Pontifícia Universidade Católica
do Rio de Janeiro

Thaís Soares de Souza

Papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à Lei Geral de Proteção de Dados (LGPD).

Dissertação de Mestrado

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração de Empresas, do Departamento de Administração de Empresas da PUC-Rio.

Orientadora: Profa. Patrícia Amélia Tomei

Rio de Janeiro
Março de 2023

PONTIFÍCIA UNIVERSIDADE CATÓLICA
DO RIO DE JANEIRO

Thaís Soares de Souza

Papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à Lei Geral de Proteção de Dados (LGPD).

Dissertação apresentada como requisito parcial para obtenção do grau de Mestre pelo Programa de Pós-graduação em Administração de Empresas, do Departamento de Administração de Empresas da PUC-Rio à Comissão Examinadora abaixo:

Profa. Patrícia Amélia Tomei
Orientadora
PUC-Rio

Profa. Adriane Domingues Quelhas
Universidade Federal Fluminense – UFF

Profa. Alessandra de Sá Mello da Costa
PUC-Rio

Profa. Patrícia Macedo Guimarães
Gama Lima e Guimarães Advocacia e Consultoria

Rio de Janeiro, 08 de março de 2023

Thaís Soares de Souza

Graduou-se em Direito pela Universidade Federal do Estado do Rio de Janeiro. Possui especialização em Direito Tributário e MBA em Gestão de Projetos. Atua como Consultora em Programa de Adequação de Empresa à LGPD.

Ficha Catalográfica

Souza, Thais Soares de

Papel da cultura organizacional no processo de adaptação das organizações de saúde brasileiras à Lei Geral de Proteção de Dados (LGPD) / Thais Soares de Souza ; orientadora: Patrícia Amélia Tomei. – 2023.
118 f. ; 30 cm

Dissertação (mestrado)–Pontifícia Universidade Católica do Rio de Janeiro, Departamento de Administração, 2023.
Inclui bibliografia

1. Administração – Teses. 2. Cultura organizacional. 3. Organizações de saúde. 4. LGPD. 5. Dados sensíveis. 6. Proteção de dados. I. Tomei, Patrícia Amélia. II. Pontifícia Universidade Católica do Rio de Janeiro. Departamento de Administração. III. Título.

CDD: 658

Agradecimentos

Em primeiro lugar, agradeço a Deus pelas bênçãos derramadas sobre minha vida e por me conceder a graça de cursar o mestrado, mesmo diante de uma insegurança que parecia não ter fim e de um cenário pouquíssimo favorável.

Ainda que eu passe todos os meus dias agradecendo, jamais será suficiente para alcançar tamanha gratidão.

Aos meus pequenos filhos, Arthur e Julia, minha fortaleza, vocês foram essenciais para a superação desse desafio. Cada choro pela distância da mamãe foi o combustível que me fortaleceu para conquistar tudo por vocês e para vocês.

Ao meu marido Marcos, agradeço por teu amor, pela compreensão, pelo apoio, pelo cuidado nos dias fáceis e nos difíceis também.

Aos meus pais, Gilberto e Eliane, minha gratidão retrocede a todos os meus dias que antecedem a essa conquista. Mostrar-me o quanto sou capaz de superar quaisquer barreiras me fez forte, focada e determinada. Além de tudo isso, juntamente com minha sogra, Maria, foram meu suporte no cuidado com as crianças para que eu pudesse participar das aulas e construir essa dissertação.

Às minhas irmãs Carla e Sabrina, agradeço por torcerem e cuidarem de mim como uma parte de vocês.

À minha psicóloga Patrícia Renaldo, agradeço por me ajudar a me conhecer melhor, ultrapassando todas as barreiras que eu mesma um dia criei; por me ouvir e por me ajudar a transformar minhas lamentações em ações.

À minha orientadora Prof.ª. Patrícia Tomei, agradeço por me aceitar em momento tão avançado e de forma tão repentina. Agradeço por me acolher, por acreditar nas minhas ideias, por me agraciar com tanta sabedoria, humildade e paixão pelo que faz e, sobretudo, por ter tido muita paciência e disponibilidade. Você é incrível e te levarei para sempre em meu coração.

Por último, e não menos importante, agradeço aos profissionais com os quais debati a proposta de pesquisa e os que aceitaram me conceder entrevista, fazendo parte desse importante projeto pessoal.

O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001.

Resumo

Souza, Thaís Soares de; Tomei, Patrícia Amélia. **Papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à Lei Geral de Proteção de Dados (LGPD)**. Rio de Janeiro, 2023. 118p. Dissertação de Mestrado – Departamento de Administração de Empresas, Pontifícia Universidade Católica do Rio de Janeiro.

Com o intuito de regulamentar o uso das informações, em 2018 foi sancionada a Lei Geral de Proteção de Dados (LGPD), mas sua aplicabilidade prática e seu alcance ainda não são claros e variam segundo a cultura de cada Organização. Esta pesquisa tem como objetivo analisar o papel dos diferentes elementos da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à LGPD, consideradas relevantes por se tratar de um dos ambientes com maior circulação de dados sensíveis. Foram realizadas entrevistas semiestruturadas com gestores de Organizações de Saúde e os casos analisados evidenciaram que: (i) há um movimento crescente de fortalecimento da proteção da vida privada; (ii) há brechas, na maioria das vezes relacionadas à conduta humana; (iii) o porte da organização e o seu perfil empreendedor são fundamentais no processo de adaptação à LGPD; (iv) este processo não inclui a preocupação com artefatos visíveis, sobretudo nas áreas com predominância da atividade-fim, como os espaços de circulação de pacientes, tampouco se valem de jargões corporativos para a fixação da identidade cultural; e (v) a Cultura Organizacional e a internalização facilitaram a adequação à LGPD. Por fim, sugerem-se estudos futuros com amostras segmentadas, que permitam um diagnóstico cultural mais amplo e favoreçam ações estratégicas segundo as diferentes Culturas Organizacionais.

Palavras-chave

Cultura organizacional, Organizações de Saúde; LGPD; Dados Sensíveis; Proteção de Dados.

Abstract

Souza, Thaís Soares de; Tomei, Patrícia Amélia (Advisor). **Role of Organizational Culture in the adaptation process of Brazilian Health Organizations to the General Law of Data Protection (GLDP).** Rio de Janeiro, 2023. 118p. Dissertação de Mestrado – Departamento de Administração de Empresas, Pontifícia Universidade Católica do Rio de Janeiro.

In order to regulate the use of information, the General Law of Data Protection (GLDP) was sanctioned in 2018, but its practical applicability and scope are still unclear and vary according to the culture of each Organization. This research aims to analyze the role of the different elements of Organizational Culture in the process of adaptation of Brazilian Health Organizations to the GLDP, considered relevant because it is one of the environments with the highest circulation of sensitive data. Semi-structured interviews were conducted with managers of Health Organizations and the cases analyzed evidenced that: (i) there is a growing movement to strengthen the protection of private life; (ii) there are breaches, mostly related to human conduct; (iii) the size of the organization and its entrepreneurial profile are fundamental in the process of adaptation to the GLDP; (iv) this process does not include the concern with visible artifacts, especially in areas with a predominance of the end-activity, such as patient circulation spaces, nor does it make use of corporate jargon for the establishment of cultural identity; and (v) Organizational Culture and internalization facilitated the adaptation to GLDP. Finally, future studies with segmented samples are suggested, allowing a broader cultural diagnosis and favoring strategic actions according to the different Organizational Cultures.

Keywords

Organizational Culture, Health Organizations; GLDP; Sensitive Data; Data Protection.

Sumário

Lista de Figuras

Lista de Tabelas

Lista de Abreviatura

ANPD – Autoridade Nacional de Proteção de Dados

ANS – Agência Nacional de Saúde Suplementar

CC – Código Civil

CDC – Código de Defesa do Consumidor (Lei nº 8.078/90)

CFM – Conselho Federal de Medicina

CIA – *Central Intelligence Agency* EUA

CIHA – Comunicação de Internação Hospitalar e Ambulatorial

CMD – Conjunto Mínimo de Dados

CPF – Cadastro de Pessoa Física

CPP – Código de Processo Penal (Decreto Lei nº 3.689/41)

CRFB – Constituição da República Federativa do Brasil

CVF – *Competing Values Framework*

DPO – *Data Protection Officer* (Encarregado dos Dados)

DUDH – Declaração Universal dos Direitos do Homem

EUA – Estados Unidos da América

GDPR – General Data Protection Regulation Europa

ISO – International Organization for Standardization

LAI – Lei de Acesso à Informação (Lei nº 12.527/11)

LDA – Lei sobre Direitos Autorais (Lei nº 9.610/98)

LGPD – Lei Geral de Proteção de Dados (do Brasil)

NSA – National Security Agency (Agência de Segurança Nacional EUA)

OEA - Organização dos Estados Americanos

ONU – Organizações das Nações Unidas

SAMU – Serviço de Atendimento Médico de Urgência

SCNES – Cadastro Nacional de Estabelecimentos de Saúde

SERPRO – Serviço Federal de Processamento de Dados

SIA/SUS – Sistema de Informação Ambulatorial

SIH/SUS – Sistema de Informação Hospitalar

SISAB – Sistema de Informação em Saúde para a Atenção Básica

SISVAN – Sistema de Vigilância Alimentar e Nutricional

Lista de Quadros

1.Introdução

1.1 Problema da Pesquisa

O homem, desde os primórdios, carrega o fardo de estar com outras pessoas, travando batalhas incansáveis para ser um indivíduo autônomo e para preservar suas experiências, seus espaços e sua liberdade de pensar, agir e viver. Todavia, garantir essa benesse nem sempre foi fácil, já que, no início das civilizações, o fundamento da vida em sociedade preceituava restrição à proteção do indivíduo, limitando-a, objetivamente, aos planos físico e patrimonial, o que anulava qualquer ocorrência que envolvesse seu âmago e suas liberdades individuais, perpassando por um severo controle de informações por Estados totalitários.

Em momento seguinte, a sociedade passou por um importante avanço, quando a tutela jurídica foi ampliada para o campo da subjetividade, de modo que se compreendeu que não bastava criar mecanismos de proteção ao indivíduo apenas para mantê-lo vivo e evitar que seu patrimônio fosse molestado, mas seria necessário garantir meios que possibilitassem desfrutar dos regalos da vida, o que lhe permitiria, enfim, ser reconhecido como um indivíduo.

Tempos depois, o movimento da subjetividade se associou à inovação tecnológica e ao avanço jornalístico que, ao mesmo tempo, possibilitavam a circulação de informações e a invasão à vida privada, desafiando os mecanismos precários de gestão da informação.

A partir de então, embora a proteção à privacidade ainda não fosse tratada com a merecida relevância, diante das diversas ocorrências de violação, que recebiam tratamentos contraditórios, tornou-se imperioso o surgimento de um novo direito. Nascia, então, o direito da personalidade, cuja aplicação prática, embora ainda discreta, teria nascido no ano de 1880 a partir da expressão “The Right To Be Let Alone” do jurista americano Thomas McIntyre Coley, presidente da Suprema Corte de Michigan.

Não obstante o importante feito de Coley, o debate sobre privacidade somente ganhou efetiva robustez no ano de 1890, a partir da publicação do artigo

"The Right to Privacy", de Warren e Brandeis, pela Harvard Law Review, considerada uma avançada discussão para a época, que seguiu como principal referência teórica até a metade do século XX, quando, em 10 de dezembro de 1948, a Assembleia Geral das Nações Unidas proclamou a Declaração Universal dos Direitos Humanos que passou a reconhecer, dentre outros direitos, a dignidade a todos os membros da família humana, bem como os fundamentos da liberdade e da justiça, sendo seguida pela Lei Fundamental da República Federal da Alemanha (1949), pela Convenção Europeia dos Direitos Humanos (1950) e pelo Tratado sobre o Funcionamento da União Europeia (Roma – 1957).

Seguidamente, há registros do debate prático de questões relativas à proteção à privacidade nos EUA, datado de 07 de junho de 1965, quando a Suprema Corte Americana julgou o caso *Griswold v. Conecticut*. Mas, apesar desse movimento de fortalecimento da proteção à vida privada que começava a se delinear, a regulamentação ainda era deficiente e limitada.

Diante desse cenário, a Europa, mais uma vez saiu na frente e, em 1970, aprovou o *Hessiches Datenschutzgesetz* (Ato de Proteção de Dados de Hesse - na Alemanha), revisada e implementada em 1978, abrindo caminho para discussão adicional sobre proteção de dados dentro e fora da República Federal Alemã.

Ao Ato de Hesse seguiram o Sw. Datalagen (Ato de Dados da Suécia de 1973); as Constituições de Portugal (1976) e da Espanha (1978) e a Convenção unificada sobre tratamento de dados pessoais, elaborada em conjunto por França, Noruega, Áustria e Suécia (1981).

Os países europeus possuíam, ainda, diversos outros normativos isolados que referenciavam, ainda que de maneira mais superficial, a proteção de dados e da privacidade, como a Convenção nº 108 do Conselho da Europa (1981); a Carta dos Direitos Fundamentais da União Europeia (2000); o Protocolo Adicional (ETS nº 181) à Convenção nº 108 (2001); o Protocolo de alteração (CETS nº 223) à Convenção nº 108 (2018) e a Diretiva 46/95 (1995 – União Europeia).

Conquanto, com o transcurso dos anos, mais intensamente em relação à sociedade do Século XXI, tem-se assistido a evolução exponencial da economia digital, com o avanço da globalização e o progresso das tecnologias da informação que, conforme salientam os autores Cunha, Hierro e Silva (2020), para além de proporcionarem avanços relevantes, como o desenvolvimento da

medicina e a possibilidade de comunicação entre indivíduos a um nível transfronteiriço e em tempo real, também podem apresentar outras consequências nocivas, como a circulação intensa, ilimitada e incontrolada de dados pessoais.

Neste cenário, mais uma vez, a Europa norteou uma das mais importantes ações públicas de proteção à privacidade, estabelecendo um único marco regulatório digital que visava mitigar as consequências negativas do avanço tecnológico, mediante a estruturação de políticas legislativas que possibilitavam a circulação segura de dados pessoais na União Europeia e com outros países e organizações internacionais, de modo a assegurar elevado nível de proteção dos dados.

Então, nesta conjuntura, em 27 de abril de 2016, nasceu o General Data Protection Regulation (GDPR), sob o nº 2016/679, pelas mãos do Parlamento Europeu e do Conselho da União Europeia, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação dessas informações no âmbito da União Europeia.

Após período de adaptação, o GDPR passou a ser exequível em 25 de maio de 2018, introduzindo mudanças de paradigmas e de procedimentos e estabelecendo alterações relevantes no funcionamento das Organizações e nos respetivos processos, de forma que deveriam passar a integrar a proteção de dados na Cultura Organizacional, obrigando os Estados-Membros a atualizarem suas leis nacionais sobre o tema e se tornando referência para outros países, como Estados Unidos, México, Índia e Brasil.

No Brasil, a proteção à privacidade ganhou evidência a partir da promulgação da Constituição Cidadã, de 1988, que se tornou referência para o legislador infraconstitucional quando da elaboração do Código de Defesa do Consumidor (Lei nº 8.078/1990); da Lei nº 9.296/1996 e do Código Civil (Lei nº 10.406/2002).

De modo contínuo, acompanhando a ascensão do tema pelo mundo e objetivando concentrar a regulamentação da proteção de dados, em 14 de agosto de 2018, foi sancionada, pelo Presidente da República Federativa do Brasil, a Lei nº 13.709/2018, conhecida como a Lei Geral de Proteção de Dados (LGPD) cuja inobservância por agentes responsáveis pelo tratamento de dados de pessoas naturais pode sujeitá-los às sanções legais em variados graus.

Todavia, tal como ocorreu com o GDPR, a LGPD também passou por um

período de vacância e somente entrou em vigor em sua integralidade a partir de 01 de agosto de 2021, compelindo forçosa adequação da Cultura Organizacional das empresas brasileiras.

Salienta-se que, antes do estabelecimento de regulamentos próprios, os processos gerenciais de tratamento de dados pessoais observavam o arbítrio individual quanto às decisões de manuseio, tratamento, armazenamento e descarte.

Porém, neste novo contexto, cada empresa e cada setor dentro da própria empresa, deve buscar sua melhor forma de adaptação para o cumprimento da LGPD, isto é, deve estudar novos mecanismos de processamentos de dados e criar procedimentos que estejam alinhados à sua Cultura Organizacional que, segundo Schein (1992), é percebida por meio de artefatos como valores, crenças e normas compartilhados que influenciam a maneira como os empregados pensam, interagem, sentem-se e comportam-se nas Organizações.

Contudo, determinados segmentos de mercado tiveram a Cultura Organizacional impactada de maneira mais significativa, em razão das peculiaridades e sensibilidade dos dados por eles tratados, como é o caso das Organizações de Saúde.

As unidades de tratamento de saúde humana são responsáveis por diversos dados sensíveis que, embora já fossem preservados pelo sigilo da relação médico-paciente[1], receberam proteção reforçada do legislador, visto que são fundamentais para o desenvolvimento da própria estrutura de saúde, bem como para a formulação e implementação das políticas públicas correspondentes.

Continuamente, salienta-se que, conforme alerta Frith et al., (2014), o gerenciamento da Cultura Organizacional tem sido visto cada vez mais como importante alavanca para o desempenho das Organizações de Saúde.

No mesmo sentido, Hernández Junco et al. (2008), relatam que componentes da Cultura Organizacional do Setor de Saúde estão relacionados à atmosfera local e ao comprometimento da força de trabalho, favorecendo a satisfação dos fornecedores (Zazzali et al., 2007), a comunicação de erros na administração de medicamentos (Wakefield et al., 2001) e a adoção de práticas para melhoria da qualidade (Shortell et al., 1995).

[1] Relação complexa caracterizada pelos compromissos e deveres firmados por ambas as partes.

No entanto, Rocha et al. (2014), após análise do resultado do estudo da psicodinâmica do trabalho em saúde, salientam que as instituições de saúde possuem, em regra, modelos tradicionais de administração e suas práticas de trabalho são sustentadas pelos princípios da organização científica do trabalho, o que, segundo os autores, na percepção dos trabalhadores analisados, faz com que os valores e as práticas organizacionais que transpõem a hierarquização sejam o controle e a rigidez no trabalho, o individualismo e a competição entre os indivíduos e a desvalorização dos trabalhadores, dificultando o trabalho em equipe, o desenvolvimento de ações de interdisciplinaridade na atenção à saúde e o alcance da qualidade dos serviços prestados.

Os autores advertem, ainda, ser necessária a transformação das práticas em saúde por meio da adoção de novas formas de gestão e de organização do trabalho como substitutos dos modelos tradicionais, privilegiando a gestão compartilhada, o trabalho em equipe, a valorização das necessidades dos indivíduos (pacientes e trabalhadores) e a humanização das relações interpessoais, o que é corroborado por Vegro et. al. (2016) que complementam pela necessidade de gestão do trabalho em saúde utilizando-se formas mais flexíveis e dinâmicas.

Segundo Nystrom (1993), para alcançar os resultados desejados, as Organizações de Saúde que reforçam sua Cultura Organizacional apresentam menor número de conflitos, maior segurança no trabalho e estabilidade e tratamentos mais adequados.

Neste sentido, desde a promulgação dos primeiros regulamentos relacionados à proteção da privacidade no Brasil, diversos autores delinearam o alcance e a relevância dos normativos, viabilizando a compreensão teórica do tema, sobretudo, com fundamento na CRFB e no CDC, pelos quais as empresas sustentavam suas soluções.

No entanto, muitas vezes, os resultados alcançados não eram satisfatórios por impropriedade do fundamento utilizado, carecendo de mecanismos mais específicos.

Deste modo, aplicar as especificidades da LGPD tornou-se fundamental. Porém, por se tratar de mecanismo ainda pouco conhecido, a literatura é superficial no que tange à profundidade de aplicação prática, principalmente no que se refere ao tratamento de dados sensíveis.

Assim, considerando-se os desafios inseridos no campo da proteção de dados pessoais e da privacidade, sobretudo no que se refere às informações na área de saúde, bem como a insuficiência de garantias efetivas e as peculiaridades do sistema gerencial desse segmento de mercado, temos a seguinte questão: "Qual o papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à LGPD?"

1.2 Objetivos: principal e específicos

O objetivo principal da presente pesquisa é analisar o papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à LGPD.

Para o alcance do objetivo principal, faz-se necessário atender os seguintes objetivos específicos secundários:

- Compreender como se dava o tratamento de dados de pessoas naturais nas Organizações de Saúde em momento anterior à publicação da LGPD.
- Compreender como se dava o tratamento de dados de pessoas naturais nas Organizações de Saúde no período compreendido entre a publicação e a entrada em vigor da LGPD.
- Compreender o que a LGPD representa para as Organizações de Saúde brasileiras.
- Analisar o papel dos diferentes elementos da Cultura Organizacional das Organizações de Saúde brasileiras em relação à forma de adaptação à LGPD.

1.3 Delimitação da Pesquisa

Esta pesquisa se concentra na análise do comportamento da cultura corporativa de Organizações de Saúde Públicas e Privadas brasileiras frente à necessidade de adequação dos processos de tratamento de dados de pessoas naturais, conforme previsto na LGPD.

Os processos analisados compreendem os fluxos e medidas adotados desde

o momento da coleta das informações, passando por seu gerenciamento, incluindo a transferência para terceiros, até o descarte.

Em razão do interesse da pesquisa estar adstrito aos dados considerados sensíveis, a análise se limitará ao tratamento das informações referentes à saúde e à vida sexual, bem como a dados genéticos e biométricos; a informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, quando vinculados às pessoas naturais com as quais as Organizações de Saúde se relacionam interna ou externamente, considerando-se clientes (pacientes) e empregados.

Além disso, a presente pesquisa estará delimitada às unidades de saúde médica para seres humanos vivos, descartando-se, por exemplo, as unidades de saúde bucal, os institutos médicos legais, os pontos de atendimento à saúde dos animais, as farmácias e drogarias, a medicina laboral e os institutos de investigação científica.

Por fim, há de se salientar que, embora se compreenda a relevância da temática que envolve crianças e adolescentes, as especificidades do tratamento de dados desse público não será objeto desta pesquisa.

1.4 Relevância do Estudo

Embora a proteção de dados não seja um tema novo, haja vista sua abordagem de forma esparsa mesmo antes da publicação de Regulamentos e Leis específicos, vê-se que somente no século XXI passou a receber o merecido tratamento prioritário.

Em razão disso, apresenta vácuo na sua aplicação, sobretudo quando se relaciona aos dados sensíveis tratados em meio a uma Cultura Organizacional tradicional, que poderá ser superado a partir do presente estudo, considerando-se que as normas contidas na LGPD são de interesse nacional e devem ser observadas por todos aqueles que manipulam dados de pessoas naturais, inclusive nos meios digitais, com o objetivo de proteger seus direitos fundamentais da liberdade, privacidade e livre desenvolvimento.

Por se tratar de uma temática ainda recente no meio acadêmico, a presente pesquisa favorece não apenas o preenchimento de lacunas, mas também a inserção desse relevante tema na pauta acadêmica.

Pesquisadores de proteção de dados; segurança da informação; direito digital e gestores de Organizações de Saúde poderão utilizar este modelo de desenvolvimento em benefício de muitas investigações acerca dos limites da privacidade e sigilo das informações.

Por outro lado, no que tange às questões práticas, a presente pesquisa possibilita que os gestores de unidades de saúde públicas e privadas brasileiras compreendam os desafios e as oportunidades trazidas pela LGPD no que se refere às práticas organizacionais de classificação, tratamento e proteção de dados.

Além disso, estar adequado à LGPD poderá minimizar as chances de a Organização de Saúde ser rejeitada pelo mercado, como ocorre, por exemplo, com instituições envolvidas em episódios de vazamento de dados[2], cujas ocorrências estão sendo observadas de perto pelos órgãos governamentais, pelos pretensos parceiros e por seus clientes.

1.5 Estrutura da Dissertação

O estudo em questão está dividido em 05 capítulos. O primeiro consiste na introdução, acompanhado do problema da pesquisa; dos objetivos principal e específicos; da delimitação da pesquisa e sua relevância.

O referencial teórico está subdividido em três partes: (i) a primeira, com questões legais que nos ajudam a compreender a temática da Proteção de Dados (perspectivas europeia e brasileira); (ii) a segunda, com questões culturais embasando os conceitos de Cultura Organizacional e tipologias para a compreender a sua dinâmica nas Organizações de Saúde; e (iii) a terceira, vinculando a aplicação prática da proteção de dados em diferentes Culturas Organizacionais, evidenciando casos reais de fragilidade de sistemas de proteção que culminaram em diversos vazamentos de dados médicos de usuários e profissionais de saúde.

O terceiro capítulo (“Metodologia da Pesquisa”) descreve o tipo de pesquisa, sua natureza e classificação, bem como as entrevistas com gestores de

[2] Vazamento de dados é definido como um incidente de segurança em que dados pessoais e/ou informações privadas e sigilosas são expostos publicamente ou a terceiros sem autorização. Dessa forma, as informações podem ser acessadas, visualizadas, copiadas, vendidas, compradas e usadas para fins diversos.

