 set. 2024.

Conselho Federal de Psicologia. **Código de Ética Profissional do Psicólogo**. Brasília: Resolução CFP nº 10, de 27 de agosto de 2005.

Costa, Ramon Silva; Oliveira, Samuel Rodrigues de. Os direitos da personalidade frente à sociedade de vigilância: privacidade, proteção de dados pessoais e consentimento nas redes sociais. Belém: **Revista Brasileira de Direito Civil em Perspectiva,** v. 5 n. 2, Jul/Dez 2019. DOI:10.26668/IndexLawJournals/2526-0243/2019.v5i2.5778

Davies, Gary; Chun, Rosa; Silva, Rui Vinhas da; Roper, Stuart. ***The Personification Metaphor as a Measurement Approach for Corporate Reputation****. UK, Manchester Business School*, 2001. DOI: 10.1057/palgrave.crr.1540137.

Davis, Stanley. **Futuro perfeito**. São Paulo: Nobel, 1990.

Doneda, Danilo. **O direito fundamental à proteção de dados pessoais**. São Paulo: Atlas, 2014.

Duran,Laís Baptista Toledo; Barbosa, Laryssa Vicente Kretchetoff. **Lei Carolina Dieckmann: Atualização Jurídico Normativa Brasileira**. ISSN 21-76-8498. ETIC, 2015.

ENISA. G**uidelines 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. Acessado em: 03 set. 2024.

Enne, A. L. **À perplexidade, a complexidade: a relação entre consumo e identidade nas sociedades contemporâneas**. Comunicação Mídia E Consumo, 2008. DOI: https://doi.org/10.18568/cmc.v3i7.68.

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: 5 set. 2024.

Fornasier, Mateus De Oliveira. **Cambridge Analytica: Escândalo, Legado e Possíveis Futuros para a Democracia**. Rio Grande do Sul, Revista Direito em Debate, 2020. DOI: 10.21527/2176-6622.2020.53.182-195.

Foucault, Michel. **Vigiar e punir: nascimento da prisão**. Petrópolis: Vozes, 1977.

Galvão, Heideivirlandia Leite; De Oliveira, Alyne Leite; Gino, Bethsaida de Sá Barreto Diaz; Viana, Hudson Josino; Araújo, Francisco Gledison Lima; Benevinuto, Noélia Marques Silva; da Silva, Denis Leonardo Ferraz. **Incidentes de Segurança: Regulação e Prática de Vazamento de Dados Pessoais Frente à LGPD**. Id on Line Revista de Psicologia, v.18, n. 72.

Ganut, Marcos. **Pesquisa LGPD no Mercado Brasileiro**. Brasil: Alvarez e Marsal, 2021. Disponível em: https://www.alvarezandmarsal.com/sites/default/files/2021-11/E-book%20LGPD%20no%20Mercado%20Brasileiro.pdf. Acesso em: 25 ago. 2024.

Garritano, Célia Regina de Oliveira; Junqueira, Felipe Holanda; Lorosa, Ely Felyppy Soares; Fugimoto, Mayara Sanae; Martins, Wallace Hostalacio Avelar. **Avaliação do prontuário médico de um hospital universitário**. Revista Brasileira de Educação Médica, v. 44, n. 1, p. 1-6, 2020. https://doi.org/10.1590/1981-5271v44.1-20190123. Acesso em: 05 set. 2024.

Gartner Glossary. Disponível em: https://www.gartner.com/en/information-technology/glossary/big-data.

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 set. 2024.

Georg, Marcus; Junior, Aldery; Alves, Carlos; Nunes, Rafael. Os desafios da Segurança Cibernética no setor público federal do Brasil: estudo sob a ótica de gestores de tecnologia da informação. Brasil: **Risti**, 2023.

Gil, Antonio Carlos. **Métodos e Técnicas de Pesquisa Social**. São Paulo: Atlas, 1987.

Harlow, Lisa L.; Oswald, Frederick L. **Big Data in Psychology: Introduction to the Special Issue**. EUA: American Psychological Association, 2016.

DOI: http://dx.doi.org/10.1037/met0000120.

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**. Londres, UCL, 2020. DOI: https://doi.org/10.26512/lstr.v12i2.34692.

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.

Junior, Jair Francisco Nunes; Silva, Davi Lico da; Magnagnagno, Odirlei Antonio. **Análise comparativa dos prontuários eletrônico e físico sobre a segurança das informações**. Paraná: FAG Journal of Health, 2021.

Koerner, Andrei. Capitalismo e vigilância digital na sociedade democrática. São Paulo: **Revista Brasileira de Ciências Sociais**, 2021.