Organizações de Saúde públicas e privadas do Brasil, acompanhadas dos procedimentos para coleta das informações e seu tratamento, com o fim de atender ao objetivo desse estudo.

No quarto capítulo, são descritos os resultados da pesquisa a partir das entrevistas realizadas.

Por fim, o quinto capítulo apresenta sugestões e recomendações de alinhamento da Cultura Organizacional às práticas de classificação, tratamento e proteção de dados em Organizações de Saúde públicas e privadas brasileiras.

2 Referencial Teórico

2.1 Aspectos legais

Não obstante o tema central da presente pesquisa estar relacionado ao papel da Cultura Organizacional na adaptação das Organizações de Saúde públicas e privadas brasileiras à LGPD, para sua adequada compreensão é necessário estender a análise para os institutos anteriores e ocorrências históricas que serviram de referência para a estruturação dos estatutos mais modernos e específicos sobre a matéria.

Deste modo, o presente capítulo será iniciado com a contextualização do direito à privacidade e da evolução do tema no cenário mundial, alcançando o sigilo médico.

Em seguida, serão analisados os conceitos e princípios do GDPR e da LGPD e as principais correntes teóricas relativas à Cultura Organizacional que se amoldam ao desafio do processo de implementação de programas internos de proteção de dados no segmento de Saúde.

Com isso, serão explorados o aspecto performativo e a maneira como as pessoas vivenciam a Cultura Organizacional em momento anterior e posterior à entrada em vigor da LGPD, bem como os impactos – positivos e negativos – decorrentes do processo de adequação ao novo Regulamento.

2.1.1 O Direito à Privacidade

Ao traduzir Radcliffe-Brown (1881), Caixeiro (1973) descreve que, no curso de sua história, a sociedade tem enfrentado diversas mudanças, mas é capaz de manter seu atributo de continuidade o que lhe possibilita ampliar seu complexo de relacionamentos sociais, analisado com base no interesse mútuo de pessoas em outras ou em um ou mais interesses comuns.

Portanto, desde o surgimento das primeiras sociedades, oriundas das aglomerações familiares e tribais, o ser humano faz parte de grupos sociais dos quais internaliza determinados comportamentos que podem ser reproduzidos através das gerações.

O ser humano é naturalmente um animal político, destinado a viver em sociedade, tendo necessidade de se associar a outros humanos para sobrevivência, embora mantenha suas características egoístas. (Aristóteles - 384-322 a.C.).

É nesse sentido que, com o tempo, passou a buscar seu reconhecimento como um indivíduo autônomo, de modo que lhe fosse possibilitado preservar suas experiências, seus espaços e sua liberdade de pensar, de agir e de viver, com ampliação das restrições[3] à sua proteção para além do plano objetivo – físico e patrimonial, já que esse modelo anulava qualquer ocorrência que envolvesse sua essência.

Mas esse panorama somente começou a mudar quando a tutela jurídica foi ampliada para o campo da subjetividade, de modo que não bastava criar mecanismos de proteção ao indivíduo apenas para mantê-lo vivo e evitar que seu patrimônio fosse molestado, mas seria necessário garantir meios que o possibilitasse desfrutar da dádiva da vida, o que lhe permitiria, enfim, ser reconhecido como um indivíduo.

Depois disso, o movimento da subjetividade uniu-se à inovação tecnológica e ao avanço jornalístico que, ao mesmo tempo, possibilitavam a circulação de informações e o ingresso na intimidade e na vida privada de outros seres humanos, desafiando os equipamentos de gestão da informação, tidos por inadequados.

No mesmo sentido, a invenção da técnica de fotografia tornou ainda maior o desafio de proteção à privacidade dos indivíduos, já que registrar fatos e momentos cotidianos passou a fazer parte da cultura social e da Cultura Organizacional.

Porém, a proteção à privacidade ainda não era tratada com a merecida relevância e, diante da ausência de proporcionalidade no julgamento das diversas ocorrências de violação à vida privada, tornou-se essencial o surgimento de um

[3] Exemplo dessa restrição histórica pode ser aferido no cenário brasileiro quando da leitura da sua primeira Constituição, a do Império do ano de 1824, em seu artigo 179, inciso XXII: *"A inviolabilidade dos Direitos Civis, e Politicos dos Cidadãos Brazileiros, que tem por base a liberdade, a segurança individual, e a propriedade, é garantida pela Constituição do Imperio, pela maneira seguinte.*
XXII. E'garantido o Direito de Propriedade em toda a sua plenitude. Se o bem publico legalmente verificado exigir o uso, e emprego da Propriedade do Cidadão, será elle préviamente indemnisado do valor della. A Lei marcará os casos, em que terá logar esta unica excepção, e dará as regras para se determinar a indemnização".
Tendo assim permanecido nas Constituições da República de 1891; 1934; 1937; 1946; 1967 e 1969.

novo direito. Nascia, então, o direito da personalidade.

Josef Kohler e Otto von Gierke teriam sido os precursores da doutrina dos direitos da personalidade (Veliz, 2021) ao traçarem parâmetros para o fluxo de comunicação entre os níveis público e privado da sociedade.

Entretanto, a aplicação prática desse direito, embora ainda discreta, teria se dado no ano de 1880, a partir da expressão "the right to be let alone" do jurista americano Thomas McIntyre Coley, presidente da Suprema Corte de Michigan (Pereira, 2021 e Zanini, 2022).

Todavia, somente no ano de 1890, o debate sobre privacidade tornou-se efetivo, a partir da publicação do artigo "The Right to Privacy", de Warren e Brandeis, pela Harvard Law Review, considerado o primeiro a tratar sobre a temática e conceituado como uma avançada discussão para a época.

"The Right to Privacy" seguiu como principal referência teórica até a metade do século XX, por volta de 1950, evidenciando uma estagnação do desenvolvimento do conteúdo, que perdeu a oportunidade de acrescentar avanços tecnológicos na sua proteção (ZANINI, 2022).

Nesse período, mais precisamente em 10 de dezembro de 1948, a Assembleia Geral das Nações Unidas proclamou a Declaração Universal dos Direitos Humanos que passou a reconhecer, dentre outras direitos, a dignidade a todos os membros da família humana, bem como os fundamentos da liberdade e da justiça, conforme Tabela 1.

Tabela 1 – Declaração Universal dos Direitos Humanos – ONU (1948)

VALORES	Liberdade; Justiça e Paz
ARTIGO 2º	Toda pessoa tem capacidade para gozar os direitos e as liberdades estabelecidos nesta Declaração.
ARTIGO 3º	Toda pessoa tem direito à vida, à liberdade e à segurança pessoal.
ARTIGO 12	Ninguém poderá sofrer intromissões arbitrárias em sua vida privada, família, domicílio ou correspondência, nem ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.
ARTIGO 19	Todos têm direito à liberdade de opinião e expressão; esse direito inclui a liberdade de, sem interferência, ter opiniões e de buscar, receber e difundir informações e ideias por qualquer meio e independentemente de fronteiras.

Fonte: elaborada pela Autora (2022)

A DUDH – ONU foi seguida pela Lei Fundamental da República Federal da Alemanha (tabela 2), promulgada no dia 23 de maio de 1949, que preceituava direitos fundamentais e os requisitos para suas limitações, válidos para todo o

povo alemão, mas que se tornou um modelo para Países do mundo inteiro que trilharam o caminho do totalitarismo a um sistema democrático.

Tabela 2 – Lei Fundamental da República Federal da Alemanha (1949)

VALORES	Dignidade; Justiça e Paz
ARTIGO 1 (1)	A dignidade da pessoa humana é intangível. Respeitá-la e protegê-la é obrigação de todo o poder público.
ARTIGO 2 (1)	Todos têm o direito ao livre desenvolvimento da sua personalidade, desde que não violem os direitos de outros e não atentem contra a ordem constitucional ou a lei moral.

Fonte: elaborada pela Autora (2022)

A partir da DUDH – ONU, o Conselho da Europa, objetivando estreitar a união entre os seus Membros, por meio da proteção e do desenvolvimento dos direitos do homem e das liberdades fundamentais, promulgou a Convenção Europeia dos Direitos Humanos (tabela 3), reafirmando seu apreço pelas liberdades fundamentais.

Tabela 3 – Convenção Europeia dos Direitos Humanos (1950)

VALORES	Liberdade; Justiça e Paz
ARTIGO 8º (1)	Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência.
ARTIGO 8º (2)	Não pode haver ingerência da autoridade pública no exercício deste direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar económico do país, a defesa da ordem e a prevenção das infracções penais, a proteção da saúde ou da moral, ou a proteção dos direitos e das liberdades de terceiros.

Fonte: elaborada pela Autora (2022)

Poucos anos após, foi publicado o Tratado sobre o Funcionamento da União Europeia, que instituiu a Comunidade Econômica Europeia (Tratado de Roma – tabela 4), assinado em 25 de março de 1957, pelo qual buscava-se uma união cada vez mais estreita entre os povos europeus mediante uma ação comum, o progresso econômico e social dos seus países, eliminando as barreiras que dividiam a Europa.

Tabela 4 – Tratado de Roma (1957)

VALORES	Cooperação; Justiça e Paz

PREÂMBULO	Resolvidos a preservar e consolidar a paz e a liberdade através desta união das suas forças econômicas, e convidando os outros povos da Europa que professam o mesmo elevado objetivo a juntarem-se a estes esforços.
ARTIGO 214	Os membros dos órgãos da Comunidade, os membros dos comités e os funcionários e outros agentes da Comunidade são obrigados, mesmo após o termo das suas funções oficiais, a não divulgar informações que, pela sua natureza, estejam abrangidas pelo segredo profissional; isso se aplica em particular a informações sobre empresas e suas relações comerciais ou elementos de custo.

Fonte: elaborada pela Autora (2022)

Ocorre que, com o advento do Estado Social; a evolução da economia digital; o avanço da globalização; o progresso das tecnologias da informação; o desenvolvimento da biotecnologia e o acesso a dados sensíveis, tornou-se necessária a adoção de medidas mais enérgicas para combater a violação da privacidade, o que já era defendido no artigo "The Right to Privacy" décadas antes, conforme trecho abaixo destacado:

> *"Se a invasão de privacidade constitui um dano jurídico, existem os elementos para exigir reparação, uma vez que já é reconhecido o valor do sofrimento psíquico, causado por ato culposo em si mesmo, como fundamento da indenização.*
> *(...)*
> *a proteção da sociedade deve vir principalmente por meio do reconhecimento dos direitos do indivíduo. Cada homem é responsável apenas por seus próprios atos e omissões. Se ele tolera o que reprova, (...), ele é responsável pelos resultados. Se ele resistir, a opinião pública irá apoiá-lo".*

Embora as legislações já publicadas fossem consideradas um avanço, havia um prenúncio de que um desenvolvimento ainda mais impactante estava por vi e o marco dessa mudança vital veio a ocorrer em 07 de junho de 1965, quando a Suprema Corte Americana (EUA) julgou um dos primeiros episódios envolvendo direito à privacidade: o caso Griswold v. Connecticut.

O caso concreto se deu no contexto de uma clínica no Estado de Connecticut (EUA) que atendia apenas mulheres casadas e as orientava sobre os métodos contraceptivos. Porém, para uma delas, teria sido receitado um anticoncepcional.

Ocorre que, no ano de 1879, o Estado de Connecticut tinha aprovado uma lei que descrevia como crime a conduta de utilizar remédio com o propósito de não engravidar, incorrendo na mesma pena quem aconselhasse ou assistisse outra pessoa na medida contraceptiva.

Após longo debate judicial, os médicos Lee Buxton e Estelle Griswold foram inocentados e libertados pela Suprema Corte que declarou que o estatuto de Connecticut violava o direito à privacidade conjugal, uma das garantias específicas da Carta de Direitos.

Os Estados Americanos, embora ainda estivessem em velocidade mais lenta, seguiam os caminhos trilhados pela Europa, conforme se viu com a Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica), de 22 de novembro de 1969 (tabela 5), adotada no âmbito da OEA, que objetivava reafirmar seu propósito de consolidar no Continente, dentro do quadro das instituições democráticas, um regime de liberdade pessoal e de justiça social, fundado no respeito aos direitos essenciais do homem.

Tabela 5 – Convenção Americana sobre Direitos Humanos (Pacto De São Jose da Costa Rica) – (1969)

VALORES	Respeito, Dignidade e Paz
ARTIGO 11 (1)	Toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade.
ARTIGO 11 (2/3)	Ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou tais ofensas.

Fonte: elaborada pela Autora (2022)

Era evidente o movimento de fortalecimento da proteção da vida privada. No entanto, era preciso ampliar o debate já que o avanço da computação e da indústria nos países mais desenvolvidos poderia colocar em risco a privacidade no mundo. E, mais uma vez, a Europa ocupou papel de destaque ao aprovar o *Hessiches Datenschutzgesetz* (Ato de Proteção de Dados de Hesse - Alemanha), revisado e implementado em 1978, considerada a primeira lei de proteção de dados na Alemanha e no mundo.

A Lei de Hesse, em sua versão original, continha dezessete parágrafos distribuídos em três capítulos. Porém, passou por diversas atualizações e sua

última versão, publicada no ano de 2021, contém cinco partes e noventa e um parágrafos.

Ao Ato de Hesse seguiram diversos outros normativos, consoante Tabela 6:

Tabela 6 – Normativos que seguiram o Ato de Hesse

ANO	PAÍSES
1973	Suécia
1976	Portugal
1978	Espanha
1981	França, Noruega, Áustria e Suécia (convenção unificada)
1981	Conselho da Europa (convenção nº 108)
1995	União Europeia (diretiva 46/95)
2000	União Europeia (carta dos direitos fundamentais)

Fonte: elaborada pela Autora (2022)

Embora diversas nações europeias já tivessem sua própria lei de proteção de dados, essas legislações, assim como suas antecessoras, ainda eram genéricas e programáticas, o que era pouco eficiente para atender a questões práticas e específicas, dificultando sua aplicação e o seu entendimento (D'avila et.al., 2021).

A partir desse momento da história, o debate sobre a proteção de dados começou a ser difundido no mundo e alcançou mais expressivamente países de fora da Europa.

Múltiplos Países do Continente Americano também delinearam seus Regulamentos próprios, embora de modo disperso, conforme resumido na Tabela 7:

Tabela 7 – Regulamentos de Proteção de dados do Continente Americano

PAÍS	ATO ELABORADO
EUA	O EUA não possui Lei Geral de Proteção de Dados. Os Estados estabelecem seus próprios Regulamentos. Os mais recentes entraram em vigor no ano de 2020: - **California Consumer Privacy Act - (CCPA)** - cria novos direitos do consumidor, que passam a ter mais controle sobre as suas próprias informações. - **New York Stop Hacks and Improve Electronic Data Security Act (NY SHIELD)** - exige que determinadas empresas sejam mais transparentes e

	adorem medidas mais cautelosas ao lidarem com dados pessoais.
CHILE (19.628/1999)	O Chile foi o primeiro país da América Latina a aprovar uma Lei Geral de Proteção de Dados, no ano de 1999, dispondo sobre a proteção da vida privada e a proteção dos dados de caráter Pessoal.
ARGENTINA (25.326/2000)	Regula os princípios gerais relativos à proteção de dados; os direitos dos detentores de dados; os usuários e gestores de arquivos, registros e bancos de dados e estabelece controle e sanções para a proteção de dados pessoais.
MÉXICO (DOF 05/07/2010)	Destina-se a proteger os dados pessoais detidos pelas pessoas singulares, a fim de regular o seu tratamento legítimo, controlado e informado, com a finalidade de garantir a privacidade e o direito de autodeterminação informativa das pessoas.
PERU (29.733/2011)	O objetivo desta Lei é garantir o direito fundamental à proteção de dados pessoais, previsto na Constituição Política do Peru, por meio de seu tratamento adequado, dentro de um quadro de respeito a outros direitos fundamentais.
COLÔMBIA (1.581/2012)	O objetivo desta lei é desenvolver o direito constitucional que todas as pessoas têm de conhecer, atualizar e retificar as informações que foram coletadas sobre elas em bases de dados ou arquivos, e os demais direitos, liberdades e garantias constitucionais a que se refere a Constituição Política.
URUGUAI (18.331/2008)	Regulamenta o direito à proteção de dados previsto na Constituição da República, ressaltando se tratar de um direito inerente à pessoa humana.

Fonte: elaborada pela Autora (2022)

No Brasil, embora o Código Penal, de 07 de dezembro de 1940, já previsse a punição com pena de detenção ou de multa para quem revelasse segredo profissional que pudesse causar danos a outra pessoa[4], a proteção à privacidade somente começou a ganhar evidência a partir da promulgação da Constituição Cidadã, de 1988, tradução da efetividade de um Estado Democrático de Direito, que objetivava aniquilar os efeitos negativos que haviam restado não apenas da Segunda Guerra Mundial (1939-1945), mas também do Estado Novo (1937-1945) e da Ditadura Militar (1964-1985).

CRFB/88
Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

*X - são invioláveis a **intimidade**, a **vida privada**, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;*

[4] Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa de um conto a dez contos de réis.

Embora o termo privacidade não esteja referenciado de maneira expressa no dispositivo constitucional, é pacífico que se trata do gênero que contempla os elementos da inviolabilidade da vida privada, da honra e da imagem das pessoas ali previstos (Masson,2021).

Neste sentido, o ditame constitucional se tornou uma das principais referências para o legislador infraconstitucional, cujos normativos balizaram, por anos, as tomadas de decisão e delinearam as Culturas Organizacionais das empresas, conforme Tabela 8.

Tabela 8 – Principais leis infraconstitucionais sobre proteção à privacidade e à intimidade

LEI	CONTEÚDO
CÓDIGO DE DEFESA DO CONSUMIDOR	Artigo 4º A Política Nacional das Relações de Consumo tem por objetivo o atendimento das necessidades dos consumidores, o respeito à sua dignidade, saúde e segurança, a proteção de seus interesses econômicos, a melhoria da sua qualidade de vida, bem como a transparência e harmonia das relações de consumo, atendidos os seguintes princípios: I - reconhecimento da vulnerabilidade do consumidor no mercado de consumo; IV - educação e informação de fornecedores e consumidores, quanto aos seus direitos e deveres, com vistas à melhoria do mercado de consumo; Dos Bancos de Dados e Cadastros de Consumidores Artigo 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos. § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas. § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público. § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
LEI DA PROPRIEDADE INDUSTRIAL (LPI) 9.279/96	Artigo 195. Comete crime de concorrência desleal quem: XI - **divulga, explora ou utiliza-se, sem autorização**, de conhecimentos, **informações ou dados confidenciais**, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou

	empregatícia, mesmo após o término do contrato. Artigo 206. Na hipótese de serem **reveladas**, em juízo, para a defesa dos interesses de qualquer das partes, **informações que se caracterizem como confidenciais, sejam segredo** de indústria ou de comércio, deverá o juiz determinar que o processo prossiga em segredo de justiça, vedado o uso de tais informações também à outra parte para outras finalidades.
LEI DE DIREITO AUTORAL (LDA) 9.610/98	Artigo 17. É assegurada a proteção às participações individuais em obras coletivas. § 1º Qualquer dos participantes, **no exercício de seus direitos morais, poderá proibir que se indique ou anuncie seu nome** na obra coletiva, sem prejuízo do direito de haver a remuneração contratada. Artigo 59. Quaisquer que sejam as condições do contrato, o editor é obrigado a **facultar ao autor o exame da escrituração na parte que lhe corresponde, bem como a informá-lo sobre o estado da edição**.
LEI DA INTERCEPTAÇÃO TELEFÔNICA 9.296/96	A CRFB prevê, em seu artigo 5º, inciso XII, que **"É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas**, salvo, no último caso, por ordem judicial nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal." O legislador infraconstitucional regulamentou a expressão "nas hipóteses e na forma que a lei estabelecer" por meio da Lei nº 9.296/96. Artigo 1º. A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, **inclusive com a indicação e qualificação dos investigados**, **salvo impossibilidade manifesta** devidamente justificada. Artigo 8°. A interceptação de comunicação telefônica, de qualquer natureza, ocorrerá em autos apartados, apensados aos autos do inquérito policial ou do processo criminal, **preservando-se o sigilo** das diligências, gravações e transcrições respectivas.
LEI GERAL DAS TELECOMUNI-CAÇÕES 9.472/97	Artigo 3°. O **usuário** de serviços de telecomunicações tem direito: IX - ao **respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço**; Artigo 21. As sessões do Conselho Diretor serão registradas em atas, que ficarão arquivadas na Biblioteca, disponíveis para conhecimento geral. § 1º **Quando a publicidade** puder colocar em risco a segurança do País ou **violar** segredo protegido ou a **intimidade de alguém**, os registros correspondentes serão mantidos em sigilo.
LEI DO HABEAS DATA 9.507/97	Artigo 4°. Constatada a **inexatidão de qualquer dado a seu respeito, o interessado**, em petição acompanhada de documentos comprobatórios, **poderá requerer sua retificação**. § 1°. Feita a retificação em, no máximo, dez dias após a entrada do requerimento, a entidade ou órgão depositário do registro ou da informação dará ciência ao interessado. Artigo 7°. Conceder-se-á **habeas data**: I - **para assegurar o conhecimento de informações relativas à pessoa do impetrante**, constantes de registro ou banco de dados de entidades governamentais ou de caráter público; II - **para a retificação de dados**, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;

	III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre **dado verdadeiro** mas justificável e que esteja sob pendência judicial ou amigável.
CÓDIGO CIVIL (CC) 10.406/02	Artigo 1º. Toda pessoa é capaz de direitos e deveres na ordem civil. Artigo 12. Pode-se exigir que **cesse a ameaça, ou a lesão, a direito da personalidade**, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei. Artigo 16. Toda pessoa tem direito ao nome, nele compreendidos o prenome e o sobrenome. Artigo 17. **O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público**, ainda quando não haja intenção difamatória. Artigo 18. **Sem autorização, não se pode usar o nome alheio em propaganda comercial**. Artigo 19. O **pseudônimo** adotado para atividades lícitas **goza da proteção** que se dá ao nome. Artigo 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou **a utilização da imagem de uma pessoa poderão ser proibidas**, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais. Parágrafo único. Em se tratando de **morto ou de ausente**, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes. Artigo 21. **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.
NOTIFICAÇÃO COMPULSÓRIA EM CASOS DE VIOLÊNCIA CONTRA MULHER 10778/03	Artigo 1º. Constituem objeto de **notificação compulsória**, em todo o território nacional, os casos em que houver **indícios ou confirmação de violência contra a mulher** atendida **em serviços de saúde públicos e privados**. Artigo 3º. A notificação compulsória dos casos de violência de que trata esta Lei tem **caráter sigiloso**, obrigando nesse sentido as autoridades sanitárias que a tenham recebido. Parágrafo único. **A identificação da vítima de violência** referida nesta Lei, **fora do âmbito dos serviços de saúde**, somente poderá efetivar-se, em **caráter excepcional**, em caso de risco à comunidade ou à vítima, a juízo da autoridade sanitária e com conhecimento prévio da vítima ou do seu responsável.
CÓDIGO DE PROCESSO PENAL **DECRETO LEI 3.689, 3/10/1941**	Embora o CPP tenha sido editado no ano de 1941, quando ainda não havia preeminência do debate sobre privacidade no Brasil, ao longo dos anos passou por diversas atualizações, a fim de acompanhar os avanços teóricos e sociais no sistema criminal brasileiro. Com isso, no ano de 2008, vinte anos após a promulgação da CRFB, a Lei nº 11.690/08 incluiu a seguinte redação: Artigo 201. Sempre que possível, **o ofendido será qualificado** e perguntado sobre as circunstâncias da infração, quem seja ou presuma ser o seu autor, as provas que possa indicar, tomando-se por termo as suas declarações. § 6º **O juiz tomará as providências necessárias à preservação da intimidade, vida privada, honra e imagem do ofendido**, podendo, inclusive, determinar o segredo de justiça em relação aos dados, depoimentos e outras informações constantes dos autos a seu respeito para evitar sua exposição aos meios de comunicação.
	Artigo 3º. Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito,

LEI DO CADASTRO POSITIVO 12.414/11	nas condições estabelecidas nesta Lei. § 1º. **Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão**, que sejam necessárias para avaliar a situação econômica do cadastrado. § 3º **Ficam proibidas** as anotações de: I - **informações excessivas**, assim consideradas aquelas que não estiverem vinculadas à análise de risco de crédito ao consumidor; e II - **informações sensíveis, assim consideradas aquelas pertinentes à origem social e étnica, à saúde, à informação genética, à orientação sexual e às convicções políticas, religiosas e filosóficas**. Art. 5º São **direitos** do cadastrado: II - **acessar gratuitamente**, independentemente de justificativa, **as informações sobre ele existentes no banco de dados**, inclusive seu histórico e sua nota ou pontuação de crédito, cabendo ao gestor manter sistemas seguros, por telefone ou por meio eletrônico, de consulta às informações pelo cadastrado.
LEI DE ACESSO À INFORMAÇÃO (LAI) 12.527/11	Artigo 31. **O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais.** § 1º As informações pessoais, a que se refere este artigo, relativas à intimidade, vida privada, honra e imagem: I - terão seu acesso restrito, independentemente de classificação de sigilo e pelo prazo máximo de 100 (cem) anos a contar da sua data de produção, a agentes públicos legalmente autorizados e à pessoa a que elas se referirem; e II - poderão ter autorizada sua divulgação ou **acesso por terceiros diante de previsão legal ou consentimento expresso da pessoa** a que elas se referirem. § 2º Aquele que obtiver acesso às informações de que trata este artigo será responsabilizado por seu uso indevido. § 3º **O consentimento** referido no inciso II do § 1º **não será exigido quando as informações forem necessárias:** **I - à prevenção e diagnóstico médico, quando a pessoa estiver física ou legalmente incapaz, e para utilização única e exclusivamente para o tratamento médico.** II - à realização de estatísticas e pesquisas científicas de evidente interesse público ou geral, previstos em lei, sendo vedada a identificação da pessoa a que as informações se referirem. III - ao cumprimento de ordem judicial. IV - à defesa de direitos humanos; ou V - à proteção do interesse público e geral preponderante. § 4º **A restrição de acesso à informação relativa à vida privada, honra e imagem de pessoa não poderá ser invocada com o intuito de prejudicar processo de apuração de irregularidades** em que o titular das informações estiver envolvido, bem como em ações voltadas para a recuperação de fatos históricos de maior relevância. § 5º Regulamento disporá sobre os procedimentos para tratamento de informação pessoal. Em seus 47 artigos, a LAI estabeleceu princípios e regras para a promover a transparência, de modo que observância da publicidade deve ser a regra geral e o sigilo, a exceção. A LAI enfatiza, ainda, a relevância da utilização de novas tecnologias e da simplificação de procedimentos, com a vedação de exigências burocráticas que possam inviabilizar o acesso a informações públicas. Nada obstante, a LAI preconiza o desenvolvimento da transparência e

	do tratamento de informações na Administração Pública, permanecendo, assim, o hiato quando se trata de dados pessoais.
MARCO CIVIL DA INTERNET (MCI) 12.965/14	Artigo 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - **inviolabilidade da intimidade e da vida privada**, sua proteção e indenização pelo dano material ou moral decorrente de sua violação. VII - **não fornecimento a terceiros de seus dados pessoais**, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei. VIII - **informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais**, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - **consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais**, que deverá ocorrer de forma destacada das demais cláusulas contratuais.
USO DO NOME SOCIAL 8.727/2016	O Decreto nº 8.727/2016 dispõe sobre o uso do nome social[5] e o reconhecimento da identidade de gênero[6] de pessoas travestis e transexuais no âmbito da administração pública federal direta, autárquica e fundacional. O Decreto prevê, ainda, que os órgãos e as entidades da administração pública federal direta, autárquica e fundacional, em seus atos e procedimentos, deverão adotar o nome social da pessoa travesti ou transexual, de acordo com seu requerimento e com o disposto no Regulamento legal, vedando o uso de expressões pejorativas e discriminatórias para referir-se a pessoas travestis ou transexuais[7]. O normativo estabelece, também, que a pessoa travesti ou transexual poderá requerer, a qualquer tempo, a inclusão de seu nome social em documentos oficiais e nos registros dos sistemas de informação, de cadastros, de programas, de serviços, de fichas, de formulários, de prontuários e congêneres dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional, que deverão conter o campo "nome social" em destaque, acompanhado do nome civil, e serão utilizados apenas para fins administrativos internos ou quando estritamente necessário ao atendimento do interesse público e à salvaguarda de direitos de terceiros[8].