Lugati, Lys Nunes; Almeida, Juliana Evangelista de. **Da evolução das legislações sobre proteção de dados: a necessidade de reavaliação do papel do consentimento como garantidor da autodeterminação informativa**. Revista de Direito, Viçosa, v. 12, n. 2, 2020. DOI: doi.org/10.32361/2020120210597.

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

Machado, André Gustavo Carvalho; Moraes, Walter Fernando Araújo de Moraes. **Estratégias de customização em massa implementadas por empresas brasileiras.** Produção, v. 18, n. 1, p. 170-183, Jan./Abr. 2008.

Martins, Marcelo Guerra; Tateoki, Victor Augusto. **Proteção de dados pessoais e democracia: fake news, manipulação do eleitor e o caso da Cambridge Analytica**. Canoas: Revista Eletrônica Direito e Sociedade, 2019. DOI http://dx.doi.org/10.18316/REDES.v7i3.5610.

Michaelis. **Dicionário brasileiro da Língua portuguesa**. 2020. Disponível em: https://michaelis.uol.com.br/moderno-portugues/busca/ portugues-brasileiro/normatizar/. Data de acesso: 13 mai. 2024.

Mohyeddin, Mahsa Agha; Gharaee, Hossein. **FAHP-TOPSIS risks ranking models in ISMS**. IEEE, 7'th International Symposium on Telecommunications, 2014. Disponível em: https://ieeexplore.ieee.org/abstract/document/7000827. Acesso em 04 set. 2024.

Nakamura, Emilio Tissato; Formigoni, José Reynaldo, Ide, Marcos Cesar. **Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais**. São Paulo, 2020.

Nascimento, Felipe Thiago de Oliveira. **A Importância do Big Data nas Organizações**. Pernambuco: UFPE, 2018. https://www.cin.ufpe.br/~tg/2018-2/TG_SI/fton.pdf Acesso em 18 abr. 2024.

Paiva, Giovanna Silva Camelo; Silva, Edvan Gomes da; Alves, Carlos André de Melo; Rabelo, Rafael Nunes. **Aplicação da Lei Geral de Proteção de Dados Pessoais para agentes de tratamento de pequeno porte: análise em clínicas odontológicas**. Navus Revista de Gestão e Tecnologia, Florianópolis, SC, v. 14, p. 01-21, jan./dez. 2024. DOI: https://doi.org/10.22279/navus.v14.1869. Disponível em: https://navus.sc.senac.br/navus/article/view/1869. Acesso em 08 set. 2024

Pereira, André Gonçalo Dias. **O Consentimento Informado na Relação Médico-Paciente**. Coimbra: Estudo de Direito Civil, Coimbra Editora, 2004. Disponível em: https://hdl.handle.net/10316/89350.

Pinheiro, Patricia Peck. **Proteção de Dados Pessoais: Comentários À Lei N 13709/2018 (Lgpd)**. São Paulo, Saraiva, 2018. ISBN-10: 8553605280.

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. DOI: http://dx.doi.org/10.14349/sumneg/2019.V10.N23.A2. Disponível em: https://blogs.konradlorenz.edu.co/files/rsn_1023_02_peloso-piurcosky.pdf. Acesso em: 04 set. 2024.

Ramírez, Norman A. S. ***Ciberresiliencia. La integración entre Seguridad de la Información y continuidad de negocio.*** Colômbia: ACIS, 2021. DOI: https://doi.org/10.29236/sistemas.n159a7.

Reinaldo Filho, Demócrito. **Lei de Proteção de Dados Pessoais aproxima o Brasil dos países civilizados**. Rio Grande do Sul: Espaço Vital Independente, 2018. Disponível em https://espacovital.com.br/noticias/lei-de-protecao-de-dados-pessoais-aproxima-o-brasil-dos-paises-civilizados-17-07-2018. Acesso em 04 set. 2024.

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.

Rodotà, Stefáno. **A Vida na Sociedade da Vigilância "A privacidade hoje"**. São Paulo: Renovar, 2008. ISBN: 9788571476882.

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: 30 ago. 2024.

Santos, Neuma; Veiga, Patrícia; Andrade, Renata. **Importância da anamnese e do exame físico para o cuidado do enfermeiro**. Salvador: Revista Brasileira de Enfermagem, 2010.

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.

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.

Silva, Bruna Nunes da. **Segurança no *WhatsApp messenger* em um estudo de caso com ataque de phishing**. Goiás, 2021. Disponivel em: https://repositorio.pucgoias.edu.br/jspui/handle/123456789/3373. Acesso em 05 set. 2024.

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

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

Teffé, Chiara Spadaccini de; Viola, Mario. **Tratamento de dados pessoais na LGPD: estudo sobre as bases legais**. Civilistica.com. Rio de Janeiro, a. 9, n. 1, 2020. http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Data de acesso: 01 set.2014.