Fonte: elaborada pela Autora (2022)

2.1.2. A privacidade na relação entre médico e paciente

A ausência de Leis específicas sobre tratamento de dados pessoais assolava muitos negócios brasileiros que conviviam com os riscos interpretativos das

[5] Designação pela qual a pessoa travesti ou transexual se identifica e é socialmente reconhecida.
[6] Dimensão da identidade de uma pessoa que diz respeito à forma como se relaciona com as representações de masculinidade e feminilidade e como isso se traduz em sua prática social, sem guardar relação necessária com o sexo atribuído no nascimento.
[7] Artigo 2º e seu parágrafo único, Decreto nº 8.727/2016
[8] Artigos 3º, 5º e 6º, Decreto nº 8.727/2016

diversas normas esparsas. Entretanto, um segmento de mercado parecia não ser afetado por essa lacuna: o serviço médico.

Isso porque, o segredo médico, embora não fosse tratado expressamente na legislação brasileira, era objeto de preocupação nas diversas normas éticas do CFM, complementadas pela CRFB, pelo Código Civil e pelo Código Penal.

Há, ainda, dezenas de normativos internos regulamentados pelo Ministério da Saúde e pela ANS (Tabela 9) que estabelecem procedimentos para registro e compartilhamento de informações de saúde de pacientes por Municípios, pelos Estados e pelo Distrito Federal, conforme preceitua o artigo 294 da Portaria de Consolidação nº 01 de 2017, do Ministério da Saúde, que acrescenta a obrigatoriedade de alimentação mensal e sistemática dos Bancos de Dados Nacionais.

Tabela 9 – Principais normativos regulamentados pelo Ministério da Saúde e pela ANS com procedimentos para registro e compartilhamento de informações de saúde de pacientes

NORMATIVO	CONTEÚDOS
CÓDIGO DE ÉTICA MÉDICA (RESOLUÇÃO CFM nº 1.931/09)	Princípios fundamentais: XI - **O médico guardará sigilo a respeito das informações** de que detenha conhecimento no desempenho de suas funções, com exceção dos casos previstos em lei. Sigilo Profissional: É **vedado** ao médico: Artigo 73. **Revelar fato de que tenha conhecimento em virtude do exercício de sua profissão**, salvo por motivo justo, dever legal ou consentimento, por escrito, do paciente. Artigo 74. Revelar sigilo profissional relacionado a paciente menor de idade, inclusive a seus pais ou representantes legais, desde que o menor tenha capacidade de discernimento, salvo quando a não revelação possa acarretar dano ao paciente. Artigo 78. Deixar de orientar seus auxiliares e alunos a respeitar o sigilo profissional e zelar para que seja por eles mantido. Documentos Médicos: É **vedado** ao médico: Artigo 85. **Permitir o manuseio e o conhecimento dos prontuários**[9] por pessoas não obrigadas ao sigilo profissional quando sob sua responsabilidade. Artigo 89. **Liberar cópias do prontuário sob sua guarda**, salvo quando autorizado, por escrito, pelo paciente, para atender ordem judicial ou para a sua própria defesa. Ensino e Pesquisa Médica: É **vedado** ao médico: Artigo 110. **Praticar a Medicina**, no exercício da docência, **sem o consentimento do paciente** ou de seu representante legal, **sem zelar por sua dignidade e privacidade** ou discriminando aqueles que negarem o consentimento solicitado.

[9] Conjunto de informações, sinais e imagens registradas, geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente e a assistência a ele prestada, de caráter legal, sigiloso e científico, que possibilita a comunicação entre membro da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo (Resolução 1.6038/02 – CFM)

RESOLUÇÃO CFM Nº 1.605, DE 15 DE SETEMBRO DE 2000	Artigo 1º. **O médico não pode**, sem o consentimento do paciente, **revelar o conteúdo do prontuário ou ficha médica**. Artigo 5º. Se houver **autorização expressa do paciente**, tanto na solicitação como em documento diverso, o médico poderá encaminhar a ficha ou prontuário médico diretamente à autoridade requisitante. Artigo 6º. **O médico deverá fornecer cópia da ficha ou do prontuário médico desde que solicitado pelo paciente** ou requisitado pelos Conselhos Federal ou Regional de Medicina.
RESOLUÇÃO CFM Nº 1.638, DE 11 DE JULHO DE 2002	Artigo 1º. Definir **prontuário médico** como o documento único constituído de um conjunto de informações, sinais e imagens registradas, **geradas a partir de fatos, acontecimentos e situações sobre a saúde do paciente** e a assistência a ele prestada, **de caráter legal, sigiloso e científico**, que possibilita a comunicação entre membros da equipe multiprofissional e a continuidade da assistência prestada ao indivíduo.
RESOLUÇÃO CFM Nº 1.821, DE 11 DE JULHO/2007	Considerando que **o sigilo profissional**, que visa preservar **a privacidade do indivíduo**, deve estar sujeito às normas estabelecidas na legislação e no Código de Ética Médica, independente **do meio utilizado para o armazenamento dos dados no prontuário, quer eletrônico quer em papel**.
PROCESSO-CONSULTA CFM Nº 1.401/2002 PC/CFM/Nº 30/2002	Princípios que devem subsidiar a normatização dos sistemas para prontuários eletrônicos: 1. O prontuário médico pode ser arquivado eletronicamente, em meio óptico ou magnético, desde que obedeça aos requisitos estabelecidos em resolução específica do Conselho Federal de Medicina e a legislação em vigor. De acordo com as mesmas diretrizes, prontuários novos já poderão ser elaborados eletronicamente. 2. Para garantir a autenticidade e a confidencialidade na transmissão dos dados, os sistemas de prontuário informatizado deverão incorporar parâmetros técnicos baseados na criptografia assimétrica de chaves (privada e pública), de acordo com as normas da ICP-Brasil. 3. A integridade das informações armazenadas deve estar garantida pelo sistema de informações. Uma vez inserido o dado no sistema, nunca mais poderá ser alterado. Caso haja necessidade de fazê-lo, o sistema deverá garantir as retificações ou acréscimos, sem modificar o registro original. Deverão desenvolver, também, um controle de acesso restrito a cada usuário, e possuir atributos para identificar qualquer usuário que acesse o banco dedados (autenticação). 4. Os sistemas de informação deverão estar aptos a periodicamente realizar cópias de segurança dos registros, e garantir a recuperabilidade imediata de qualquer informação ou documento pertencente ao prontuário. 5. Os sistemas para o desenvolvimento de prontuários eletrônicos poderão ser certificados pelo Conselho Federal de Medicina, de modo que obtenham um tipo de selo de qualidade que ateste sua subordinação às normas contidas na resolução específica. 6. O CFM deverá estudar a possibilidade de obter o credenciamento como Autoridade Certificadora, vinculada à AC-Raiz da ICP-Brasil, com o objetivo de oferecer a todos os médicos brasileiros uma assinatura eletrônica, que poderia ser entregue junto com o seu registro no Conselho Regional.
RESOLUÇÃO Nº 6/2016 – MINISTÉRIO DA SAÚDE	Instituiu o CMD da Atenção à Saúde conceituado como sendo o documento público que coleta os dados de todas as Organizações de Saúde do país em cada contato assistencial, compondo o Registro Eletrônico de Saúde e integrando o Sistema Nacional de Informação de Saúde. Nos termos desta Resolução, em seu artigo 4º, o CMD da Atenção à Saúde compreende dados essenciais com os seguintes fins: •subsidiar as atividades de gestão, planejamento, programação, monitoramento, avaliação e controle do sistema de saúde, da rede de atenção

	à saúde e das Organizações de Saúde; •subsidiar a formulação, o monitoramento e a avaliação das políticas de saúde; •compor as estatísticas nacionais de saúde, permitindo conhecer o perfil demográfico, de morbidade e mortalidade da população brasileira atendida nas Organizações de Saúde; •conhecer as atividades assistenciais desenvolvidas por todas as Organizações de Saúde no país; •fomentar a utilização de novas métricas para a análise de desempenho, alocação de recursos e financiamento da saúde; •possibilitar a realização dos processos administrativos necessários às três esferas de gestão do SUS, inclusive o faturamento dos serviços prestados; •disponibilizar informações assistenciais em nível nacional comparáveis com as informações internacionais em saúde. O documento regulamentador esclarece, ainda, que compõem o CMD da Atenção à Saúde, os dados das seguintes naturezas: •administrativos: são aqueles relacionados com a gestão de recursos das Organizações de Saúde que prestam assistência, tais como humanos, materiais ou financeiros; •clínico-administrativos: são aqueles relacionados com a gestão dos pacientes, enquanto usuários das Organizações de Saúde; e •clínicos: são aqueles relacionados ao estado de saúde ou doença dos indivíduos, expressos em diagnósticos, procedimentos e tratamentos realizados.

Fonte: elaborada pela Autora (2022)

Muito embora a temática da proteção à privacidade e do sigilo médico já se encontrasse abarcada nas Resoluções do CFM e estivesse inserida na Cultura Organizacional das Organizações de Saúde, entendia-se por fundamental que a proteção às garantias constitucionais ao sigilo, à privacidade, à autonomia e à dignidade fossem reforçadas por uma Lei formal, hierarquicamente superior às Resoluções e com imposição de penalidades mais rígidas.

Destarte, o presente capítulo buscou contextualizar o surgimento do direito à privacidade cintilando o quanto foram indispensáveis os saltos das gerações passadas pelos abismos absolutistas e o quanto tem sido relevante os debates construtivos sobre o tema, podendo ser resumido com a seguinte citação *"Um mundo sem privacidade é perigoso. A privacidade diz respeito à capacidade de manter certas coisas íntimas para si mesmo (...) a privacidade nos protege de pressões indesejadas e abusos de poder* (Veliz, 2021, p. 24).

2.1.3. A privacidade na relação de trabalho

Embora a Consolidação das Leis Trabalhistas (CLT) brasileira tenha sido editada na década de 40, mais precisamente no ano de 1943, diversas foram as

alterações em seu texto para adequá-la às novas realidades sociais e corporativas.

Nesta linha, duas mudanças relevantes puderam ser identificadas.

A primeira se deu pela Lei nº 9.799/1999, com a inclusão do artigo 373-A, inciso IV, pelo qual é vedado às empresas exigir de mulheres atestado ou exame, de qualquer natureza, para comprovação de esterilidade ou gravidez, na admissão ou permanência no emprego.

E a mais recente ocorreu com a reforma trabalhista, no ano de 2017, que assentou alterações significativas na redação original como a inclusão do artigo 223-C que estabelece que "a honra, a imagem, a intimidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física são os bens juridicamente tutelados inerentes à pessoa física".

Não obstante a previsão legal, cuja base principiológica é a CRFB, ainda havia (e há) muitos questionamentos sobre a forma mais adequada para que as pessoas disponibilizem seus dados pessoais no ambiente corporativo, inclusive sobre como as empresas cuidam deles.

Questiona-se, ainda, como delinear uma nova história, com respeito à vida privada dos empregados, em Culturas Organizacionais consolidadas por décadas com um modelo de comando e controle, fundamentado unicamente no consentimento, e como tratar os casos de invasão de privacidade no trabalho.

A CRFB e a CLT não trazem respostas concretas para esses questionamentos, possibilitando interpretações diversas, o que culmina em relações corporativas inseguras e acalora o debate relativo à matéria.

2.1.4 Entendendo o GDPR

O século XXI foi marcado por ocorrências relacionadas à privacidade, seja em relação aos normativos desenvolvidos em seu berço, seja em relação aos episódios que se tornaram públicos como no caso da tensão de ameaça à defesa da privacidade instalada pelo WikiLeaks[10] e pelas denúncias de Edward Snowden[11], conforme descreve Ilara Hämmerli Sozzi de Moraes, na obra Temas

[10] WikiLeaks é uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em sua página, lançada em dezembro de 2006, postagens de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis. (fonte: Wikipédia)

[11] Edward Joseph Snowden é um analista de sistemas, ex-administrador de sistemas da CIA do

e Saúde Coletiva, que cita, ainda, o trecho no qual Snowden dizia ser possível "grampear" qualquer pessoa, inclusive o Presidente, se tivesse apenas seu e-mail pessoal.

A recorrência de fatos semelhantes atraiu a atenção do mundo, exigindo a adoção de medidas mais enérgicas para regulamentar e punir o uso indevido de informações vinculadas à privacidade e tornou forçoso o debate mais intenso acerca da proteção de dados. Não havia mais tempo a perder. A sociedade mundial estava sedenta por olhares direcionados e respeitosos aos direitos fundamentais que lhes foram garantidos após tantos anos de escuridão e derramamento de sangue.

Em razão disso, a partir de um movimento mundial, a União Europeia, cujos Países já possuíam diversas normas isoladas sobre proteção de dados, entabulou um novo momento histórico ao decidir reestruturar suas políticas legislativas, de forma a possibilitar a circulação mais segura de dados pessoais no seu complexo de países e entres esses e outros países e organizações internacionais.

Desta forma, em 27 de abril de 2016, o Parlamento Europeu e o Conselho da União Europeia aprovaram o GDPR, registrado sob o nº 2016/679, que revogou os institutos correspondentes vigentes à época.

O GDPR passou por um período de vacância e teve sua exigibilidade iniciada em 25 de maio de 2018, com aplicação uniforme nos 27 países membros da União Europeia e, ainda, nos 03 países do Espaço Econômico Europeu: Noruega; Islândia e Liechtenstein.

Não obstante o GDPR estabelecer processos de proteção das pessoas singulares, no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados no âmbito da União Europeia, a Lei Geral não possui sua aplicação limitada aos cidadãos daquele espaço econômico, visto que pode ser aplicada mesmo quando os titulares dos dados estão em trânsito no território da União e ainda quando empresas sediadas na União Europeia armazenem os dados em outro Território, conforme salienta Maldonado et. al.(2020).

Os citados autores reforçam, ainda, que o ponto central do GDPR seria a

Governo dos EUA e ex-contratado da NSA que, no ano de 2013, tornou públicos detalhes de vários programas que constituem o sistema de vigilância global da NSA americana, incluindo tráfego de informações e espionagem.

proteção de direitos e garantias fundamentais dos cidadãos, de modo a reduzir eventuais riscos que pudessem decorrer da coleta e do futuro tratamento desses dados.

Cunha et.al. (2020) acrescentam que com o GDPR surgiram diversos novos direitos, como o direito à comunicação de violação de dados pessoais ao titular; direito de portabilidade de dados de um prestador de serviços para outro e direito a um prazo de resposta.

Relacionando-se a esses direitos, Cunha et.al. (2020) citam novos deveres consagrados no GDPR, como autorregulação; transparência e obrigação de reportar uma violação de dados.

Não obstante o volume de dados protegidos pelo GDPR, considerando-se as especificidades das informações coletadas, esta Lei Geral não será aplicada às atividades de segurança pública e de defesa nacional, bem como não se utilizará quando da aplicabilidade de dados pessoais por uma pessoa natural no exercício exclusivo de atividades pessoais ou domésticas ou, ainda, por autoridades competentes para efeitos de prevenção, investigação, detecção e repressão de infrações penais ou da execução de sanções penais.

2.1.5 A Influência do GDPR no Brasil

Compreender que a criação de uma Lei Geral contribui para determinar a estabilidade e a segurança de um país em suas relações de comércio internacional e com investidores foi relevante para o avanço no tema de proteção de dados no Brasil, seguindo o caminho já trilhado pela União Europeia.

As similaridades entre o GDPR e a LGPD alcançam ainda a proposta de conferir classificação ao arcabouço legal a partir da unificação de diferentes estatutos jurídicos que tratavam sobre o tema. Só no Brasil, havia cerca de 40 documentos que, de alguma forma, governavam os dados pessoais, conforme registra Koch (2019) ao analisar a LGPD como a versão brasileira do GDPR.

Assim, uma organização que estivesse em conformidade com o GDPR já estava à frente das demais, em termos mercadológicos e regulatórios.

Embora haja diversos outros pontos semelhantes entre os Institutos Legais, como o significado de dados pessoais e a definição dos direitos dos titulares, é

possível verificar a existência de diferenças, como a obrigatoriedade determinada pelo GDPR de contratação de encarregado em situações que envolvam entidade pública; tratamento em grande escala ou quando a natureza do tratamento exigir, enquanto a LGPD mantém o tópico como opcional, possibilitando que a autoridade nacional estabeleça as hipóteses de dispensa da necessidade de sua indicação.

Outra diferença significativa recai sobre o que se qualifica como base legal para processar dados pessoais, visto que o artigo 6º do GDPR prevê seis bases legais para o processamento e o artigo 7º da LGPD lista dez bases.

Todavia, embora haja diferenças nos textos das duas Leis Gerais, a estrutura, os princípios, os direitos, os deveres e as garantias previstos evidenciam que a LGPD foi construída a partir da literalidade do GDPR, o que lhe confere validação relativa do mercado.

2.1.6 Entendendo a LGPD

Como já abordado acima e salientado por Kohls et.al. (2021), a proteção à privacidade não é tema novo na legislação brasileira, visto que, mesmo de maneira esparsa e genérica, outros normativos já haviam previsto proteção ao instituto.

Não obstante os normativos isolados já existentes, casos reais demonstravam ser necessário aprofundar a proteção legislativa, consolidando-os, de modo a estabelecer estatuto específico que regulamentasse os requisitos, direitos, deveres e garantias dos titulares de dados pessoais operados nos ambientes *online* ou *offline*.

Nessa linha, então, seguindo a tendência mundial, após oito anos de debate no Congresso Nacional, em 14 de agosto de 2018, foi sancionada a Lei nº 13.709/2018, conhecida como LGPD, que se fundamenta nos pilares do respeito à privacidade; da autodeterminação informativa[12]; da liberdade de expressão, de informação, de comunicação e de opinião; da inviolabilidade da intimidade, da

[12] "**Autodeterminação informativa** consiste na capacidade do indivíduo em saber, com exatidão, quais de seus dados pessoais estão sendo coletados, com a consciência da finalidade para que se prestarão para, assim, diante de tais informações, tomar a decisão de fornecê-los ou não, levando-se em conta os benefícios e malefícios que o tratamento de seus dados poderá lhe acarretar". Kohls et.al. (2021, p. 22)

honra e da imagem; do desenvolvimento econômico e tecnológico e a inovação; da livre iniciativa, a livre concorrência e a defesa do consumidor; e dos direitos humanos, do livre desenvolvimento da personalidade, da dignidade e do exercício da cidadania pelas pessoas naturais.

O ano de 2022 marcou mais um avanço no debate, tendo em vista que o tema foi chancelado pela Lei Maior, com a promulgação da Emenda Constitucional nº 115/2022, que acrescentou o direito à proteção de dados pessoais no rol de direitos e garantias fundamentais ao cidadão, conferindo maior segurança aos titulares de dados e, por consequência, a possibilidade de mais investimentos internacionais no País.

Não obstante o enriquecimento da discussão, a LGPD ainda possui diversos desafios, e um deles, senão o mais relevante, é a mudança de Cultura Organizacional, posto que o texto legal cria novos direitos para o titular dos dados que afetarão diretamente os procedimentos operacionais das organizações.

2.1.7. Abrangência da LGPD

Nos termos do seu Artigo 3º, a LGPD se aplica a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do setor da economia, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no Brasil; a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no Brasil; ou os dados pessoais objeto do tratamento tenham sido coletados nesse País.

Para fins da citada Lei, serão considerados coletados no Brasil os dados pessoais cujo titular se encontre no País no momento da coleta, exceto se provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto na LGPD.

A aplicação da LGPD será excetuada, consoante prevê seu Artigo 4º, nas hipóteses de o tratamento de dados pessoais ser realizado por pessoa natural para

fins exclusivamente particulares e não econômicos ou, ainda, quando realizado para fins exclusivamente jornalístico, artísticos, acadêmicos, de segurança pública; de defesa nacional; de segurança do Estado ou de atividades de investigação e repressão de infrações penais

2.1.8. Conceitos definidos pela LGPD

O Artigo 5º da LGPD conceitua diversos elementos essenciais para a compreensão dos ditames legais e necessários para o desenvolvimento da presente pesquisa, como descrito na Tabela 10.

Tabela 10 – Conceitos definidos pela LGPD

ITEM	DEFINIÇÃO
DADO PESSOAL	Informação relacionada a pessoa natural identificada ou identificável.
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.
DADO ANONIMIZADO	Dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
BANCO DE DADOS	Conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
TITULAR	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
CONTROLADOR	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
OPERADOR	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
ENCARREGADO	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
AGENTES DE TRATAMENTO	O controlador e o operador.
TRATAMENTO	Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.
ANONIMIZAÇÃO	Utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.
CONSENTIMENTO	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

BLOQUEIO	Suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados.
ELIMINAÇÃO	Exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado.
TRANSFERÊNCIA INTERNACIONAL DE DADOS	Transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o Brasil seja membro.
USO COMPARTILHADO DE DADOS	Comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.
RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS	Documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.
ÓRGÃO DE PESQUISA	Órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico.
AUTORIDADE NACIONAL	Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

Fonte: elaborada pela Autora (2022)

2.1.9. Tratamento de Dados e LGPD

Conforme já abordado, a tecnologia é apontada como a principal causa de mudança social nas últimas décadas, visto que contribuiu para o aumento do fluxo de informações e promoveu conflitos e anseios na sociedade que nem sempre estavam previstos nas Leis.

A esses conflitos e anseios soma-se o ampliadíssimo sentido da expressão "tratamento de dados", representado por uma lista não taxativa de ações, fazendo com que, nas palavras de Teixeira e Armelin (2020), seja indispensável a aplicação de princípios que norteiem a aplicação da Lei, pois eles serão capazes de alcançar ocorrências futuras, ainda que diante de novas tecnologias e em uma realidade social diversa.

Por esse ângulo, a LGPD mostra-se mais conectada às peculiaridades do tema, visto que preceitua em seu Artigo 6º que as atividades de tratamento de dados pessoais deverão observar a boa-fé e os princípios descritos na Tabela 11:

Tabela 11 – Princípios da LGPD

PRINCÍPIO	DEFINIÇÃO
FINALIDADE	Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.
ADEQUAÇÃO	Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.
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.
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.
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.
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.
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.
PREVENÇÃO	Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.
NÃO DISCRIMINAÇÃO	Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.
RESPONSABILI-ZAÇÃO 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.

Fonte: elaborada pela Autora (2022)

Embora alguns desses princípios já estivessem previstos em Leis preexistentes, a LGPD os aborda de forma mais específica ao tratamento de dados e amplia o campo de tutela, conforme esclarece Bioni (2018) ao descrever que a LGPD se aplica, sem diferenciações, a operações de tratamento que ocorram por qualquer meio, eletrônico ou não, a despeito da finalidade, do mercado de atuação ou do regime jurídico aplicável (público ou privado).

2.1.10 Bases Legais da LGPD

Na passagem das diversas Leis analisadas para o desenvolvimento do presente trabalho, verificou-se a ausência de fundamentos legais (ou a sua inadequação) que dessem amparo ao tratamento de dados pessoais realizado pelo controlador.

Sequencialmente, com o objetivo de preencher esse vazio normativo, o Artigo 7º da LGPD designa as dez bases legais, ou seja, as hipóteses nas quais poderá se dar o tratamento de dados pessoais, sendo elas as descritas na Tabela 12:

Tabela 12 – Bases Legais da LGPD

BASE LEGAL	FUNDAMENTO
CONSENTIMENTO	Mediante o fornecimento de consentimento pelo titular.
OBRIGAÇÃO LEGAL	Para o cumprimento de obrigação legal ou regulatória pelo controlador.
POLÍTICAS PÚBLICAS	Pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas.
PROCESSOS	Para o exercício regular de direitos em processo judicial, administrativo ou arbitral.
CONTRATOS	Para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular e a seu pedido.
PESQUISA	Para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização.
PROTEÇÃO	Para a proteção da vida ou da incolumidade física do titular ou de terceiro.
TUTELA DA SAÚDE	Para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária.
INTERESSES LEGÍTIMOS	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.
PROTEÇÃO DE CRÉDITO	Para a proteção do crédito.

Fonte: elaborada pela Autora (2022)

Não obstante o rol prever dez elementos distintos, cumpre destacar dois, que mais são objeto de questionamentos e recebem relevo especial da Lei Geral: Consentimento e Interesse Legítimo.

A LGPD estabelece que o consentimento deve ser uma manifestação livre, informada e inequívoca (fornecido por escrito ou por outro meio que demonstre a manifestação de vontade) pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada, sendo nulas as autorizações genéricas e cabendo ao controlador o ônus de provar que o consentimento foi obtido em conformidade com as regras legais.

E, ainda, caso seja fornecido por escrito, o consentimento deverá constar de cláusula destacada das demais cláusulas contratuais.

Acontece que não é todo e qualquer consentimento que será válido para possibilitar o tratamento de dados pessoais, sejam eles sensíveis ou não, visto que a própria Lei dispensa sua exigência em determinados casos como, por exemplo, quando os dados forem tornados manifestamente públicos pelo titular, desde que observados os seus demais direitos.

Há de se salientar, ainda, que, como já dito, o consentimento pode ser revogado a qualquer tempo pelo titular dos dados, inclusive quando discordar das alterações de informação quanto à finalidade, à forma e à duração do tratamento; à identificação do controlador e ao compartilhamento dos dados, consoante prevê o §6º do Artigo 8º da Lei em comento.

No que se refere ao Interesse Legítimo, cumpre destacar que a LGPD não apresenta definição concreta acerca do que consideraria legítimo, o que torna necessária a aplicação do conceito previsto nos Artigos 47, 48 e 49 do GDPR Europeu, realçando o seguinte:

Artigo 49, 1 - 2, 3 e 4 – GDPR

"Quando uma transferência não puder ser baseada em uma disposição do artigo 45 ou 46, incluindo as disposições relativas às regras corporativas vinculativas, e nenhuma das derrogações para uma situação específica referida no primeiro parágrafo do presente número for aplicável, ***uma transferência para um país terceiro ou uma organização internacional só pode ocorrer se a transferência não for repetitiva , diz respeito apenas a um número limitado de titulares de dados, é necessário para efeitos de interesses legítimos convincentes prosseguidos pelo responsável pelo tratamento que não sejam anulados pelos interesses ou direitos e liberdades do titular dos dados, e o responsável pelo tratamento avaliou todas as circunstâncias que envolvem os dados transferência e, com base nessa avaliação, forneceu garantias adequadas no que diz respeito à proteção de dados pessoais.*** *O responsável pelo tratamento deve informar a autoridade de controlo da transferência. O responsável pelo tratamento deve, para além de fornecer as informações referidas nos artigos 13.º e 14.º, informar o titular dos dados sobre a transferência e sobre os* ***interesses legítimos*** *imperiosos prosseguidos".*

Nesta linha, a LGPD estabelece em seu Artigo 10 que o legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam, ao apoio e promoção de atividades do controlador e à proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os

direitos e liberdades fundamentais. O mesmo Artigo 10, em seus parágrafos, define que, quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados e deverão ser adotar medidas para garantir a transparência do tratamento fundamentado nessa base legal. Além disso, a autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Há de se salientar que, mesmo antes da edição da LGPD, Leonardi (2011), já destacava o Legítimo Interesse como base legal necessária para estimular o desenvolvimento econômico e tecnológico do País,

"Dados sem insight são inúteis – em realidade, dados brutos estão para o conhecimento assim como a areia está para os chips de silício. Dados bem utilizados – dados "inteligentes" – permitem análises profundas e conhecimento integrado que beneficiam a sociedade. A análise inteligente de dados é um dos principais impulsionadores da economia atual e do crescimento futuro – e isso só se faz possível mediante o emprego correto do ***legítimo interesse*** *como base legal do tratamento" (*Kohls et.al.,2021, p.55)

2.1.11. Direitos dos Titulares dos Dados

Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, conforme preceitua o Artigo 17 da Lei Geral.

Além disso, a LGPD relaciona rol de direitos do titular dos dados pessoais em relação ao controlador, conforme Tabela 13:

Tabela 13 – Direitos dos Titulares dos Dados nos termos da LGPD

DIREITO	DESCRIÇÃO
CONFIRMAÇÃO	O titular dos dados pessoais tem direito, a qualquer momento, de solicitar a confirmação da existência de tratamento e deverá ser atendido imediatamente, em formato simplificado, ou, em até 15 dias, em declaração clara e completa.
ACESSO	O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, bem como, a qualquer momento, de solicitar a confirmação de acesso aos dados quando deverá ser atendido imediatamente, em formato simplificado, ou, em até 15 dias, em

	declaração clara e completa.
CORREÇÃO	O titular dos dados pessoais tem direito a obter, a qualquer momento, a correção de dados incompletos, inexatos ou desatualizados.
SUPRESSÃO/ ELIMINAÇÃO	O titular dos dados pessoais tem direito a obter, a qualquer momento, anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na LGPD, exceto quando necessário para cumprimento de obrigação legal ou regulatória; para pesquisa; transferência a terceiro ou para uso exclusivo do controlador (anonimizados).
PORTABILIDADE	O titular dos dados pessoais tem direito a obter, a qualquer momento, a portabilidade dos dados a outro fornecedor de serviço ou produto, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial.
TRANSPARÊNCIA COMPARTILHAMENTO	O titular dos dados pessoais tem direito a obter, a qualquer momento, informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados.
INFORMAÇÃO - NÃO CONSENTIMENTO	O titular dos dados pessoais tem direito a obter, a qualquer momento, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
REVOGAÇÃO DE CONSENTIMENTO	O titular dos dados pessoais tem direito a revogar o consentimento, a qualquer momento, por procedimento gratuito e facilitado, ratificados os tratamentos consentidos anteriormente, enquanto não houver requerimento de eliminação
PETIÇÃO	O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional e os organismos de defesa do consumidor
REVISÃO	O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito **INTERESSE** o ou os aspectos de sua personalidade.
INTERESSE	Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.
GARANTIA	Os direitos e princípios expressos na LGPD não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que o Brasil seja parte.
INFORMAÇÃO - NÃO CONSENTIMENTO	O titular dos dados pessoais tem direito a obter, a qualquer momento, informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa.
REVOGAÇÃO DE CONSENTIMENTO	O titular dos dados pessoais tem direito a revogar o consentimento, a qualquer momento, por procedimento gratuito e facilitado, ratificados os tratamentos consentidos anteriormente, enquanto não houver requerimento de eliminação
PETIÇÃO	O titular dos dados pessoais tem o direito de peticionar em relação aos seus dados contra o controlador perante a autoridade nacional e os organismos de defesa do consumidor

Fonte: elaborada pela Autora (2022)

2.1.12 Dados Sensíveis

Como indicado no tópico correspondente às definições legais, dado pessoal sensível é todo 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.

No que se refere aos dados pessoais sensíveis, aos quais o Legislador projetou especial proteção, tendo em vista o seu potencial discriminatório, a LGPD estabelece que seu tratamento apenas poderá ocorrer quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas e, na hipótese de não haver o consentimento, o tratamento somente será possível quando for indispensável para as hipóteses[13] de Políticas Públicas, Processo, Contratos, Obrigação Legal, Pesquisa, Tutela da Saúde, Proteção e Prevenção[14].

No que tange a esse grupo de dados, a LGPD prevê, ainda, que a comunicação ou o uso compartilhado de dados pessoais sensíveis entre controladores com objetivo de obter vantagem econômica poderá ser objeto de vedação ou de regulamentação por parte da autoridade nacional.

Por fim, Toscano (2022) alerta que o estabelecimento dessas vedações como regra tem a finalidade de evitar situações discriminatórias.

2.1.13 Dados Anonimizados

Precisa a LGPD, como já salientado, que dado anonimizado é dado relativo ao titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento, que impõem a perda da possibilidade de associação, direta ou indireta.

Deste modo, os dados anonimizados não serão considerados dados pessoais para os fins da LGPD, salvo quando o processo de anonimização ao qual foram submetidos for revertido, utilizando exclusivamente meios próprios, ou quando, com esforços razoáveis (levando em consideração fatores objetivos, tais como custo e tempo necessários), puder ser revertido.

A anonimização, portanto, é uma maneira de preservar a identidade do titular dos dados pessoais de uma série de riscos e, segundo corroborado pelo

[13] Vide definições na Tabela 12.

[14] Garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardado o direito de informação e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

SERPRO ao reproduzir o entendimento de especialistas, “dados anonimizados são essenciais para o crescimento da inteligência artificial, da internet das coisas, do aprendizado das máquinas, das cidades Inteligentes, da análise de comportamentos, entre outros”[15].

2.1.14 Sanções

Um dos principais pontos que destacam a LGPD ao compará-la com as anteriores que, de alguma forma abordavam a proteção à privacidade, é a possibilidade de os agentes de tratamento de dados, ficarem sujeitos a sanções administrativas diversas, em razão das infrações cometidas às normas previstas na Lei Geral.

A LGPD elenca as sanções administrativas[16] que podem ser aplicadas pela ANPD, após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados a gravidade e a natureza das infrações e dos direitos pessoais afetados; a boa-fé, a cooperação, a vantagem auferida ou pretendida e a condição econômica do infrator; a reincidência; o grau do dano; a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados; a adoção de política de boas práticas e governança; a pronta adoção de medidas corretivas e a proporcionalidade entre a gravidade da falta e a intensidade da sanção, observando-se as hipóteses da Tabela 14:

Tabela 14 – Sanções previstas na LGPD

SANÇÃO	DESCRIÇÃO
ADVERTÊNCIA	Advertência, com indicação de prazo para adoção de medidas corretivas.
MULTA SIMPLES	Multa de até 2% do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 por infração.
MULTA DIÁRIA	Multa diária, observado o limite total de 50.000.000,00 por infração.

[15] https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-anonimizados-lgpd

[16] As sanções previstas na LGPD não substituem e não excluem as sanções administrativas, civis ou penais.

PUBLICIZAÇÃO	Publicização da infração após devidamente apurada e confirmada a sua ocorrência.
BLOQUEIO	Bloqueio dos dados pessoais a que se refere a infração até a sua regularização.
ELIMINAÇÃO	Eliminação dos dados pessoais a que se refere a infração.
SUSPENSÃO BANCO DE DADOS - PARCIAL	Suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador.
SUSPENSÃO ATIVIDADE - PARCIAL	Suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período.
PROIBIÇÃO - ATIVIDADE	Proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

Fonte: elaborada pela Autora (2022)

A austeridade normativa acometeu as organizações que, com o receio de sofrerem penalidades, vêm tomando medidas de segurança, técnicas e administrativas cada vez mais rigorosas no tratamento de dados pessoais, a fim 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, em observância ao teor do Artigo 46 da LGPD.

Entretanto, embora preveja penalidades pela inobservância das medidas de segurança de dados, a LGPD não esclarece quais seriam os mecanismos de proteção necessários. Sendo assim, a aplicação prática da Lei depende da coletânea de outros normativos, ou, simplesmente, de um *framework*, como a ISO[17], para o desenvolvimento de boas práticas já validadas e aceitas internacionalmente.[18]

A ISO possui dezenas de padrões que tratam do ativo de informações seguras. Dentre eles, podem ser citados conforme Tabela 15:

Tabela 15 – Padrões de tratamento do ativo de informações seguras

ISO	DESCRIÇÃO
27000	Fornece a visão geral, os termos e as definições comumente usados nos sistemas de gerenciamento de segurança da informação. Este documento é aplicável a todos os tipos

[17] A ISO é uma organização internacional não governamental independente, sediada na Suíça, com 167 membros de organismos nacionais de normalização. Por meio de seus membros, reúne especialistas para compartilhar conhecimento e desenvolver Normas Internacionais voluntárias, baseadas em consenso e relevantes para o mercado que apoiam a inovação e fornecem soluções para os desafios globais.

[18] Frameworks são estruturas compostas por um conjunto de códigos genéricos que permite o desenvolvimento de sistemas e aplicações.

	e tamanhos de organização.
27001	Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação no contexto da organização. Também inclui requisitos para a avaliação e tratamento dos riscos de segurança da informação adaptados às necessidades da organização. Os requisitos estabelecidos na ISO/IEC 27001:2013 são genéricos e destinam-se a ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.
27002	Fornece diretrizes para padrões organizacionais de segurança da informação e práticas de gerenciamento de segurança da informação, incluindo a seleção, implementação e gerenciamento de controles levando em consideração o ambiente de risco de segurança da informação da organização.
27005	Fornece diretrizes para gerenciamento de riscos de segurança da informação, tendo sido desenvolvido para auxiliar a implementação satisfatória da segurança da informação com base em uma abordagem de gerenciamento de risco.
27701	Especifica os requisitos e fornece orientação para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gerenciamento de Informações de Privacidade no contexto das organizações de todos os tipos e portes.

Fonte: elaborada pela Autora (2022)

Neste sentido, nos termos da Lei Geral e dos regulamentos complementares publicados por organismos internacionalmente respeitados, como medidas técnicas podem ser considerados os processos de controle de acesso às informações no limite da necessidade de cada agente; gerenciamento de sistemas por senhas; execução regular de *backups*; configuração de segurança das estações de trabalho dos empregados que manuseiam dados sensíveis e utilização regular da autenticação eletrônica multifatorial.

No que tange ao gerenciamento de senhas, cumpre ressaltar a necessidade de observância dos critérios de sua definição, visto que, conforme pesquisa divulgada em novembro de 2021, pelo serviço de senhas da NordPass, das 200 senhas mais expostas pelo mundo, a combinação "123456" ocupou o ranking mundial.

Registra-se, ainda, que nomes próprios, times de futebol e palavras como "felicidade", "sucesso" e "família" estavam nas 50 primeiras posições.

Já como medidas administrativas, podem ser considerados os mecanismos de revisão dos instrumentos contratuais celebrados com empregados, fornecedores, parceiros, clientes e prestadores de serviços, de modo a adequar suas cláusulas à LGPD e ao sistema de segurança da organização, bem como a estruturação de políticas de segurança da informação e a realização de treinamentos internos de modo a conscientizar os operadores responsáveis pelo tratamento dos dados sensíveis da necessidade de observância dos regramentos estabelecidos.

2.1.15 Regras de Tratamento de Dados de Saúde

Este tópico clarifica o objeto central da presente pesquisa, os dados de saúde que, como visto, é um dos principais elementos sensíveis da vida privada.

Antes de adentrar no processo de tratamento desses dados, é importante registrar que, conforme salientam Barbosa e Lopes (2021), no que se refere aos dados de saúde, o GDPR foi a primeira legislação a desenvolver uma conceituação, definindo-os, em seu artigo 4º, como sendo dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de Organizações de Saúde, que revelem informações sobre o seu estado de saúde.

A legislação europeia destaca, ainda, como vetor importante dos dados de saúde os dados genéticos como sendo os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa.

No entanto, conforme determina a Lei Geral Europeia, a regra de vedação poderá ser excepcionalizada quando:

- houver consentimento expresso do titular para uma ou mais finalidades especificadas.

- o tratamento for necessário para efeitos do cumprimento das obrigações e do exercício dos direitos específicos do responsável pelo tratamento ou do titular dos dados no domínio do direito do trabalho e da segurança social e proteção social.

- o tratamento for necessário para proteger os interesses vitais do titular dos dados ou de outra pessoa singular quando o titular dos dados for pessoa física ou legalmente incapaz de dar o seu consentimento.

- o tratamento é efetuado no decurso das suas atividades legítimas com as devidas garantias por uma fundação, associação ou qualquer outra entidade sem fins lucrativos com fins políticos, filosóficos, religiosos ou sindicais e na condição

de o tratamento se referir exclusivamente aos membros ou a antigos membros do órgão ou a pessoas que com ele tenham contato regular no âmbito das suas finalidades e que os dados pessoais não sejam divulgados fora desse órgão sem o consentimento dos titulares dos dados.

- o tratamento diz respeito a dados pessoais que são manifestamente tornados públicos pelo titular dos dados.

- for necessário para a instauração, exercício ou defesa de ações judiciais ou sempre que os tribunais atuem na sua capacidade judicial.

- for necessário por motivos de interesse público substancial, com base no direito da União ou do Estado-Membro, que deve ser proporcionado ao objetivo prosseguido, respeitar a essência do direito à proteção de dados e prever medidas adequadas e específicas para salvaguardar os direitos fundamentais e os interesses do titular dos dados.

- for necessário para fins de medicina preventiva ou do trabalho, para avaliação da capacidade de trabalho do trabalhador, diagnóstico médico, prestação de cuidados ou tratamentos de saúde ou sociais ou gestão de sistemas e Organizações de Saúde ou de assistência social.

- tratamento necessário por motivos de interesse público no domínio da saúde pública, como a proteção contra ameaças transfronteiriças graves para a saúde ou a garantia de elevados padrões de qualidade e segurança dos cuidados de saúde e dos medicamentos ou dispositivos médicos e para fins de arquivo de interesse público, para fins de investigação científica ou histórica ou para fins estatísticos.

Entretanto, não obstante a relevância do modelo europeu, haja vista a necessidade de delimitação de escopo, no que tange às regras de tratamento de dados de saúde, a partir deste ponto, a pesquisa se limitará ao espaço territorial brasileiro, analisando-se as significativas mudanças perpetradas pela LGPD na Cultura Organizacional das Organizações de Saúde públicas e privadas brasileiras, eis que há questionamentos relativo à aparente conflito entre os avanços em pesquisas de diagnósticos com os ditames legais.

A legislação brasileira, quanto a esse tópico, assenta que é vedada 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 Organizações de Saúde, de assistência farmacêutica e de assistência à saúde, desde que observada a vedação às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários.

A LGPD excepciona o tratamento de dados pessoais sensíveis referentes à saúde também para os serviços auxiliares de diagnose e terapia, em benefício dos interesses dos titulares de dados, e para permitir a portabilidade de dados quando solicitada pelo titular e para as transações financeiras e administrativas resultantes do uso e da prestação das Organizações de Saúde.

O Artigo 13 da Lei Geral brasileira estabelece que, na realização de estudos em saúde pública, os órgãos de pesquisa poderão ter acesso a bases de dados pessoais, que serão tratados exclusivamente dentro do órgão e estritamente para a finalidade de realização de estudos e pesquisas e mantidos em ambiente controlado e seguro, conforme práticas de segurança previstas em regulamento específico e que incluam, sempre que possível, a anonimização ou pseudonimização[19] dos dados, bem como considerem os devidos padrões éticos relacionados a estudos e pesquisas.

Neste sentido, a divulgação dos resultados ou de qualquer excerto do estudo ou da pesquisa, em nenhuma hipótese, poderá revelar dados pessoais, sendo o órgão de pesquisa o responsável pela segurança da informação, bem como não será permitida, em circunstância alguma, a transferência dos dados a terceiro, cujo acesso será objeto de regulamentação por parte da autoridade nacional e das autoridades da área de saúde e sanitárias, no âmbito de suas competências.

No que tange à aplicação da LGPD nas Organizações de Saúde, verifica-se que as operações afetadas são diversas, como, por exemplo, para a elaboração de prontuários médicos, o armazenamento (em ambiente físico ou virtual) e sua

[19] Pseudonimização é o tratamento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, senão pelo uso de informação adicional mantida separadamente pelo controlador em ambiente controlado e seguro (artigo 13, § 4º, LGPD)

eliminação; pesquisas clínicas; compartilhamento de dados pessoais sensíveis como quando da solicitação de autorização para realização de exames ou atualização do estado de saúde; processos de reembolso de despesas; e, ainda, a retenção do receituário médico em farmácias e cadastro em programas de descontos, para certos medicamentos.

Nestes casos, embora haja outras nove hipóteses permissivas na LGPD, o consentimento do titular é de extrema relevância para o gerenciamento dos processos na esfera da saúde, onde a coleta de dados íntimos dos pacientes, dos consumidores e dos empregados é condição imprescindível ao exercício da atividade.

Portanto, a implementação da LGPD nas Organizações de Saúde é tradução de respeito aos direitos e garantias dos titulares dos dados pessoais, bem como fortalece a competitividade empresarial, visto que a observância às Lei, o *Compliance*, é considerado um diferenciador num mercado altamente competitivo, além de prevenir a aplicação de penalidades.

2.1.16 A LGPD e o Sigilo Médico

Não obstante o Código de Ética Médica e as Resoluções do CFM já preverem proteção ao sigilo da relação médico-paciente, com o advento da LGPD, a proteção dos dados pessoais e sensíveis dos usuários deveriam se dar por um aspecto amplo, tendo em vista a proteção vigorosa do Legislador.

Ocorre que, como já dito, a LGPD não traz previsão detalhada sobre os requisitos inerentes ao sigilo médico, muito embora esse já fosse objeto de preocupação nas diversas normas éticas do CFM, complementadas pela CRFB, pelo Código Civil e pelo Código Penal e já estivesse integrada à Cultura Organizacional das unidades médicas.

Todavia, a ausência de uma Lei formal poderia trazer fragilidades para ambas as partes quando da ocorrência de situações reais de conflito.

Neste sentido, embora a LGPD trate do tema de forma generalista, sem pormenorizar as normas para o sigilo médico, a Lei Geral é fundamental para embasar as normas setoriais de ética médica possibilitando abordagens mais seguras para os direitos e garantias fundamentais dos pacientes.

2.1.17 A LGPD e os Trabalhadores de Serviços Médicos

A LGPD tem aplicação em todos os setores da economia, o que significa dizer que também é aplicável às relações trabalhistas, que debatem diretamente elementos relacionados à privacidade, conforme descrito na CLT e reproduzido na Tabela 16.

Tabela 16 – Elementos da privacidade de empregados previstos na CLT

ARTIGO	DESCRIÇÃO
223-C	A honra, a imagem, a intimidade, a liberdade de ação, a autoestima, a sexualidade, a saúde, o lazer e a integridade física são os bens juridicamente tutelados inerentes à pessoa física.
168	Será **obrigatório exame médico**, por conta do empregador, nas condições estabelecidas neste artigo e nas instruções complementares a serem expedidas pelo Ministério do Trabalho: I - a admissão; II - na demissão; III - periodicamente. §2º. Outros **exames complementares poderão ser exigidos**, a critério médico, para apuração da capacidade ou aptidão física e mental do empregado para a função que deva exercer. §6º. Serão **exigidos exames toxicológicos**, previamente à admissão e por ocasião do desligamento, quando se tratar de motorista profissional, assegurados o direito à contraprova em caso de resultado positivo e a confidencialidade dos resultados dos respectivos exames.
169	Será **obrigatória a notificação das doenças profissionais e das produzidas em virtude de condições especiais de trabalho**, comprovadas ou objeto de suspeita, de conformidade com as instruções expedidas pelo Ministério do Trabalho.
373-A	Ressalvadas as disposições legais destinadas a corrigir as distorções que afetam o acesso da mulher ao mercado de trabalho e certas especificidades estabelecidas nos acordos trabalhistas, é **vedado**: IV - **exigir atestado ou exame**, de qualquer natureza, **para comprovação de esterilidade ou gravidez**, na admissão ou permanência no emprego.