Thornhill, Stewart; Amit, Raphael. ***Learning About Failure: Bankruptcy, Firm Age, and the Resource-Based View***. Vol. 14. *Canada: Organization Science*, 2003.

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 Proteção de Dados, RGPD). Jornal Oficial da União Europeia, L 119/1, 4 mai 2016. Disponível em: https://gdpr-info.eu. Acesso em: 5 set. 2024.

Vance, Patricia de Salles; Ângelo, Claudio Felisoni de. Reputação Corporativa: uma Revisão Teórica. **Revista de Gestão USP**. São Paulo: v. 14, n. 4, p. 93-108, outubro/dezembro de 2007.

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. DOI: https://doi.org/10.20912/rdc.v15i36.18. Disponível em: https://san.uri.br/revistas/index.php/direitosculturais/article/view/18. Acesso em: 19 jul 2024.

Vilela, Gabriel Badim. **Lgpd: Um Estudo Sobre As Principais Responsabilidades E Penalidades Previstas Na Lei**. Goiás: Pontifícia Universidade Católica De Goiás Escola De Ciências Exatas E Da Computação, 2021.

Vozniuk; Andrii A.; Klymenko, Olga A.; Savchenko, Andrii V; Tarasevych, Tetiana Yu; Dudorov, Olexandr O. **Electronic Money and Payments as Means of Committing Crimes**. Londres: Academic Journal of Interdisciplinary Studies, 2020. DOI: https://doi.org/10.36941/ajis-2020-0069.

Werthein, J. A sociedade da informação e seus desafios. Brasília: Ciência Da Informação, **Revista IBICT**, 2000.

Whitman, Michael E; Mattord, Herbert J. *Threats To Information Security Revisited.* ***Journal of Information System Security****,* Vol. 8 *Issue* 1, p21-41. 21p*.,* 2012.

Ziraba, Abdallah; Okolo, Chinedum. ***The Impact of Information Technology (It) Policies and Strategies to Organization's Competitive Advantage***. GRIN Verlag, Santa Cruz, CA, United States, 2018. ISBN: 3668689962.

Zaia, Priscila; Oliveira, Karina da Silva; Nakano, Tatiana de Cássia. **Análise dos Processos Éticos Publicados no Jornal do Conselho Federal de Psicologia**. São Paulo, Psicologia: Ciência e Profissão Jan/Mar. 2018 v. 38 n°1, 8-21. https://doi.org/10.1590/1982-3703003532016.

Zuboff, Shoshana. **A era do capitalismo de vigilância: a luta por um futuro humano na nova fronteira do poder**. Tradução de George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

APÊNDICES

Apêndice A: Roteiro de Entrevista

1. Conhecimento da LGPD

1. Você já ouviu falar da LGPD?

2. Acredita que a LGPD afeta sua atuação?

3. Acredita estar em conformidade com a LGPD?

2. Políticas de segurança da Informação

4. Como é feita a coleta de dados pessoais dos pacientes?

   Ex. Ficha cadastral, coleta durante as consultas, anotações restritas ao terapeuta, etc.

5. Que tipos de dados pessoais são coletados e incluídos na ficha do paciente?

   Exemplos de dados pessoais: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer; endereço de IP (Protocolo da Internet) e cookies, entre outros.

   Exemplos de dados pessoais sensíveis: aqueles relativos à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

3. Conscientização e Consentimento

6. Você costuma obter consentimento dos pacientes sobre a coleta e uso de dados pessoais?

7. O consultório atende menores de idade? Se sim, como obtém consentimento para a coleta destes dados?

4. Controle de acesso e treinamento interno

8. Existe controle de acesso aos dados dos pacientes em seu consultório?

9. Os profissionais do consultório receberam algum treinamento ou conscientização sobre as disposições da LGPD ou proteção de dados pessoais?

10. Há uma política de senhas fortes e/ou troca periódica de senhas?

11. Existe uma política específica de retenção de dados?

    Ex. Excluir os dados ao fim do tratamento, manter dados para contato futuro, manter por x anos, etc.

5. Segurança de Dados Pessoais e armazenamento

12. Como os dados pessoais dos pacientes são armazenados?

    Ex. Computador, HD externo, nuvem, cadernos e/ou documentos em papel, arquivo físico, etc.

13. Existe alguma espécie de proteção a esses dados?

    Ex. Proteção por senha, verificação em duas etapas, criptografia, vpn, vigilante, armário com tranca, cadeado, etc.

14. Existe alguma espécie de backup para o caso de algum evento de perda e/ou vazamento de dados?

6. Cotidiano em consultórios de psicologia

15. Você informa os pacientes quanto à política de privacidade do consultório?

16. Existem prontuários dos pacientes? Se não, como é armazenado o histórico do paciente?