Fonte: elaborada pela Autora (2022)

Nesse ambiente, desde a seleção até o momento posterior à rescisão do contrato, diversos dados pessoais e a imagem de pessoas naturais são coletados e tratados, como histórico de licenças, existência de contato com agentes nocivos, informações referentes a saúde física e mental, tipo sanguíneo, filiação sindical, orientação sexual e armazenamento de dados biométricos.

Há de se considerar, ainda, que, em se tratando de Organizações de Saúde, além da hipótese de compartilhamento de dados para concessão de benefício de plano de saúde, os empregados podem se valer da estrutura física do empregador para realização de consultas e exames médicos, próprio e de dependentes, aumentando o debate acerca da autonomia e possível fragilização do exercício dos direitos da personalidade do empregado.

Portanto, pautado no fundamento da autodeterminação informativa construído pela LGPD, o empregado deve ser estimulado a tomar o controle sobre a destinação dos dados pessoais dos quais é titular, justificado por uma relação de transparência que deverá desenvolver com o controlador desses dados, quem deverá adotar padrão de qualidade de segurança, com regras de boas práticas e *compliance*; treinamentos e políticas internas, como forma de prevenir eventual vazamento e, por consequência, a ocorrência de danos irreparáveis à dignidade, à vida privada e à intimidade do empregado.

Ocorre que, tendo em vista a ausência de tratamento específico da LGPD e da CLT, quanto aos requisitos para tratamento de dados em ambiente profissional, há diversos momentos em que os direitos da personalidade do empregado conflitam com os interesses econômicos do empregador. Nestes casos, o empregado pode se valer de medidas legais como Reclamação Trabalhista individual perante a Justiça do Trabalho; Denúncias a órgãos de fiscalização, em especial Ministério Público do Trabalho e Ministério do Trabalho; Ação coletiva proposta pelo Ministério Público do Trabalho (MPT), na hipótese de haver dano à coletividade e Denúncia à ANPD.

Outro ponto relevante no que se refere à relação da LGPD com as questões trabalhistas diz respeito à base legal que fundamentará a atuação da Organização de Saúde, na qualidade de empregadora. Nesse tópico, em razão de sua relevância e controvérsias, também se dará destaque ao consentimento. Como já salientado, o consentimento deve ser uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

No entanto, sua aplicação nas relações trabalhistas ainda é vista com muita cautela, sobretudo em razão do "princípio básico do Direito do Trabalho", que pressupõe a hipossuficiência do trabalhador frente ao empregador, em razão do desequilíbrio de poder e pela dependência econômica, o que poderia desvirtuar a manifestação legítima de vontade.

Por isso, caso o empregador opte pela utilização do consentimento com fundamento legal para o tratamento dos dados do empregado, é recomendado que observe as regras legais previstas na LGPD, tal como a formalização por escrito ou por outro meio que demonstre a manifestação de vontade do titular e, em sendo por escrito, que priorize a utilização de cláusula destacada.

2.1.18 Correção de Informações nas Organizações de Saúde

O Artigo 18, III, da LGPD, estabelece que o titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição, a correção de dados incompletos, inexatos ou desatualizados.

No entanto, o instituto necessita de cautela quando se trata de registros médicos, visto que não devem ser alterados exclusivamente por ausência de concordância do titular do prontuário, em observância ao princípio fundamental da liberdade profissional, previsto no Código de Ética Médica[20], sob pena de configura um abuso desse direito.

Deste modo, no que tange à proteção ao adequado tratamento de dados pessoais, sob a égide da LGPD, opiniões clínicas e diagnósticos registrados em documentos médicos, salvo quando contiverem falhas ou imprecisões, não possuem obrigatoriedade de correção.

2.1.19 Telemedicina

Em abril de 2020, foi publicada a Lei nº 13.989, que dispõe sobre o uso da telemedicina, durante a crise causada pelo coronavírus (COVID-19), significando dizer que seria autorizado o exercício da medicina mediado por tecnologias para fins de assistência, pesquisa, prevenção de doenças e lesões e promoção de saúde.

A principal proposta da telemedicina é complementar o atendimento presencial (e não o substituir), de modo a reduzir o intervalo de tempo entre as consultas. Ocorre que, por ocorrer no ambiente online, essa forma de atuação ainda gera insegurança e questionamento quanto à lisura da base tecnológica para inserção de dados pessoais e informações íntimas de pacientes.

É indiscutível que a telemedicina é um avanço e deixa mais evidente que a proteção e a privacidade de dados instituíram uma nova cultura corporativa. Entretanto, debate-se se esse modelo de atendimento virtual permanecerá ativo

[20] Código de Ética Médica – Item VIII - O médico não pode, em nenhuma circunstância ou sob nenhum pretexto, renunciar à sua liberdade profissional, nem permitir quaisquer restrições ou imposições que possam prejudicar a eficiência e a correção de seu trabalho.

no futuro, embora tenha se tornado uma prática muito comum e com consequências positivas, segundo o CFM.

A Resolução nº 2.314, de 20 de abril de 2022, do CFM, ao regulamentar a telemedicina previu diversos elementos com a salvaguarda da LGPD. Todavia, chama a atenção o teor do Artigo 3º que estabelece que, nos serviços prestados por telemedicina, os dados e imagens dos pacientes, constantes no registro do prontuário devem ser preservados, obedecendo as normas legais e do CFM pertinentes à guarda, ao manuseio, à integridade, à veracidade, à confidencialidade, à privacidade, à irrefutabilidade e à garantia do sigilo profissional das informações.

O destaque é necessário pois, aparentemente, pelo menos no que se refere à estrutura normativa, o CFM não hesitou em adequar-se ao regulamento geral de proteção de dados, a LGPD. Porém, a aplicação prática ainda demanda ações efetivas para que a proteção de dados disponibilizados no meio digital alcance a proposta legal e garanta efetivamente a segurança à dignidade e à privacidade almejada pelos cidadãos ao longo de toda a história, o que não mais pode ser suprido pelo sigilo médico e pelo simples e genérico consentimento.

2.2 Aspectos Culturais

2.2.1 Conceituando Cultura Organizacional

Embora Elliot Jacques (PERRET, 2009) já mencionasse o conceito de cultura nas décadas de 40 e 50, como sendo a forma habitual e tradicional de pensar e agir, sensivelmente compartilhada pelos membros ou grupos da empresa, somente nos anos 80 ficou mais evidente a inquietação dos administradores com os valores e as crenças comuns dos empregados e o impacto que reproduzem nos resultados das organizações. Passou-se a debater, então, a Cultura Organizacional.

Neste sentido, Schein (1983) analisa o conceito de cultura no seio organizacional definindo-o como um instrumento estruturalmente complexo que envolve um grande conjunto de pressupostos e crenças capazes de definir como os membros de um grupo enxergam suas relações internas e externas e compartilham suas histórias que, como fruto de alinhados entre si, gerarão paradigmas

comportamentais de alta ordem sobre a natureza do espaço, realidade, tempo, pessoas e relações.

Segundo o autor, a Cultura Organizacional, então, é o padrão de suposições básicas que um dado grupo inventou, descobriu ou desenvolveu ao aprender a lidar com seus problemas de adaptação externa e integração interna — um padrão de suposições que funcionou suficientemente bem para ser considerado válido e, portanto, para ser ensinado aos novos membros como a maneira correta de perceber, pensar e sentir em relação a esses problemas.

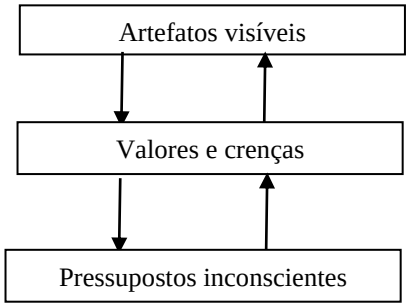
Schein (1998) esclarece que a evolução da cultura é um processo de vários estágios da formação do grupo e a Cultura Organizacional definitiva sempre refletirá a interação complexa entre as suposições e teorias que os fundadores levam para o grupo inicialmente e o que o grupo aprende posteriormente com suas próprias experiências.

A Cultura Organizacional, portanto, é capaz de estimular mudanças na estrutura e nos procedimentos da organização e no comportamento de seus membros, sendo constantemente desempenhada e criada por nossas interações com outros e moldada por comportamento de liderança, em um conjunto de estruturas, rotinas, regras e normas. (SCHEIN, 2009).

2.2.2 Modelo de Schein (1991) de três Níveis de Cultura Organizacional

A cultura tange todos os aspectos da organização: estrutura, estratégia, processos e sistemas de controle e para que seu conceito seja melhor absorvido, Schein (1991) propõe a cisão em três níveis, conforme Figura 1.

Figura 1 – Três Níveis de Cultura Organizacional



Fonte: Schein (1991) – adaptada pela Autora

Os três níveis podem ser descritos como:

- **Artefatos visíveis**, considerados, pelo autor, como sendo fáceis de se observar, mas difíceis de se decifrar e podem ser exemplificados como sendo a arquitetura do meio-ambiente; a linguagem; a tecnologia e os produtos; as demonstrações emocionais; os mitos e as histórias contadas sobre a organização; suas listas de valores publicadas; seus rituais e cerimônias observáveis; os processos organizacionais pelos quais esses comportamentos se tornam rotineiros e os elementos estruturais, como cartas, descrições formais de como a organização funciona e organogramas.

- **Valores e crenças** que governam o comportamento das pessoas, considerados, pelo Autor, como sendo toda aprendizagem refletida em um grupo que se incorpora em uma ideologia ou filosofia organizacional e pode servir como guia para lidar com a incerteza de eventos intrinsecamente incontroláveis ou difíceis.

- **Pressupostos inconscientes**, também chamados de Suposições Básicas Subjacentes, definidos pelo autor como a parte mais profunda da Cultura Organizacional, que não sofre mudanças ou se transformam lentamente, sendo considerados um consenso que resulta de sucesso repetido na implementação de certas crenças e valores.

> *Qualquer cultura de grupo pode ser estudada nesses três níveis – o nível de seus artefatos, o nível de suas crenças e valores expostos e o nível de suas suposições básicas prevalecentes. Se alguém não decifrar o padrão de suposições básicas que está operando, não saberá como interpretar corretamente os artefatos ou quanto crédito dar aos valores articulados. Em outras palavras, a essência de uma cultura está no padrão das suposições básicas prevalecentes e, uma vez que alguém as entenda, é possível entender facilmente os níveis mais superficiais e lidar apropriadamente com eles. (SCHEIN, 2009, p. 33).*

2.2.3 Modelo de Fleury (1996) de manifestações culturais

A partir da concepção de Schein (1991), Fleury(1996) sinaliza a necessidade de uma proposta conceitual que incorpore a dimensão política na interpretação da cultura e conceitual a Cultura Organizacional como tendo sido concebida a partir de um conjunto de valores e pressupostos básicos expressos em elementos simbólicos, que em sua capacidade de ordenar, atribuir significações, construir a identidade organizacional, tanto age como elemento de comunicação e consenso, como resulta e instrumentaliza as relações de dominação. (FLEURY, 1996)

Para compreensão da Cultura Organizacional, Fleury sugere as seguintes perspectivas:

- Histórico das organizações: análise do ambiente no qual o estabelecimento empresarial está inserido, a partir do momento da criação, de sua inserção no contexto político e da forma pela qual os fundadores inspiram a visão da organização.
- Processo de socialização de novos membros: capacidade da organização de transmitir valores e comportamentos aos novos membros.
- Política de Recursos Humanos: Desenvolvimento de mecanismos de Recursos Humanos compatíveis com o padrão cultural da organização (processos de recrutamento, seleção, treinamento etc.).
- Processos de comunicação e decisão: Desenvolvimento de mecanismos de comunicação e decisão compatíveis com o padrão cultural da organização, sejam formais (reuniões, memorandos etc.) ou informais.
- Organização do processo de trabalho: Indicação das categorias profissionais da organização, que possibilita, inclusive, o mapeamento das relações de poder existentes.

2.2.4 Modelo de Quinn & Rohrbaugh (1983) do Valor Competitivo Framework (CVF)

Quinn & Rohrbaugh (1983) desenvolveram a tipologia cultural CVF que auxilia a análise da eficácia das políticas organizacionais e a efetividade das ações propostas pelas lideranças e distingue quatro tipos de cultura com limites e características claras, permitindo a comparação de cultura em todas as

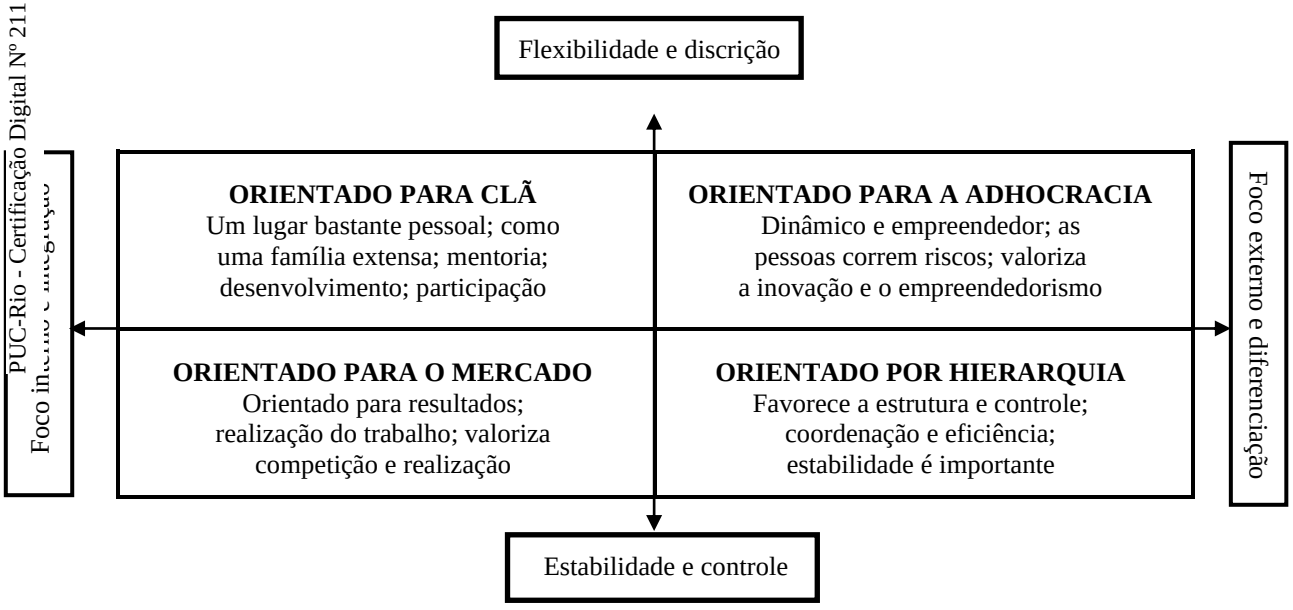
organizações.

Na tipologia cultural CVF, duas dimensões são usadas para diferenciar os tipos de organização. Uma dimensão (horizontal) mostra a orientação de uma organização para o mundo exterior, evidenciando aquelas que só cuidam do bem-estar e desenvolvimento da própria organização dentro de seu ambiente (Quinn & Rohrbaugh, 1983) e buscam ser diferentes para ficarem à frente dos concorrentes.

A segunda dimensão (vertical) enfatiza que algumas organizações são mais eficazes quando são estáveis e outras se beneficiam por serem flexíveis (Quinn & Rohrbaugh, 1983).

A Tipologia cultural CVF posiciona quatro tipos de Cultura Organizacional, conforme Figura 2:

Figura 2 – Quatro perfis de Cultura Organizacional



Fonte: Cameron e Quinn (1999) – adaptada pela Autora

a) Cultura tipo Mercado, Objetivos ou Racional: fazer rápido

Insere-se no modelo dos objetivos racionais, estando orientada para o exterior, desempenho e controle. Tem como fins a produtividade, a competitividade e a eficiência, utilizando o planeamento e a fixação de objetivos como meios para os

alcançar. A liderança deve ser diretiva, orientada para as metas e encorajar a produtividade.

b) Cultura tipo *Adhocracia*, Inovação ou Empreendedora: fazer primeiro

Insere-se no modelo dos sistemas abertos, estando por isso orientada para a flexibilidade, mudança e para o exterior. Os seus fins são o crescimento e a aquisição de recursos, utilizando a rapidez de resposta e a capacidade de adaptação como meios para os atingir. O critério de eficácia assenta na quota de mercado e no volume de negócios. O líder deve reforçar a vontade de correr riscos e a capacidade de desenvolver uma visão estratégica, assim como facilitar a aquisição de recursos, legitimidade e conseguir visibilidade.

c) Cultura tipo Clã ou Apoio: fazer junto

Enquadra-se no modelo das relações humanas, como tal coloca a ênfase na flexibilidade e no lado interno da organização. Tem como principal objetivo a criação e a manutenção da coesão e do empenho dos seus membros, valorizando a confiança, a participação e o sentimento de pertença. Procura o envolvimento das pessoas e fomenta o trabalho em equipa. O critério de eficácia assenta no desenvolvimento do potencial humano e no envolvimento das pessoas. A liderança deve reforçar a participação, a consideração, o apoio e a lealdade, bem como estimular o trabalho em grupo.

d) Cultura tipo Hierarquia ou Regras: fazer direito

Está ligada ao modelo dos processos internos, colocando a ênfase no meio interno e na estabilidade, caracterizada por um trabalho formalizado e bastante estruturado. Visa a segurança e a estabilidade, devendo o líder utilizar as regras, os procedimentos e a gestão da informação para manter a organização unida.

As Culturas do Clã e Empreendedora compartilham sua ênfase na flexibilidade (Quinn et al., 1983), permitindo assim a mudança. No entanto, a Cultura do Clã valoriza a coesão e é focada internamente, enquanto a Empreendedora, caracterizada pela inovação, pelo crescimento e pela adaptabilidade, é mais orientada para o exterior, o que permite que reconheça as pressões externas para arriscar e mudar na busca de se tornar líder de mercado.

Os gestores que operam dentro de uma Cultura Racional querem ser competitivos, porque seus consumidores são seletivos e escolhem a alternativa mais eficiente e isso indica ganância e liderança orientada para objetivos, refletida em altos salários de gestão (Jacobs et al., 2013).

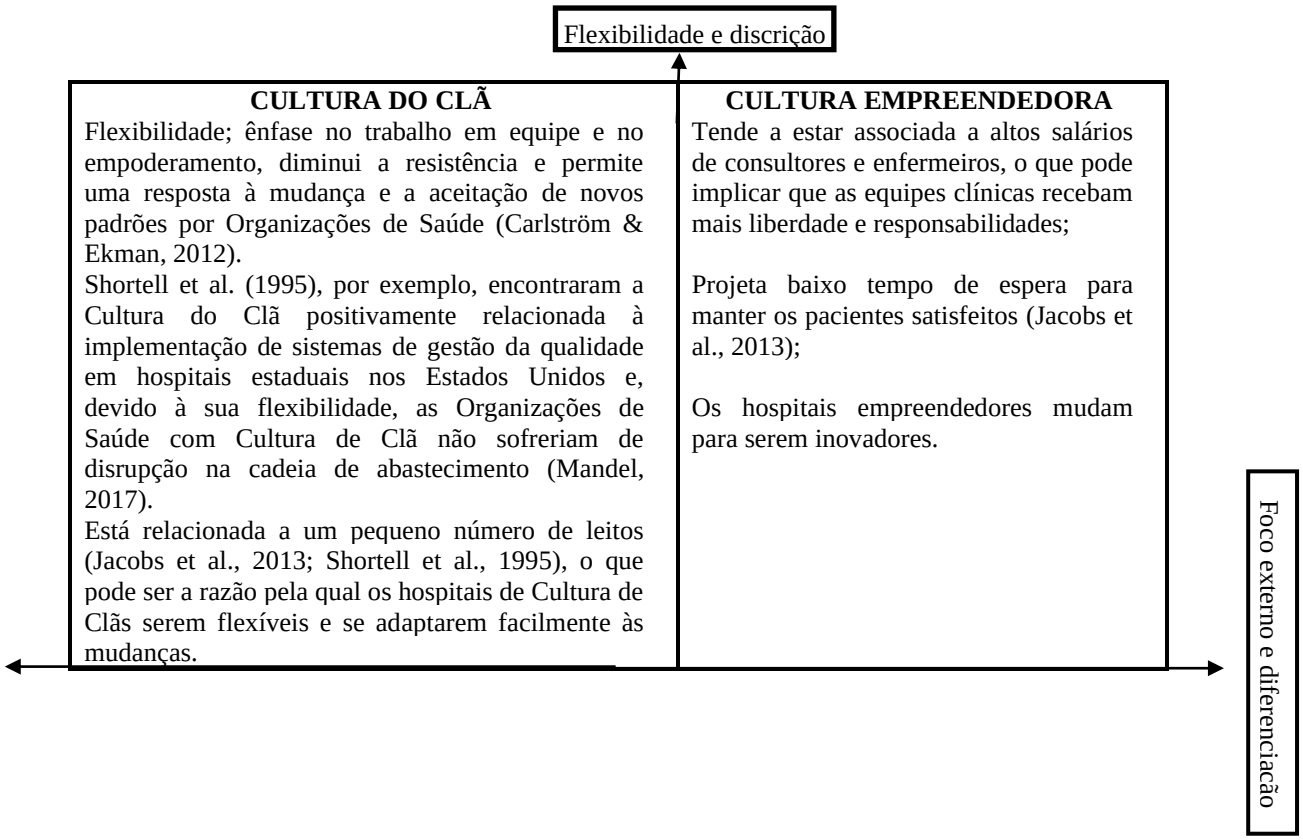
Já uma organização com Cultura Hierárquica concentra-se na organização interna e está comprometida com regras e políticas, o que dá suporte à qualidade dos dados (Jacobs et al., 2013). No entanto, surgem problemas com a adaptação às pressões externas.

2.2.5 A Cultura de Organizações de Saúde

Kooistra (2018) destaca que literatura, frequentemente, relaciona o método CVF, de Quinn e Rohrbaugh (1983), à análise da Cultura de Organizações de Saúde (Acar & Acar, 2012; Carlström & Ekman, 2012; Jacobs et al., 2013; Mandal, 2017; Shortell et al., 1995; Wagner et al., 2014).

Assim, sob o prisma do método CVF, a Cultura de Organizações de Saúde pode ser interpretada de acordo com a Figura 3 (Kooistra, 2018):

Figura 3 – Perfis de Cultura Organizacional de Organizações de Saúde



CULTURA RACIONAL	CULTURA HIERÁRQUICA
Tende a estar presente em hospitais que possuem grande capacidade financeira e gerencial (Jacobs et al., 2013); A ampliação da participação de investidores privados no setor hospitalar pode aumentar competição e os salários dos administradores, o que favorece a Cultura Racional. Hospitais com Cultura Racional se adaptam à mudança principalmente para ficar à frente de concorrentes e para evitar interrupções na cadeia de suprimentos (Mandal, 2017).	As características hierárquicas parecem restringir os processos de mudança e podem estar presentes em grandes hospitais. Nos hospitais suecos, por exemplo, a Cultura Hierárquica induz medo no coletivo, o que dificulta a mudança (Carlström & Ekman, 2012). Devido à manutenção da estabilidade e controle, as Organizações de Saúde com Cultura Hierárquica têm dificuldades em responder a interrupções na cadeia de suprimentos (Mandal, 2017). Shortell et al (1995) descobriram que grandes hospitais têm mais dificuldades em implantar um sistema de qualidade do que hospitais de pequeno porte, porque os grandes hospitais são organizados burocraticamente e têm uma Cultura Hierárquica. Nesse sentido, os grandes hospitais enfrentam desafios difíceis ao se adaptarem a uma mudança institucional

Estabilidade e controle

Fonte: elaborada pela Autora (2022)

A Cultura Organizacional, portanto, é uma divisão importante desse processo organizacional, sendo considerada um determinante-chave tanto no funcionamento dos sistemas de saúde quanto na qualidade dos cuidados prestados (Davies et al, 2009).

Neste sentido, tem-se que há elementos da Cultura Organizacional que podem constituir um freio ou um impulso para o desenvolvimento de um serviço de excelência, sobretudo quanto aos desafios enfrentados pelas equipes hospitalares.

Quanto aos aspectos da cultura que poderiam constituir um freio são a pouca capacidade de visão de futuro, a má comunicação, a pouca colaboração entre as áreas, as especialidades e serviços (trabalho em equipe), a não gestão por processos, o desenvolvimento não pleno de valores como consagração, senso crítico e autocrítico, a criatividade e a unidade, a pouca sistematicidade na atuação do pessoal para o alcance de objetivos de curto e longo prazo e a insuficiente participação de empregados na solução de problemas em seu nível, características semelhantes às identificadas na pesquisa de Rocha et. al. (2014).

Podem constituir um freio, ainda, o uso de punições e ameaças como forma de realização das atividades, a má organização do trabalho e a gestão insuficiente do conhecimento, que afetam diretamente a continuidade do atendimento médico.

Por outro lado, o desenvolvimento de uma Organização de Saúde de excelência pode ser impulsionado por uma mudança institucional fomentada pela Cultura Organizacional e moldado por restrições formais e informais.

Muitas dessas restrições estão relacionadas à estrutura das organizações. Com essa compreensão, o Centro Regional de Estudos sobre o Desenvolvimento da Sociedade da Informação (Cetic.br), departamento do Centro de Informação em Redes Brasileira (NIC.br), vinculado ao Comitê Gestor da Internet Brasileira (CGI.br), no ano de 2022, realizou uma pesquisa com amostra inicial de 6.029 estabelecimentos de saúde e 4.486 profissionais de saúde e com amostra efetiva de 2.127 estabelecimentos de saúde e 1.942 Profissionais de saúde[21].

Dentre os estabelecimentos de saúde, foram contempladas as Organizações públicas e privadas, com e sem internação, estabelecidas em todas as regiões do País.

Com isso, foram mapeados os perfis quanto ao tipo de informação armazenada, transmitida/recebida, bem como a forma de armazenamento e acesso ao conteúdo.

De acordo com a pesquisa, as Organizações de Saúde entrevistadas utilizam meios eletrônicos e físicos (papel) para manutenção das informações pessoais dos pacientes, conforme Tabela 17.

Tabela 17 - Forma de manutenção das informações clínicas e cadastrais nos prontuários dos pacientes

FORMA DE MANUTENÇÃO DAS INFORMAÇÃO DOS PACIENTES	TOTAL DE ORGANIZAÇÕES
APENAS EM FORMATO ELETRÔNICO	617
APENAS EM PAPEL	213
PARTE EM PAPEL E PARTE EM FORMATO ELETRÔNICO	1.234

Fonte: CGI/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – adaptada pela Autora

[21] Coleta de dados: Entrevistas telefônicas (CATI) e questionário web

Em complemento a esse ponto, estimativa divulgada pela Anestech[22] aponta que 92% dos anestesistas do Brasil ainda usam papel para registrar os prontuários dos pacientes, com lançamento de informações a cada cinco minutos, o que pode significar, em procedimentos complexos, até cem anotações e um alto risco quanto à integridade e segurança dessas informações.

Em relação às organizações que utilizam, ainda que parcialmente, sistemas eletrônicos, a pesquisa apontou quais os dados por elas armazenados, conforme Tabela 18.

Tabela 18 – Dado sobre o paciente disponível eletronicamente nas Organizações de Saúde

DADO DO PACIENTE DISPONÍVEL ELETRONICAMENTE	TOTAL DE ORGANIZAÇÕES
DADOS CADASTRAIS	1.850
ADMISSÃO, TRANSFERÊNCIA E ALTA DO PACIENTE	1.255
ALERGIAS DO PACIENTE	1.468
DIAGNÓSTICO, PROBLEMAS OU CONDIÇÕES DE SAÚDE DO PACIENTE	2.874
PRINCIPAIS MOTIVOS QUE LEVARAM O PACIENTE AO ATENDIMENTO OU CONSULTA	1.510
RESULTADOS DE EXAMES LABORATORIAIS DO PACIENTE	1.425
LAUDO DE EXAMES RADIOLÓGICOS DO PACIENTE	1.000
IMAGENS DE EXAMES RADIOLÓGICOS DO PACIENTE	681
LISTA DE MEDICAMENTOS PRESCRITOS AO PACIENTE	1.361
SINAIS VITAIS DO PACIENTE	1.170
HISTÓRICO OU ANOTAÇÕES CLÍNICAS SOBRE O ATENDIMENTO AO PACIENTE	1.638
ANOTAÇÕES DE ENFERMAGEM SOBRE O PACIENTE	1.319
VACINAS ADMINISTRADAS AO PACIENTE	1.106

Fonte: CGI/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – adaptada pela Autora

Dentre os dados de pacientes armazenados pelas organizações que utilizam sistema eletrônico, há aqueles que costumam ser enviados ou recebidos, conforme Tabela 19.

Tabela 19 - Funcionalidades de troca de informações de paciente entre Organizações de Saúde

TIPO DE INFORMAÇÃO	TOTAL DE ORGANIZAÇÕES

[22] https://medicinasa.com.br/anestesistas-prontuario/

INFORMAÇÕES CLÍNICAS	702
ENCAMINHAMENTOS ELETRÔNICOS	872
RELATÓRIO SOBRE A ASSISTÊNCIA PRESTADA AO PACIENTE NO MOMENTO EM QUE TEVE ALTA OU FOI ENCAMINHADO A OUTRO ESTABELECIMENTO DE SAÚDE	830
LISTA DE TODOS OS MEDICAMENTOS PRESCRITOS AO PACIENTE	638
RESULTADOS DE EXAMES LABORATORIAIS	681
RESULTADOS DE EXAMES DE IMAGEM	489
PLANO DE CUIDADOS DA ENFERMAGEM	489

Fonte: CGI/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – adaptada pela Autora

Por fim, o CGI/NIC.br concluiu que as Organizações de Saúde brasileiras acessam os prontuários dos pacientes armazenados eletronicamente, por meio de pontos diversos, conforme Tabela 20.

Tabela 20 - Pontos de acesso ao prontuário eletrônico do paciente

PONTO DE ACESSO	TOTAL DE ORGANIZAÇÕES
COMPUTADORES FIXOS DISTRIBUÍDOS PELA ORGANIZAÇÃO	1.744
REDE INTERNA QUE PODE SER ACESSADA EM QUALQUER LUGAR DO ESTABELECIMENTO POR UM COMPUTADOR PORTÁTIL, TABLET OU CELULAR	1.234
FORA DA ORGANIZAÇÃO, PELA INTERNET	936

Fonte: CGI/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – adaptada pela Autora

2.3. Aspectos legais e culturais: A Cultura de Proteção de Dados nas Organizações de Saúde

Ao longo dos últimos anos, observou-se um aumento no uso de computadores e acesso à Internet pelas Organizações de Saúde, surgindo, a partir de então, os chamados "Hospitais 4.0"[23]. No Brasil, o número de Organizações de Saúde que utilizam a tecnologia para registro de informação de pacientes passou de 82% no ano de 2019 para 88% em 2021[24], o que foi crucial para o combate aos efeitos e ao avanço da epidemia causada pela

[23] Integração dos serviços hospitalares com tecnologia.
[24] https://cetic.br/media/docs/publicacoes/2/20211130124545/tic_saude_2021_livroeletronico.pdf

COVID-19.

Além disso, a pandemia causada pela COVID-19 impactou a Cultura Organizacional das Organizações de Saúde ao evidenciar a necessidade do uso de tecnologias disruptivas, como Inteligência Artificial (IA) e *Big Data Analytics*, por permitirem o desenvolvimento de inovações tecnológicas mais avançadas para descoberta de vacinas e medicamentos; monitoramento de pacientes infectados; dispositivos de telemedicina e análise de dados como medida de políticas públicas.

Esse avanço traz, além de muitos benefícios, grandes desafios para a estruturação de medidas de preservação da privacidade e garantia dos direitos individuais dos pacientes e profissionais de saúde, com a adoção de ferramentas de segurança modernas e adequação de processos internos à LGPD.

São profundos os impactos para adequação das Organizações de Saúde que controlam dados pessoais sensíveis referentes à saúde (Dallari & Monaco, 2021. Em razão disso, pesquisas[25] revelam que, no ano de 2021, menos da metade das Organizações de Saúde havia implementado medidas de adequação às exigências da LGPD e apenas um terço tinha uma política de segurança da informação definida.

Alerta-se que ainda há muitos desafios para serem superados até a garantia da segurança jurídica que sustentará o avanço da saúde digital no Brasil (Ministério da Saúde, 2021), visto que, além da necessidade de ajustes nos procedimentos básicos, ainda permanecem lacunas sensíveis sobre como deve ser realizada a transferência de dados com terceiros, a interoperabilidade em saúde e a definição de procedimentos para os profissionais de saúde.

As ferramentas de segurança da informação são parte da cultura de garantia para o avanço da saúde digital e foram mapeadas pelo CGI/NIC.br, conforme Tabela 21.

[25] A coleta dos dados foi realizada por entrevistas por telefone e questionário web com 1.524 gestores entre janeiro e agosto de 2021.

Tabela 21 – Ferramentas de segurança da informação utilizadas por Organizações de Saúde

FERRAMENTAS DE SEGURANÇA DA INFORMAÇÃO	TOTAL DE ORGANIZAÇÕES
ASSINATURA ELETRÔNICA	915
ARQUIVOS E E-MAILS CRIPTOGRAFADOS	1.000
PROTEÇÃO POR SENHA DE ARQUIVOS ENVIADOS OU RECEBIDOS	1.021
PROTEÇÃO POR SENHA DO ACESSO AO SISTEMA ELETRÔNICO	1.744
ANTIVÍRUS	1.914
FIREWALL	1.319
CRIPTOGRAFIA DA BASE DE DADOS	936
CERTIFICADO DIGITAL	1.063
BIOMETRIA PARA ACESSO AO SISTEMA ELETRÔNICO	255
DUPLO-FATOR DE AUTENTICAÇÃO	383
PROTEÇÃO CONTRA VAZAMENTO DE INFORMAÇÃO (DLP- DATA LOSS PROTECTION/ PREVENTION)	596

Fonte: CGI/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – adaptada pela Autora

A pesquisa mapeou, também, as medidas adotadas pelas Organizações de Saúde em relação à LGPD, conforme Tabela 22.

Tabela 22 – Medidas adotadas por Organizações de Saúde em relação à LGPD

MEDIDA ADOTADA	TOTAL DE ORGANIZAÇÕES
DEFINIU O ENCARREGADO DE SEGURANÇA DE DADOS	702
DISPONIBILIZOU CANAIS DE ATENDIMENTO E INTERAÇÃO COM OS TITULARES DOS DADOS	553
PUBLICOU A POLÍTICA DE PRIVACIDADE EM WEBSITE	553
REALIZOU CAMPANHA DE CONSCIENTIZAÇÃO INTERNA COM MAIS DE 50% DOS EMPREGADOS	872
IMPLEMENTOU UM PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DE DADOS	659

Fonte: CGI/NIC.br, Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação – adaptada pela Autora

Embora a pesquisa do CGI/NIC.br aponte que já havia um movimento de preocupação com a segurança da informação, é evidente que, no ano de 2022, ainda era discreto e seria necessário fortalecer a cultura de proteção de dados das Organizações de Saúde, de modo que seus processos e procedimentos estivessem alinhados à LGPD como parte indissociável da Cultura Organizacional.

Ser parte indissociável da Cultura Organizacional significa dizer, também, que a proteção de dados é respeitada pelos líderes que, no exercício de um papel importante no delineamento do comportamento dos profissionais, ensinam certas crenças e valores no sentido de reduzir a incerteza em áreas críticas (SCHEIN, 2017), possibilitando a construção de um novo *mindset* dos empregados, o que é necessário em novos cenários e modelos de gestão mais modernos e maduros (MADRUGA, 2021).

2.3.1 Fragilidade dos Sistemas de Proteção de Dados nas Organizações de Saúde

Durante toda a história, a sociedade tem acompanhado diversos episódios de exposição de informações sensíveis relacionadas à saúde de usuários – pacientes e empregados.

O primeiro exemplo é o memorável caso do Imperador Otto von Bismarck, figura extremamente popular da Alemanha, que, no ano de 1898, foi fotografado em seu leito de morte, dentro de sua própria casa, com o objetivo de negociação das imagens do seu corpo.

Não obstante a edição de Leis específicas de proteção de dados e os investimentos em segurança da informação, estudiosos afirmam que ainda não é possível eliminar os riscos em sua integralidade e as empresas da área de saúde permanecem na iminência de invasão à vida privada e vazamento de dados.

Estudo[26] da Varonis, com a análise de mais de 3 bilhões de arquivos de 58 empresas privadas, em todo o mundo, aponta que as Organizações de Saúde ainda estão distantes do modelo ideal de segurança dos dados.

O resultado analisado apontou que empresas do setor de saúde tinham grupos de contas-fantasma[27] cadastradas com números alarmantes, conforme Tabela 23.

[26] Publicado pela revista Medicina S/A em 28/04/2021- https://medicinasa.com.br/seguranca-digital-saude/

[27] A Conta fantasma é uma forma de conta de convidado com permissões limitadas e será usada como a conta padrão do sistema até que o dispositivo seja marcado como recuperado, impedindo que qualquer pessoa entre em suas outras contas de usuário ou acesse dados de usuário. Fonte: https://help.eset.com/home_eset/pt-BR/antitheft_issue_no_fakeuseraccount.html#:~:text=A%20Conta%20fantasma%20%C3%A9%20uma,ou%20acesse%20dados%20de%20usu%C3%A1rio.

Tabela 23 – Volume de contas-fantasma em Organizações de Saúde

VOLUME DE CONTA-FANTASMA	TOTAL DE ORGANIZAÇÕES
MAIS DE 10.000	22
ENTRE 1.000 E 10.000	57
ATÉ 1.000	21

Fonte: Elaborada pela Autora

Além disso, a pesquisa evidenciou contas de ex-empregados para acesso aos sistemas que não haviam sido encerradas, bem como contas de terceiros que deveriam ter sido usadas apenas por um período e continuavam ativas, se tornando alvo para *Hackers*, *Black Hat, Script Kiddies, Cracker*, *Spy Hacker*, [28].

> *"Mesmo com a LGPD, as empresas do setor de Saúde no Brasil ainda não têm a segurança de dados como um foco de tecnologia. O investimento ainda é visto como um gasto desnecessário. Porém, a tendência é que cada vez mais as empresas do setor de Saúde sofram com ataques virtuais -e com penalizações pesadas, porque guardam muitos dados sensíveis." (Mariana Nunes, Gerente de Canais da Varonis no Brasil - R*evista Medicina S/A)[29]

O estudo da Varonis aponta, ainda, que todas as organizações avaliadas apresentaram volumes altos de arquivos confidenciais e acessíveis por qualquer usuário que tivesse uma conta cadastrada, sem controle de acesso por perfil, ainda

[28] Hacker é uma pessoa que possui um grande conhecimento informático e que se encontra em constante estudo sobre a área, capaz de invadir o sistema de outrem para entretenimento e aprendizagem, e não a fim de criminalizar, bem como auxiliar aqueles que não possuem seu conhecimento.
Black Hat (hacker mal-intencionado): diferentemente dos white hats, os black hats se utilizam das vulnerabilidades que encontram para obter dados sigilosos, como dados pessoais, senhas, dados bancários etc. São definidos, por alguns autores, como subcategoria dos crackers.
Script Kiddies não têm um alvo certo. Normalmente, utilizam ferramentas prontas que foram produzidas por algum "black hat", sem saber exatamente como ela funciona. O "script kid" não sabe ao certo o que está fazendo, e, por este motivo, quando consegue invadir um site importante, acaba fazendo certo alvoroço.
Cracker: pertencente ao "lado negro". Possui muito conhecimento informático, tendo como foco principal em seu estudo o funcionamento dos softwares (programas). São responsáveis pela criação dos cracks, que são ferramentas utilizadas na quebra da ativação de um software comercial, facilitando a pirataria. São definidos como criminosos, eis que operam em fraudes bancárias e eletrônicas, furto de dados, golpes, entre outros.
Spy Hacker: hackers contratados por empresas para obterem dados sigilosos de empresas concorrentes.

[29] Publicado pela revista Medicina S/A em 28/04/2021- https://medicinasa.com.br/seguranca-digital-saude/

que houvesse variação em virtude do tamanho da Organização de Saúde, conforme Tabela 24.

Tabela 24 – Acesso a arquivos confidenciais em Organizações de Saúde

ORGANIZAÇÃO DE SAÚDE POR PORTE	TOTAL DE ARQUIVOS CONFIDENCIAIS ACESSADOS POR QUALQUER USUÁRIO
PEQUENO PORTE (ATÉ 500 EMPREGADOS)	22
MÉDIO PORTE (ENTRE 500 E 1.500 EMPREGADOS)	14
GRANDE PORTE (MAIS DE 1.500 EMPREGADOS)	11

Fonte: Elaborada pela Autora

Ademais, do volume total de arquivos confidenciais com acesso disponível a todos os usuários com conta cadastrada, cerca de 70% eram arquivos com informações desatualizadas que ficavam como inativas por um longo período (meses ou anos).

> *"Arquivos desatualizados representam risco e custo, mas não agregam muito valor", (...) Eles são uma oportunidade para as organizações reduzirem os riscos rapidamente. Se ninguém está usando esses dados, eles realmente precisam ser abertos a todos na empresa? É preciso identificar essas oportunidades e diminuir a exposição rapidamente." (Mariana Nunes, Gerente de Canais da Varonis no Brasil - R*evista Medicina S/A)[30]

Contas de acesso a sistemas criadas e disponibilizadas com baixo controle; informações confidenciais abertas a todos da organização; falha humana; inadequação de processos de tratamento de dados dão origem a inúmeros casos de vazamentos de dados de saúde, o que demanda uma resposta rápida e eficaz ao incidente e reparação dos danos.

Nesse ponto, podem ser citadas ocorrências públicas, em diversos países, de aplicação de penalidade a unidades de Saúde, como o Centro Hospitalar Barreiro Montijo, de Portugal, multado, no ano de 2018, em cerca de R$ 400 mil Euros por violação a regras do GDPR, expondo dados clínicos dos pacientes, bem

[30] Publicado pela revista Medicina S/A em 28/04/2021- https://medicinasa.com.br/seguranca-digital-saude/

como concedendo acesso indiscriminado a um conjunto de dados por parte de profissionais, que só deveriam acessá-los em casos pontuais.[31]

Em março de 2018, o hospital holandês Erasmus MC foi criticado por falha na proteção de dados confidenciais após 46 crianças infectadas pelo HIV terem seus endereços de e-mail vazados por um enfermeiro especialista ao enviar um boletim informativo.

Em novembro de 2019, um hospital do Brooklyn, EUA, sofreu um ataque cibernético que levou o hospital a perder dados de pacientes, como nomes e imagens cardíacas e dentárias, conforme descreve a *Checkpoint Research*, em seu Boletim de Inteligência de Ameaça de 11 de novembro de 2019.

A *Checkpoint Research* descreve, ainda, os episódios dos Centros de Fertilidade de Illinois (FCI), clínicas de fertilidade com sede nos EUA, que relataram uma violação das informações pessoais de saúde de 80.000 pacientes, bem como dos empregados da empresa. Neste caso, o invasor teria utilizado uma conta administrativa para obter acesso a dados altamente confidenciais generalizados.

Continuamente, descreve que o provedor de Organizações de Saúde Broward Health, com sede na Flórida, EUA, sofreu uma violação significativa que afetou mais de 1,3 milhão de indivíduos, na qual os criminosos cibernéticos obtiveram acesso às informações médicas dos pacientes.

No Brasil, o Hospital Israelita Albert Einstein, em projeto conjunto com o Ministério da Saúde, confirmou que, em 25 de novembro de 2020, houve o vazamento de dados de 16 milhões de pessoas que tiveram suspeita ou diagnóstico confirmado para COVID-19. De modo contínuo, os dados pessoais e médicos expostos ficaram disponíveis na Internet por cerca de um mês, após o vazamento de senhas de sistemas do Ministério da Saúde[32]. Entretanto, embora a LGPD já

[31] Após longa disputa judicial, em julho de 2020, a CNPD reapreciou o pedido de dispensa da aplicação da multa, inicialmente apresentado no ano de aplicação da multa, admitindo que, em contexto pandêmico – COVID-19, a situação específica do infrator e do interesse público em concreto afetado com a aplicação da multa prevalece, nestas circunstâncias excepcionais, sobre o interesse público de punição do infrator.
Não obstante, o Hospital ajustou sua Política de Privacidade (http://www.chbm.min-saude.pt/cidadao/protecao-de-dados), estabelecendo elementos saneadores aos riscos apontados no relatório do CNPD de Portugal, como, exemplo, a regra de que dados relacionados com a sua saúde apenas serão tratados por profissionais obrigados a sigilo e na medida do necessário à prestação de cuidados de saúde.

[32] Em 26/11/2020, o Hospital Israelita Albert Einstein, em São Paulo, Brasil, emitiu nota à imprensa confirmando o vazamento dos dados e dando publicidade às medidas tomadas, como a

existisse, os dispositivos que regulam as sanções aplicáveis em tais casos ainda não estavam em vigor, de modo que não puderam ser aplicados.

Não obstante a impossibilidade de aplicação de penalidades da LGPD antes do início de sua vigência, qualquer titular de dados pessoais vazados indevidamente nesses episódios poderia pleitear judicialmente a indenização pelos danos materiais e morais decorrentes.

Foi o que ocorreu com o caso do Hospital Santa Helena, do Distrito Federal, Brasil, em ação distribuída em 15 de janeiro de 2021, tendo sido condenado pelo Tribunal de Justiça do Distrito Federal e dos Territórios a pagar indenização total de cerca de R$ 7.000,00 (sete mil reais), por danos morais e materiais, a uma paciente e a um dos seus familiares que foram vítimas de golpe durante o período de internação na unidade, uma vez que houve falha na guarda da informação pelo Hospital, possibilitando a ação de criminosos que lhes aplicaram golpes[33].

Há de se registrar que esse tipo de golpe não é recente. Porém, conforme esclarece o Sindicato dos Hospitais, Clínicas e Laboratórios de São Paulo (SINDHOSP)[34], a pandemia pela COVID-19 retomou a prática de ações por estelionatários que penetram no sistema informativo das Organizações de Saúde, aproveitando-se do momento de fragilidade de pacientes e familiares, e se passam por médicos ou empregados dos hospitais com o objetivo de auferir vantagem econômica indevida.

O SINDHOSP acrescenta que é importante a adoção de medidas preventivas, como revisão dos processos digitais e governança interna tendo por referência a LGPD, de modo a manter seguros os dados sensíveis dos pacientes.

No entanto, não é apenas a operação humana, de profissionais de saúde e gestores de unidades médicas, que coloca em risco a integridade dos dados pessoais, visto que equipamentos inteligentes também são canais propícios ao vazamento de dados, conforme de verifica na pesquisa[35] da Consultoria Unit42,

demissão do empregado por ter infringido as normas internas adotadas para garantir proteção e segurança de dados.

[33] Processo nº PJe: 0702262-27.2021.8.07.0016 – Tribunal de Justiça do Distrito Federal e dos Territórios

[34] https://sindhosp.org.br/protecao-dados-saude-golpe/

[35] Segundo informações da Unit[42], a pesquisa foi realizada utilizando dados de *crowdsourcing* de varreduras de mais de 200.000 bombas de infusão nas redes de hospitais e outras organizações de saúde usando o IoT Security for Healthcare da Palo Alto Networks.

que mostra que 75% das bombas de infusão, dispositivos conectados à rede que fornecem medicamentos e fluidos aos pacientes em Organizações de Saúde, são vulneráveis a falhas e possuem o potencial de colocar vidas em risco ou expor dados confidenciais de pacientes.

E os episódios que expõem as fragilidades do sistema de segurança das unidades de saúde não se encerram pelos narrados neste tópico, haja vista que diversos outros casos de vazamento de dados e informações sigilosas em Organizações de Saúde se tornam públicos diariamente, acendendo um alerta para a sociedade e somando-se a diversas outras fraudes digitais e vazamentos que, no ano de 2021, colocaram o Brasil, pelo segundo ano consecutivo, no topo mundial em vazamento de dados, com 2,8 bilhões de dados sensíveis expostos, conforme Relatório de Atividade Criminosa Online no Brasil divulgado pela *Axur* em fevereiro de 2022.

Considerando-se, então, que os ataques cibernéticos são um problema real, bem como considerando-se que os ataques de *ransomware* em Organizações de Saúde cresceram 94% no ano de 2021 e estão numa crescente, conforme o Relatório *"The State of Ransomware in Healthcare 2022",* da *Sophos*, a fim de contribuir com o avanço do tema, a presente pesquisa orientará os tons de rigor necessários ao fluxo do tratamento das informações, reduzindo os riscos de descumprimento da Lei, por possibilitar a exposição indevida de dados sensíveis, e de aplicação de penalidades, de modo a otimizar a Cultura Organizacional das Organizações de Saúde.

2.3.2 O papel da Cultura Organizacional no processo de adequação de Organizações de Saúde à LGPD

Oliveira e Lopes (2018) remeteram inquérito a 190 clínicas médicas distribuídas pelos 18 distritos de Portugal mais os arquipélagos da Madeira e dos Açores, entre os meses de outubro e dezembro de 2017[36], a fim de avaliar a implementação do GDPR europeu no segmento de saúde.

Todavia, apenas 30% das unidades contactadas responderam às perguntas sobre a implementação das medidas vertidas no regulamento, bem como sobre as

[36] Cerca de 6 meses antes de o GDPR passar a ser exequível.

ações de formação e sensibilização dos empregados sobre as novas regras e os planos internos já realizados para estarem em conformidade com o Regulamento.

Não obstante o baixo volume de respostas, o resultado da pesquisa de Oliveira e Lopes (2018) impressiona, visto que, poucos meses antes da efetividade do GDPR, a adesão ainda era baixa, conforme Tabela 25.

Tabela 25 – Organizações de Saúde frente ao GDPR

MEDIDA ADOTADA	TOTAL DE ORGANIZAÇÕES
IMPLEMENTAÇÃO DO GDPR	4
DESCONHECIMENTO DO GDPR	11
NÃO PENSAVAM EM IMPLEMENTAR O GDPR	11

Fonte: Oliveira e Lopes (2018)

Os que afirmaram que não pensavam na implementação do GDPR apresentaram como justificativa: a falta de recursos financeiros; a adoção de práticas de tratamento de dados consideradas suficientes; a falta de necessidade de investimento em razão do tamanho da organização ou a falta de conhecimento sobre como adotar as medidas.

Embora a duração da implementação do GDPR dependesse da complexidade da atividade da empresa; do volume e da variedade de dados pessoais utilizados; do estado de maturidade da empresa em termos organizacionais; da adequabilidade e da flexibilidade dos sistemas de informação e da disponibilidade de todos os envolvidos, mais da metade das organizações respondentes considerou insuficiente o período de dois anos de vacância para adaptação da Cultura Organizacional (Oliveira e Lopes, 2018).

A Cultura Organizacional desempenha um papel decisivo na adaptação ao Regulamento de Proteção de Dados, sobretudo quando a organização não fornece orientação suficiente (Kooistra, 2018). Ademais, é capaz de identificar, entre outros, por que algumas organizações respondem lentamente à mudança institucional, enquanto outras organizações são capazes de responder rapidamente às pressões externas.

Kooistra (2018) aponta diversas ambiguidades do GDPR, reproduzidas pela LGPD, e acrescenta que o Regulamento Geral é difícil de ler. Por exemplo, uma das condições de dados de saúde pede consentimento explícito, mas nenhuma definição é dada para a palavra “explícito”, o que poderia afetar a implementação

do consentimento (Armstrong & Bywater, 2017), além de possibilitar interpretações diversas pelas Organizações de Saúde que acabam estabelecendo suas próprias políticas, bem como adaptam a Lei à sua Cultura Organizacional.

Assim, se os hospitais seguem Culturas Organizacionais diferentes, as informações podem ser interpretadas de forma diferente e, portanto, os hospitais podem reagir de forma diferente.

Ao pesquisar se e como a Cultura Organizacional influenciou o processo de adaptação de hospitais da Holanda ao GDPR, Kooistra (2018), tomando por base a sugestão da literatura de que a Cultura Organizacional influencia a forma como uma mudança é adaptada e que o tamanho da Organização de Saúde influencia na Cultura Organizacional, selecionou seis hospitais de tamanhos diversos (sendo três de pequeno porte e três de grande porte), entrevistando doze profissionais em cada um deles.

O resultado da pesquisa de Kooistra (2018) descreve que todos os hospitais pesquisados promoviam o GDPR durante a introdução de novos empregados e faziam
apresentações sobre o assunto durante as reuniões. Essas eram as únicas técnicas pelas quais um pequeno hospital promovia o GDPR.

Verificou-se, ainda, que 28 hospitais conscientizavam os empregados para o GDPR por meio do jornal da equipe e da intranet. No entanto, o depoimento de um dos entrevistados chamou atenção por afirmar que técnicas como essas não funcionavam, já que a equipe de atendimento não lia os comunicados pois estava ocupada com o cuidado com pacientes, diferentemente da equipe que trabalha nos escritórios. E essa diferença de abordagem precisaria ser observada pela liderança.

No quesito “portabilidade de dados”, cinco hospitais holandeses afirmaram que não tinham controle sobre a liberdade de fluxo de dados na União Europeia. Já no tópico “registro das atividades de processamento”, quatro unidades não mantinham registro de atividades de processamento antes da entrada em vigor do GDPR, sendo que, as unidades que faziam registros, os consideravam frágeis e incompletos.

O DPO em hospitais de pequeno porte emprega uma dupla jornada em vez de uma função de tempo integral como os DPO de dois grandes hospitais. Mas, quando se trata de violações de dados, todos os hospitais dependem da

cultura e conscientização entre os empregados.

Por fim, Kooistra (2018) identificou algumas semelhanças e diferenças em como grandes e pequenos hospitais se adaptaram às mudanças trazidas pelo Regulamento de Proteção de Dados, destacando que o processo se deu de forma diferente, mas com técnicas que melhor se adaptavam à cultura e à realidade da Organização de Saúde.

3 Metodologia de pesquisa

3.1. Tipo de Pesquisa

Conforme mencionado na introdução do trabalho, a questão-chave da pesquisa é: "Qual o papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à LGPD?"

A escassez de estudos sobre a adaptação de Organizações de Saúde à LGPD nos leva a escolher uma metodologia qualitativa, visto que possibilita explorar tópicos relevantes; encontrar respostas para os problemas identificados e descrever processos (Rynes & Gephart, 2004).

A presente pesquisa é descritiva, com padronização das técnicas utilizadas para a coleta dos dados, afastando potenciais interferências ou julgamentos de cunho pessoal sobre os resultados obtidos (Mayring, 2014 e Gil, 1999).

Assim, a escolha do método de pesquisa descritivo-analítica, com abordagem qualitativa, possibilitará compreender o fenômeno da adaptação das Organizações de Saúde à LGPD em sua complexidade.

3.2. Coleta de dados

Além dos dados secundários coletados em pesquisa documental (livros, periódicos e matérias jornalísticas), neste trabalho foram coletados dados primários, mediante a realização de entrevistas semiestruturadas, que favorece uma análise sobre a adaptação à LGPD pelas Organizações de Saúde brasileiras.

Inicialmente, foram convidados dez gestores de Organizações de Saúde diversas. Porém, apenas cinco responderam às entrevistas individuais de cerca sessenta minutos cada, tendo sido gravadas e transcritas, com a autorização dos entrevistados.

A gravação permitiu que a entrevistadora se concentrasse na entrevista, o que permitiu um questionamento profundo, bem como a possibilidade de a entrevistadora fazer perguntas extras, quando necessário, e ajustar as perguntas às respostas do respondente.

As questões das entrevistas semiestruturadas foram separadas em duas categorias. A primeira parte da entrevista está preocupada com os aspectos legais da mudança institucional. Para cada mudança, foram feitas perguntas relacionadas ao tempo de adoção e como a mudança é implementada.

A segunda categoria está relacionada aos aspectos culturais. As questões desta parte visam analisar a Cultura Organizacional do hospital em momentos distintos: antes e após a publicação da LGPD, bem como encontrar evidências sobre a relação entre Cultura Organizacional e a mudança institucional.

O roteiro resumido a seguir tem o total de sete subcategorias, conforme Quadro 1:

Quadro 1 – Roteiro da entrevista

CATEGORIA	SUB CATEGORIA	QUESTÃO	OBJETIVO DA QUESTÃO
Aspectos Culturais	Normas	Já ouviu falar da LGPD?	Identificar se já há programa de adequação à LGPD implementado e o nível de abrangência da implementação da LGPD, bem como fazer uma análise histórica do processo de mudança.
		Como se dava o tratamento de dados de saúde antes da publicação da LGPD (14 de agosto de 2018)?	
		Implementou a LGPD na Organização de Saúde?	
		Se implementou, quando e como foi realizado esse processo?	
		Por quais grupos profissionais a implementação da LGPD é influenciada?	
		Se não implementou, implementaria?	
		Se não implementaria, qual a razão?	
		Se implementaria, pode precisar se seria a longo, a médio ou a curto prazo?	
	Liderança	Entre os anos de 2018 e 2022, a liderança estabeleceu alguma medida de delineamento do comportamento dos empregados para a adoção de práticas de proteção de dados?	Identificar o compromisso da liderança com a proteção de dados.
		Se estabeleceu, a liderança promove algum controle de leitura e cumprimento das práticas de proteção de dados pelos empregados?	
	Pessoas - empregados	Os empregados são informados sobre a LGPD quando são contratados?	Identificar o grau de conhecimento dos empregados sobre a LGPD; as práticas de saúde e de gerenciamento de informações sobre empregados e dependentes
		Os empregados efetivos são capacitados/ conscientizados/reciclados das práticas de proteção de dados?	
		Há canal de comunicação interno específico para reforçar as medidas de proteção de dados?	
		Como é o acesso dos empregados ao estabelecimento físico da Organização de Saúde? (exemplo: Biometria, crachá)	
		Como a Organização de Saúde cumpre a determinação de garantir exames admissionais, periódicos e demissionais aos empregados?	
		Qual o meio de coleta e armazenamento de informações de empregados quando da contratação e da atualização de dados	

		cadastrais e documentais pessoais e de dependentes?	pós LGPD.
		Há controle e limitação de acesso às informações de empregados e dependentes?	
		Com a saída de empregados da Organização de Saúde, as respectivas contas e senhas de acesso aos sistemas são excluídas ou mantidas?	
	Valores	A unidade de saúde é certificada em algum padrão ou framework de segurança que inclua armazenamento de dados (exemplo: ISO)?	Identificar as boas práticas de gestão da privacidade.
		Há artefatos de comunicação de boas práticas de proteção de dados disponibilizados pela Organização de Saúde (exemplo: cartazes, telas digitais)?	
Aspectos Legais	Princípios	Em relação a dados incompletos, inexatos ou desatualizados, há política de correção e/ou eliminação e/ou revogação de consentimento a partir da requisição do titular? Há canal de comunicação direcionado exclusivamente para esse fim?	Identificar o cumprimento dos princípios da LGPD
		Há 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?	
		Há Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais?	
		Há prática de informação ao titular dos dados acerca da finalidade da coleta das informações?	
		Há política interna de controle da compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento?	
		Há política de adequação da coleta de dados que sejam essenciais à finalidade pretendida?	
	Gestão de dados	Como é o acesso de terceiros ao estabelecimento físico da Organização de Saúde (exemplo: biometria, fotografia)?	Identificar as práticas do gerenciamento de dados; o perfil dos dados coletados e o tratamento aplicado, bem como o respeito à dignidade de um dado sensível.
		Quais os dados coletados dos pacientes?	
		Foi realizado mapeamento dos dados tratados pela Organização de Saúde e adequação à base legal correspondente?	
		Há transferência de dados para outros países?	
		Qual a forma de cadastro e manutenção das informações clínicas e pessoais de pacientes nos prontuários (exemplo: sistema eletrônico, fichas em papel)?	
		Se ficha de papel, onde ficam armazenadas e como se dá o controle de acesso?	
		Se sistema eletrônico, onde está disponibilizado e como se dá o controle de acesso?	
		Qual o ponto de acesso aos prontuários eletrônicos dos pacientes (exemplo: computador na própria Organização de Saúde; acesso remoto)?	
		Há troca (envio/recebimento) de informações de pacientes com terceiros externos? Se sim, quais os dados trocados e os meios de comunicação utilizados?	
		Há controle das informações que podem ou não ser transferidas a terceiros?	
		O hospital aderiu à prática da telemedicina? Como se dá a coleta de informações do paciente e a identificação do profissional de saúde? O atendimento fica gravado e arquivado?	

		Quais são as informações solicitadas dos empregados e de seus dependentes e como é feito o controle de acesso às informações?	
		Qual o tratamento dado a informações obsoletas inseridas no sistema? Há política de eliminação de dados?	
		Há utilização de Inteligência Artificial e/ou de Big Data no monitoramento de pacientes?	
		Possui câmeras de segurança? Se sim, em quais locais?	
		A Organização de Saúde autoriza a utilização de "nome social" de transgêneros em seus sistemas de cadastro de empregados e pacientes?	
		Há definição de procedimento de portabilidade de dados do titular, a seu pedido, para outra empresa?	
		Há processos específicos de tratamento de dados sensíveis de pacientes e empregados?	
		Possui contas fantasmas? Se sim, qual o volume?	
		Há prática de criação de conta de terceiros para uso em período determinado? Se sim, com o término do período, as contas são excluídas ou permanecem ativas?	
	Segurança de Dados	Utiliza alguma ferramenta de segurança da informação (exemplo: assinatura eletrônica; arquivos e e-mails criptografados; proteção por senha de arquivos enviados ou recebidos; proteção por senha do acesso ao sistema eletrônico; antivírus; *firewall*; criptografia da base de dados; certificado digital; biometria para acesso ao sistema eletrônico; duplo-fator de autenticação; proteção contra vazamento de informação)?	Identificar o grau de segurança dos dados coletados.
		Implementou algum plano de resposta a incidentes de segurança de dados?	
		Implementou algum processo para tornar os dados pessoais anônimos?	
		Publicou a política de privacidade em website?	
		Disponibilizou canais de atendimento e interação com os titulares dos dados?	
		Utiliza alguma tecnologia para tornar dados armazenados anonimizados?	
		Definiu o encarregado de segurança de dados (DPO)?	
		Há registros de vazamentos de dados de saúde na Organização?	
		Há histórico de ação judicial em razão de questões relacionadas à proteção de dados de pacientes ou empregados)?	
		A Organização de Saúde já sofreu alguma sanção por descumprimento de regras de proteção de dados?	

Fonte: elaborado pela Autora

3.3. Seleção das Organizações de Saúde e dos Entrevistados

Foram selecionados cinco gestores, que, separadamente, representam um consultório médico; duas redes hospitalares (sendo uma responsável pela gestão de 15 hospitais; 409 centros médicos e uma operadora de saúde e a outra sendo gestora de 12 hospitais e 30 clínicas) e uma organização social prestadora de

serviços para unidades públicas de saúde. As entrevistas foram realizadas por videochamada e o critério da seleção dos participantes foi de conveniência e acessibilidade. Foram utilizados contatos pessoais para acessar todos os respondentes. Todos os participantes eram gestores de Organizações de Saúde. O Quadro 2 resume a informação demográfica dos entrevistados.

Quadro 2 – Informação demográfica dos participantes

N° entrevistado	Gênero	Formação Profissional	Função na Organização	Organização em que atua	Esfera Administrativa da Organização	Tempo de trabalho na Organização
1	Masculino	Médico	Gestor/Médico	Consultório Médico	Privada	40 anos
2	Masculino	Advogado	Diretor Jurídico / DPO	Rede Hospitalar de Medicina Diagnóstica de Alta Complexidade: - Grupo hospitalar (15 hospitais no Brasil) - Centros Médicos (379 consultórios e 30 unidades ambulatoriais de oncologia) - Operadora de saúde	Privada	13 anos
3	Feminino	Graduação em Matemática. Especialização em finanças. Mestrado em administração	Diretora Financeira	Hospital	Privada	3 anos
4	Feminino	Graduação em Nutrição. Especializações em Gestão Hospitalar	Diretora de Operações	Rede Hospitalar, com 12 Hospitais e 30 Clínicas distribuídos por 6 Estados Brasileiros	Privada	4 anos e 4 meses
5	Feminino	Graduação em Psicologia. Especialização em Gestão de Serviços de Saúde e em Qualidade e Segurança do Paciente	Gerente de Qualidade	Prestadora de Serviços Públicos por meio de Contrato de Gestão – UPAs, Hospitais e Centros de Especialidades Municipais	Organização Social	12 anos

Fonte: elaborado pela Autora

4 Análise dos Resultados

Neste capítulo, são discutidos os resultados da pesquisa, a partir da análise das respostas que estão relacionadas às subcategorias para, em seguida, responder à questão de pesquisa: "Qual o papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à LGPD?"

Nos casos analisados, é evidente o movimento de fortalecimento da proteção da vida privada e a ampliação do debate pelo mundo foi essencial para a construção de uma Cultura Organizacional de Saúde pautada na proteção da privacidade; no respeito aos princípios fundamentais e no sigilo profissional.

Em razão disso, todos os entrevistados, embora relatem que já tinham ouvido falar da LGPD e, com menor ou maior profundidade, já haviam analisado o impacto da nova Lei na rotina da Organização de Saúde que integram, sustentaram que as principais Leis infraconstitucionais (tabela 8) e os normativos regulamentados pelo Ministério da Saúde e pela ANS com procedimentos para registro e compartilhamento de informações de saúde de pacientes (tabela 9) já impunham um dever de privacidade que apenas teria sido corroborado pela LGPD. Os trechos das entrevistas a seguir ilustram esta constatação:

> *Já atuo há 25 anos na saúde. A LGPD só veio corroborar na saúde o que já era uma prática, que é a garantia da privacidade das informações de pacientes, sobretudo dos pacientes se pensarmos em prontuários médicos. Essa é uma guarda que já é tratada à luz da LGPD mesmo antes de ela existir no âmbito hospitalar. (Entrevistada 4)*

> *Têm regimentos próprios que tratam da ética médica. Então, essa ética médica é regimentada e é uma das diretrizes que norteiam essa guarda; o Direito do Consumidor é outra, que tem a garantia do é que seu como privativo, e a própria Constituição do Brasil, que garante que tem o direito privativo, tanto que não pode ser divulgado nem para parente seu se não for por uma ordem*

legal. (Entrevistada 4)

Na realidade, eu trabalhei há algum tempo, uns 30 anos de hospital particular. Eu acho que a rotina nunca mudou em relação à proteção de dados. A coisa funcionava em termos de prontuário. Naquela época era em papel mesmo que você fazia o prontuário. Mas acho que nunca houve nenhuma diferença em relação a isso. (Entrevistado 1)

A meu ver, de uma forma geral, os médicos têm uma consciência muito clara em relação à coisa do sigilo médico. Acho que é uma cultura que existe e a meu ver isso não impactou muito as coisas não. (Entrevistado 1)

Essa Lei de proteção de dados só veio respaldar os procedimentos já realizados. Não vi impactar em nada. (Entrevistado 1)

A gente quando iniciou o processo aqui, vou ser muito sincero, existia uma certa descrença. Porque, toda lei nova que muda demais uma organização, assim como foi o Código de Defesa do Consumidor, era aquela coisa: isso vai pegar ou não vai? Era aquela famosa lei que pega ou que não pega. E a gente viu que, assim como o Código do Consumidor, assim, uma coisa que já foi incutida na nossa realidade como empresa (...) a LGPD, a meu ver, tem um condão, um alcance muito parecido. Diante disso, ela teve como primeira reação da liderança o questionamento: "Mas vai pegar? É isso mesmo? Essas multas que vocês estão dizendo são muito altas? Etc". (Entrevistado 2)

Apesar desta constatação do grupo, foi enfatizado por dois entrevistados, que a LGPD apenas teria trazido mais burocracia para um processo que funcionava adequadamente com as Lei e os Normativos esparsos e um deles

relatou que compreende maior aplicabilidade da Lei aos Hospitais, descartando os Consultórios Médicos de menor porte, o que fortalece o discurso de resistência aferido na pesquisa de Oliveira e Lopes (2018), conforme descrito no item 2.3.2 da presente pesquisa e evidenciado no trecho da entrevista abaixo transcrito (respondido após a entrevistadora questionar se achava o programa da LGPD eficiente):

> *Mais ou menos. Porque eu acho que muitas coisas, igual a processo de certificação. Tenho o maior respeito pela ISO, por todos os processos de certificação. Porque eu que acho que uma coisa é o objetivo maior e outra coisa é a prática do dia a dia. Então, assim, exemplo claro sobre isso: como é que eu não vou chamar o cliente pelo nome? Vou chamar ele pelo que? Ah, não pode expor os dados do cliente... Então, o que que eu faço? Você quer ser chamado como? Outra questão: o prontuário do paciente é sigiloso. Ok, sempre foi. Mas veja, às vezes, é muito comum que um médico compartilhe com outro para tirar uma dúvida. Fica entre eles. Termos assinados e tal. Mas como é que você garante que esse cara não vai sair e falar? (...) Como é que eu asseguro isso? É um livre arbítrio. A pessoa pode chegar em casa e falar de você, né?! E aí?!*
>
> *Então, eu acho que essa multa que eles ofereceram: "Ah, eu vou multar a empresa em não sei quantos por centos do faturamento" isso é uma coisa bizarra, porque têm coisas que saem do controle da gente. Não existe um ambiente 100% controlado.*
>
> *Eu acho interessante o objetivo, eu acho que tem que ter, mas fazendo analogia com as certificações, onde os caras exigem não sei quantos indicadores, mas, na prática, você usa? Então por que você tem aquele indicador? É para você fazer correndo antes de o auditor chegar para dizer que você tem?*
>
> *Isso atrapalha o gestor ao invés de ajudar. (Entrevistada 3)*

> *A Lei de proteção de dados só veio a respaldar. Veio só dar mais um respaldo. Nada mais que isso. Eu acho que ela não impactou a vida dos médicos. Uma coisa é a nível de empresa, que tem outros interesses; quer omitir determinados dados, qualquer coisa assim. Mas a nível de médico, eu acho que ela não impactou. (Entrevistado 1)*

Do mesmo modo, os diferentes processos identificados, inclusive no seio das Redes Hospitalares (onde há Organizações com portes diversos), corroboram o que já havia sido salientado por Kooistra (2018), pelo qual o processo de adequação das grandes e das pequenas Organizações de Saúde se daria de forma diferente, mas com as técnicas que melhor se adaptavam à sua cultura e realidade, visto que os recursos disponíveis também são diferentes.

Ao ser questionado sobre o processo de formalização nas unidades que compõem a Rede Hospitalar, um dos entrevistados narrou que:

> *Deu muito trabalho. Uma empresa com 40 mil funcionários, com o volume que tem. Atuação em seis estados e no DF, quer dizer, isso para Care Delivery. Pensando em Operadora, é o Brasil todo. A gente tinha muita coisa pra fazer. Então deu trabalho porque onde a gente encontrou um pouco mais de resistência, a gente teve que ir escalando para implementar todas essas mudanças. (...) fato de estar numa empresa americana, isso ajudou. (Entrevistado 2)*

Já em relação à Organização Social, em razão das peculiaridades de suas características, a entrevistada 4 narrou que o processo de formalização "*está sendo implementado a partir dos resultados de uma consultoria de Compliance*".

Ao ser questionada se considera o Programa LGPD efetivo, a entrevistada 5 relatou que:

> *Sim, apesar de ainda estar em implementação. Pois, além de atender à legislação, se efetiva como importante*

> *ferramenta de proteção ao colaborador/instituição e cliente. (Entrevistada 5)*

Embora tenha sido identificada uma desconfiança da liderança em relação à aprovação da LGPD que, por consequência, evidencia uma resistência à Norma Geral, quatro, dos cinco entrevistados, implementaram um programa formal e documentado de proteção de dados com fundamento na LGPD, conduzido por uma liderança engajada. Porém, até o final do ano de 2022, apenas um havia concluído integralmente as etapas do processo de adequação em todas as unidades.

Não obstante a lentidão nos processos de formalização analisados, verifica-se que as duas grandes Redes Hospitalares possuem maior grau de adequação à LGPD[37], sobretudo em relação aos mecanismos administrativos e tecnológicos de proteção de dados.

Ao se questionar se, após a LGPD, teve alguma mudança administrativa ou tecnológica, um entrevistado respondeu que:

> *Teve por conta da necessidade de proteção maior dos dados que nós temos armazenados, para eventuais ataques cibernéticos etc. Além disso, para estarmos mais seguros, deixarmos nossos clientes também seguros. A gente também implementou muitas mudanças envolvendo anonimização, criptografia e mascaramento de dados. (Entrevistado 2)*

> *A gente conseguiu separar ambiente de trabalho do ambiente de estudo. (Entrevistado 2)*

> *Como nossa empresa guarda muito dado em nuvem, a gente revisou quem eram os nossos parceiros; a gente distratou alguns contratos; assinou outros contratos, inclusive com cláusulas de privacidade específicas, até*

[37] Enquanto uma delas já finalizou o processo de adequação, esforçando-se apenas para sua manutenção, a outra já havia concluído 80%

> *para preservar financeiramente se houver qualquer tipo de problema. (Entrevistado 2)*

Enquanto isso, a menor unidade, o Consultório Médico, sequer deu indícios de que pretende implementar a Lei Geral, visto que já atua no modelo atual desde momento anterior à publicação da LGPD, conforme trecho extraído da sua entrevista, o que se assemelha ao resultado obtido pela análise de Oliveira e Lopes (2018) na tabela 25, item "não pensavam em implementar o GDPR".

> *Só trabalho dessa forma, desde março de 2016. (Entrevistado 1)*

Neste sentido, há elementos que evidenciam que Organizações de maior porte e com o perfil empreendedor são capazes de responder mais rapidamente às pressões externas e a desembolsar mais recursos financeiros para estarem em *compliance*.

Dentre as Organizações com Programa LGPD, uma realizou a divulgação do Programa e/ou de suas recomendações apenas para os empregados e, semelhante ao resultado da pesquisa de Kooistra (2018), quase que a totalidade demonstrou compromisso com a capacitação interna, de modo que investem em treinamentos desde o momento da contratação e realizam manutenção periódica do conhecimento, de modo a garantir que os empregados observarão a LGPD como parte de sua rotina de trabalho e como garantidora do respeito à sua vida privada no ambiente profissional, ainda que em Organizações de Saúde pautadas em Culturas Organizacionais consolidadas em modelo de comando e controle.

> *O que mudou neste sentido, a partir da Lei, foi uma disseminação do próprio conteúdo da Lei, num formato obrigatório, em caráter de treinamento, para 100% da Instituição. (Entrevistada 4)*

> *Então, o que por vezes poderia parecer restrito ao âmbito de quem lidasse diretamente com uma série de informações do paciente, em especial as informações escritas e muito*

> *em especial as informações de prontuários, se estendeu para todo tipo de informação, para uma maior preocupação com informações desde a porta de entrada, desde o momento de admissão do paciente na recepção. (Entrevistada 4)*
>
> *Nós temos grupos de estudos. Nós promovemos encontros de debates envolvendo privacidade. Em toda a Companhia, sem restrição de cargo, tempo de cargo etc. (Entrevistado 2)*

Destoa desse direcionamento de capacitação apenas a Organização que não pretende se formalizar, visto que seus empregados não receberam treinamento específico em relação à Norma Geral. Ao ser questionado se as funcionárias compreendiam o processo de sigilo; a necessidade de proteção de dados e a existência da Lei, o entrevistado relatou o seguinte:

> *Olha, nem sei te dizer se elas sabem... provavelmente não sabem dessa história de Lei de proteção de dados. Eu acho que elas não conhecem a legislação. Mas elas entendem que estão lidando com alguma coisa muito séria, que tem que ter atenção. Até pelo nível delas... eu vejo na prática diária delas que elas entendem que estão lidando com alguma coisa muito séria, com pessoas. (Entrevistado 1)*
>
> *A gente nunca soube que era necessário fazer alguma coisa em relação às Secretárias. (Entrevistado 1)*

Em relação ao gerenciamento, dos quatro gestores que implementaram um programa formal da LGPD, três nomearam um encarregado de proteção de dados (DPO), contrastando, em termos percentuais, com o baixo volume aferido na pesquisa do CGI/NIC.br (tabela 22). Porém, chama a atenção o fato de que todos esses profissionais, inclusive os das grandes Redes Hospitalares, desempenham dupla jornada, diferentemente do resultado da pesquisa de Kooistra (2018), pela qual verifica-se que os grandes Hospitais da Holanda tinham seus DPOs em

função de tempo integral.

Embora tenha se observado o acúmulo de funções dos DPOs, durante as entrevistas, foi possível constatar que não há impacto negativo no exercício da função, visto que todos esses profissionais recebem suporte de diversas áreas internas, sobretudo da Tecnologia da Informação, o que contribui para a aplicação prática da Lei, inclusive com a utilização de *framework.*

Chama a atenção, ainda, que nas grandes Redes Hospitalares entrevistadas o DPO está alocado no Departamento Jurídico, embora uma delas tenha o processo de adequação sido gerenciado pela Diretoria de Operações, diferentemente do que ocorre nas demais, que concentram seus processos de proteção de dados nas áreas de Tecnologia da Informação e Recursos Humanos.

No que tange à base legal do tratamento de dados, dos quatro gestores que implementaram Programa LGPD, três realizaram mapeamento dos dados de pacientes tratados para adequação à base legal correspondente. Ocorre que, durante as entrevistas, foi possível perceber que a base do consentimento é utilizada de maneira mais presente nas relações com os próprios empregados, sendo pouco utilizada na relação com os pacientes, visto que, segundo o DPO de uma das Redes Hospitalares, seria um limitador do cumprimento da missão da Organização de Saúde, já que pode ser revogado total ou parcialmente a qualquer momento. Conforme descrito no trecho da entrevista abaixo reproduzida:

> *A base legal que a gente utiliza é a execução do contrato, porque, se eu tivesse que lidar com consentimento, eu tava na roça. A gente sabe que o consentimento pode ser revogado, total ou parcialmente, a qualquer momento etc e tal. Como é que eu iria conseguir cumprir minha missão, seja como hospital, seja como operadora, se eu tivesse que gerenciar consentimento desse universo todo. Então, nós entendemos que nossa base legal é a execução do contrato. (Entrevistado 2)*

Constatou-se, então, que as bases de dados “Contratos”; “Obrigação Legal” e “Tutela da Saúde” são priorizadas.

Em relação aos direitos dos titulares dos dados, em todas as Organizações

de Saúde entrevistadas com processo de adequação formalizado, os Programas de LGPD contemplam, por exemplo, a adequação das informações incompletas, inexatas ou desatualizadas, o que pode ser feito por qualquer canal de comunicação, visto que não há um canal exclusivo para esse fim.

Já em relação à forma de manutenção das informações clínicas e cadastrais nos prontuários dos pacientes, dois gestores entrevistados relatam que suas Organizações utilizam apenas sistema eletrônico e três fazem o controle das informações de forma híbrida (eletrônico e físico), o que está proporcionalmente adequado ao volume das Organizações entrevistadas pelo CGI/NIC.br (tabela 17).

Em relação à Cultura de Proteção de Dados nas Organizações de Saúde, quanto à segurança da informação, todas as Organizações que implementaram um Programa formal incluíram, por exemplo, ferramentas como assinatura eletrônica; e-mails criptografados e proteção por senha, corroborando com o resultado da pesquisa do CGI/NIC.br (tabela 21). Todavia, apenas uma das Redes Hospitalares utiliza, a partir dos preceitos da LGPD e em relação à base de dados sensíveis, tecnologia para tornar dados armazenados anonimizados.

Todavia, embora tenham sido implementadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais por todas as Organizações entrevistadas, durante uma das entrevistas foi relatada a ocorrência de episódio que evidencia suspeita de vazamento de dados, após o início de implantação do Programa LGPD, consoante trecho da entrevista abaixo.

> *Nós tivemos uma situação específica, que está em análise, que envolve um profissional médico que fez a impressão de um prontuário, que ele tinha atribuição para fazer, pelo cargo que ele exercia, e esse prontuário acabou sendo utilizado num determinado processo judicial. Isso geral a necessidade de a gente entender que tipo de falha houve e etc. (...) houve até a mudança da governança na época. (...) diante desse flow todo errado, a gente mudou algumas coisas. Foi bem no começo na LGPD. Mas, pra mim, foi uma falha. (Entrevistado 2)*

Entretanto, não há registro de aplicação de sanção pela ANPD e/ou de

ação judicial movida por descumprimento às regras da LGPD.

Episódios de vazamento, como o identificado em uma das entrevistadas, fortalecem o discurso de estudiosos que sustentam que, não obstante a edição de Leis específicas de proteção de dados e os investimentos em segurança da informação, ainda não é possível eliminar os riscos em sua integralidade e as empresas da área de saúde permanecem na iminência de invasão à vida privada e vazamento de dados, bem como corrobora o estudo da Varonis que aponta que as Organizações de Saúde ainda estão distantes do modelo ideal de segurança dos dados.

Cumpre registrar que, durante a entrevista na qual foi relatado episódio de vazamento de dados, ficou evidente que a falha decorreu de ação humana e transpareceu uma falta de comprometimento com a cultura de proteção de dados da Organização.

Diante da gravidade do fato e de modo a evitar novas ocorrências, necessário é reavaliar os mecanismos de processamento de dados adotados, bem como verificar se os procedimentos criados estão alinhados à Cultura Organizacional e se esta foi compreendida pelos empregados.

De toda sorte, ao que parece, as Organizações estão alinhando a gestão de informações com as práticas trabalhistas, conforme se verifica no trecho da entrevista abaixo:

> *Como alguns treinamentos são mandatórios pra toda a Companhia, sobre esses existe um controle acerca disso, exemplo: lista a, b, c ainda não fez o tratamento. É necessário fazer e tal. Uma eventual falha na forma de tratar dados, sim, ela é passível de punição. Isso consta no contrato de trabalho e já tivemos situação de punição disciplinar baseada na CLT por conta disso na empresa. (...) Eu já tive desligamento por justa causa por conta disso. (Entrevistado 2)*

No que tange aos valores, conclui-se que a cultura de proteção de dados das Organizações de Saúde entrevistadas não inclui a preocupação com artefatos visíveis, sobretudo nas áreas com predominância da atividade-fim, como os

espaços de circulação de pacientes, tampouco se valem de jargões corporativos na fixação da identidade cultural.

O trecho da entrevista a seguir descrito evidencia o impacto da ausência de artefatos que identifiquem a adequação da Cultura Organizacional à LGPD, o que fragiliza a transparência na relação com os pacientes.

> *Então eu vejo assim... para o paciente. O paciente nem sabe o que é LGPD. Mas ele sentiu um pouco uma estranheza: "Não... mas porque não tem mais o meu CPF? Como é que vão saber quem eu sou?" A gente teve até questões relacionadas a isso. (Entrevistada 3)*

> *Pro paciente a gente não teve muita mudança... mas para o colaborador, muitas. A gente aqui compartilhava senha com os colaboradores e hoje em dia não pode mais porque agora os acessos são rastreados. (Entrevistada 3)*

> *Não como recado que o público capte dessa forma. E aí acho mais difícil que ele perceba isso no que vira essa prática, mas que ele não capta como. Como, por exemplo, se existem TV's até em postos que sejam da assistência, postos de enfermagem, por exemplo, eles nunca têm nenhuma informação de paciente, então nunca tem a identificação, né? Então, se você passar, você não saberá quem está em nenhum dos leitos que estão ali. Você não vai reconhecê-los nominalmente. Mas isso não é algo que seja talvez capturado prontamente por um cliente, né? É algo que faz parte dessa regulação e dessa atenção. A prática da preservação de privacidade, sigilo. (Entrevistada 4)*

Nesse ponto, vislumbra-se semelhança ao discurso colhido por em sua pesquisa, sobretudo em relação ao entrevistado que afirmou que as técnicas de conscientização do GDPR, por meio de jornal da equipe e da intranet, não funcionavam, já que a equipe de atendimento não lia os comunicados pois estava

ocupada com o cuidado com pacientes, diferentemente da equipe que trabalha nos escritórios, conforme trecho da entrevista abaixo reproduzido extraído do texto original de Kooistra (2018):

> *"Care staff in particular do not read it, they are busy with care. Office staff deals with it differently. They sit down, take a cup of coffee and take their time to read it. That is not possible in care. I have to look at it rather differently. And that is, tell, tell, tell. Inviting yourself to department meetings and talk. Very simple." (Kooistra, 2018. p. 31)*

Outro fator relevante que, embora não tenha equivalência nas demais pesquisas identificadas como base para o presente trabalho, corresponde ao fato de que as Organizações com perfil de empresa familiar e/ou com forte apego à figura pessoal do fundador, três das cinco Organizações entrevistadas, relataram maior ausência de processos formais ou maior resistência à inserção da cultura de proteção de dados antes da contratação de gestores externos ou da fusão com empresa estrangeira, conforme se afere no trecho da entrevista transcrito a seguir:

> *Assim como toda boa empresa familiar, os quatro donos se dividiam aqui na gestão e não tinham processos formais estabelecidos... o que tinha era em pouquíssimas áreas. É lógico que a assistencial, como todos são médicos, era a que mais se aproximava de uma formalização, justamente pela necessidade intrínseca da operação. Por exemplo, os prontuários aqui eram ainda prontuários em papel, né?! Mas sempre se teve muita preocupação com o sigilo das informações. (Entrevistada 3)*

> *Pelo fato de a gente ter um controlador americano, o americano é meio neurótico com essa questão de estar 100% em compliance (que bom que é assim), não teve isso de a lei pega ou não pega. Ele disse: Vamos! A gente teve uma influência da nossa matriz controladora. (Entrevistado*

2)

Destaca-se, ainda, que, durante as entrevistas, foram relatados discursos de uma Cultura Organizacional forte, com valores claros, o que ajudaria no processo de motivação e retenção de pessoal. Em razão disso, parte dos entrevistados sentiu segurança para afirmar que o grau de identificação e lealdade dos empregados à Organização é elevado, o que contribuiria para o fortalecimento da imagem e quase que a totalidade afirmou que os empregados se sentiam numa "grande família" dentro da Organização, consoante exaltaram os entrevistados nos trechos das entrevistas abaixo transcritas.

> *Numa empresa com 40 mil funcionários, você ter, em números reais, 86% de treinamento realizado é um índice muito alto de treinamento de privacidade não mandatório realizado. Se não houvesse engajamento do time, porque eu iria ter um engajamento tão alto em um treinamento não mandatório, entende?*
>
> *Olhando sob o aspecto de privacidade, eu entendo que sim. Tem um outra coisa, também, que é essa questão da integridade, que é muito dia a dia nosso. Então, jogar o jogo certo, seguir a regra correta, é muito importante, nem que seja pela preocupação de não cometer uma ato falho, de não cometer um erro honesto, como se diz. Eu sinto o engajamento sim, de não fazer o errado, de fazer o certo. (Entrevistado 2)*
>
> *Eles adoram trabalhar aqui. Se sentem acolhidos. Eles têm amor pela empresa. Eu tenho uma rotatividade muito baixa. Eu tenho pessoas que estão aqui há muito tempo. Se você olha o tempo de casa, tem um grupo muito grande com mais de 10 anos. Eu tenho um perfil de gente mais jovem na entrada, no acesso, no atendimento e esse tem uma rotatividade um pouquinho maior, embora eles*

> *acabem ficando mesmo. Esse ano a gente fez um monte de campanha para eles estudarem. Paguei curso de Excel, fiz cinco turmas de Excel. Então, assim, eles gostam da casa. Eles têm satisfação em estar aqui. Eles reconhecem o esforço da Organização em ajudá-los. Eu sinto o clima daqui muito bom. (Entrevistada 3)*

> *Nesse aspecto, a proposta é que ele se aproxime e faça uma interligação positiva, de uma extensão de sua vida. Não sendo o "esse aqui é meu tempo do sofrimento e depois eu tenho a minha vida". Existem muitas práticas que têm a proposta de inclusão. (Entrevistada 4)*

> *Percebo que os funcionários se sentem integrando uma grande família sim... muito disso vem do próprio direcionamento do negócio que, tem muito o foco em preservar a privacidade, o sigilo... mas também tem grande preocupação com o respeito aos funcionários e preza pela liberdade de expressão. (Entrevistada 5)*

Sobressai, também, dentro dessa relatada Cultura Organizacional supostamente forte, que a LGPD não impactou o tipo de perfil necessário para que um empregado tivesse uma carreira meteórica, visto que, todos os entrevistados afirmaram que o perfil profissional seria avaliado pelas características do cargo, de acordo com os valores já existentes na Organização, tanto pela ótica técnica quanto comportamental.

Inclusive, chamou a atenção um dos relatos que afirmou ser o cumprimento de leis, o que incluiria a LGPD, sem exclusividade, um dos pilares do valor "integridade", que já integrava o rol de cinco valores atrelados à Cultura Organizacional daquela Organização de Saúde, consoante trecho da entrevista destacado abaixo:

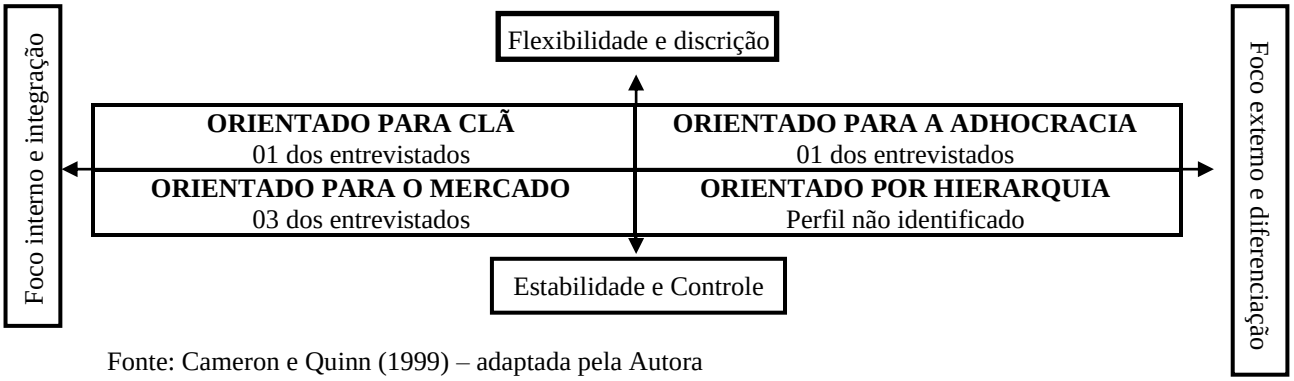
> *A gente tem cinco valores na empresa[38]. O primeiro deles é a integridade. Integridade tem várias facetas. Mas o cumprimento do que é lei, o cumprimento do que é certo talvez seja um bom resumo disso. Então, sendo um dos cinco valores, o primeiro dos valores, cumprir lei, ser íntegro nesse sentido, ele é condição sine qua non, para se fazer qualquer carreira aqui dentro. (Entrevistado 2)*

A relação entre a internalização de valores organizacionais (valores *'taken for granted'*, Schein,1991) e a prática das normas de LGPD, é importante, e está amplamente discutida na literatura organizacional. (Fleury,1986; Quinn & Rohrbaugh, 1983).

Embora se classifiquem como Organizações com cultura forte, pouco mais da metade dos entrevistados acredita que existem comportamentos e práticas na Organização que devem ser mudados, seja pela necessidade de investimento em inovação, para que se mantenha competitiva no mercado, ou seja pelo fato de compreender que os processos são vivos e precisam ser revisitados a todo tempo. Todavia, não foi possível identificar nenhuma fala que vinculasse eventual necessidade de mudança às questões trazidas pela LGPD.

Embora os entrevistados tivessem tido a liberdade para descrever a Cultura Organizacional de suas Organizações de Saúde, uma das dimensões da pesquisa semiestrutura buscou compreender as suas características por meio da análise da tipologia cultural Quinn & Rohrbaugh (1983) e foram identificados três tipos de cultura:

Figura 4 – Perfis da Cultura Organizacional das Organizações de Saúde entrevistadas



Fonte: Cameron e Quinn (1999) – adaptada pela Autora

[38] Integridade, relacionamento, compaixão, inovação e performance.

Verifica-se, portanto, que três dos cinco gestores entrevistados tiveram suas Organizações classificadas no perfil orientado para o Mercado ou Objetivos, ou seja, inseridas no modelo dos objetivos racionais; orientadas para realização do trabalho e para o controle, como se verifica nos trechos extraídos das entrevistas e abaixo colacionados:

> *Olha, a prática da empresa é de aproximação e participação. Ela vem trabalhando muito esse aspecto da valorização da cultura e traz alguns tópicos que são relacionados a isso, a convidar a participação, o máximo de pessoas para as tomadas de decisões ou para contribuições que possam levar à tomada de decisão do âmbito da matriz de responsabilidade. Existe ainda uma hierarquização...ela tem mais uma um desenho cartesiano do que grau 360. Mas é muito característico das instituições de saúde, porque você, de fato, tem algumas posições que se conservam para o modelo de gestão se concretizar, ter a performance e avaliar o negócio como um todo. Então tem as instâncias de uma matriz de responsabilidade, dos organogramas. Mas, especificamente na que eu trabalho, existe um convite à participação em fóruns específicos de todos os níveis da organização. (Entrevistada 4)*

> *Junto da nossa certificação, em 2019, muito impulsionado por essa profissionalização de gestão, a gente tá implantando como se fosse um ERP. (...) é um sistema da área de saúde. Os grandes hospitais (...) já trabalham (...). Então, assim, o que vai acontecer quando a gente acabar a implantação desse sistema, que a gente está planejando agora para esse ano, a gente não vai ter mais papel. Então a gente vai ter prontuário eletrônico, tudo dentro desse sistema que vai mapear desde a entrada do paciente no acesso até chegar em mim, o faturamento, recebimento, contabilidade. Então, a ideia é que esse caminho seja todo sistêmico, que hoje não é, hoje é uma colcha de retalho. (Entrevistada 3)*

> *Nós somos prestadores de serviços públicos, por meio de contrato*

de gestão e toda nossa atuação é guiada pelo que prevê o contrato. Percebemos que a Organização tem um foco importante nas pessoas e valoriza os perfis agregadores, já que esse é o perfil que entendemos que melhor integra o grupo e dá mais tranquilidade para a gestão.

Temos contratos com o Poder Público para gerenciar algumas unidades de saúde, precisamos agregar os grupos internos para não correrm os risco de impactar esses contratos. (Entrevistada 5)

Esse perfil tem como principais características a estabilidade, a produtividade, a competitividade, a eficiência, o planejamento e uma liderança diretiva, orientada para o alcance das metas, dando robustez ao que diz Mandal, 2017 em relação ao fundamento de que hospitais com cultura racional se adaptam à mudança, principalmente para ficar à frente de concorrentes e para evitar interrupções na cadeia de suprimentos.

Continuamente, verifica-se que um dos gestores entrevistados teve sua Organização classificada no perfil orientado para o Clã ou Apoio, enquadrada no modelo das relações humanas, com ênfase na flexibilidade e no lado interno da Organização. Uma de suas importantes características é o fomento do trabalho em equipe e uma liderança que deve reforçar a participação e o envolvimento das pessoas, conforme se vê no trecho extraído da entrevista:

São vários consultórios, mas cada um tem seu programa. Eu não compartilho dados com as pessoas do consultório. Cada um tem o seu provedor. Nós não trabalhamos com a mesma empresa. Os meus dados não são compartilhados. Até a nível de secretária, elas também não têm acesso. Elas só acompanham minha agenda de pacientes do dia, do mês, da semana. Mas elas não têm acesso a nada.

(...)

São três secretárias.

(...)

Elas sabem que não, quando alguém pergunta alguma coisa sobre um paciente, elas falam que não sabem e não podem informar. Isso

é bem transparente, é bem claro. (Entrevistado 1)

Destaca-se que se classificou como Organização de Cultura Clã o Consultório Médico que não se adequou e não pretende se adequar às regras estabelecidas pela LGPD, por entender que os normativos já existentes seriam suficientes. Neste sentido, o fundamento de focar em um modelo altamente flexível com foco majoritariamente interno parece coerente com o posicionamento adotado, além de corroborar os argumentos de Jacobs et al., 2013; Shortell et al., 1995 pelos quais essa Cultura está relacionada a unidades pequenas (com pequeno número de leitos).

Ter quatro das cinco Organizações classificadas com perfil com foco no campo interno, Mercado e Clã, justifica, ainda, o resultado da pesquisa relacionada ao uso do nome social por pacientes. Isso porque, embora haja legislação específica que preveja a possibilidade do uso do nome social por pessoa travesti ou transexual, quatro, dos cinco gestores entrevistados, relataram que suas Organizações de Saúde possuem procedimentos rígidos vinculados à apresentação de documento de identificação oficial, o que pode fragilizar o direito da personalidade dessas pessoas, bem como utilizar de maneira inadequada dados sensíveis, tais como os relativos à vida sexual e os aspectos genéticos relacionados ao transexualismo.

Continuamente, verificou-se que um dos gestores entrevistados tem sua Organização com um perfil orientado para a Adhocracia, onde as pessoas correm riscos, valorizam a inovação e o empreendedorismo, bem como buscam uma posição competitiva no sistema global. Dentre suas principais características estão o crescimento e a aquisição de recursos, volume de negócios e um líder que deve reforçar a capacidade de desenvolver uma visão estratégica, assim como facilitar a aquisição de recursos, conforme destaque do trecho da entrevista:

> *Toda empresa está concorrendo no mercado, fora um ou outro monopólio que exista, está concorrendo no mercado. E a gente precisa entender que a gente precisa de inovação, que é um outro valor da empresa (...) toda empresa precisa inovar. Só que a gente tem que jogar o jogo dentro das quatro linhas, junto com a regra debaixo*

> *do braço. Não adianta eu dizer assim: "ah, eu vou vender plano de saúde para um determinado grupo, cliente x, ele tem cinco mil vidas e é um excelente contrato... se, na verdade, esse grupo está querendo uma série de informações dos beneficiários que, pela lei, não devo compartilhar. Isso não é uma coisa da Organização que eu trabalho, é uma coisa do mercado.*
>
> *A gente quer competir no mercado... um mercado justo, que segue as leis e as lideranças do mercado e as nossas devem estar conscientes de que a gente deve inovar. Mas deve inovar dentro daquele retângulo, aquele campo demarcado do que a gente pode ou não pode fazer.*
>
> *Eles têm que ter inovação para criar e eu também tenho que ter inovação, eu, eu, meu time, pra dar solução pra eles do que a gente pode fazer. Porque simplesmente dizer não, não vai funcionar.*
>
> *Essa é uma cultura que a gente vê muito. Antes da LGPD eu acho que existia uma fragilidade na forma de transferências pontuais de dados e etc e isso é uma coisa que mudou o mercado.*
>
> *(Entrevistado 2)*

Novamente, o perfil dos entrevistados mostrou-se coerente com a orientação de sua Cultura, uma vez que contempla Organização que buscou expansão para o mercado internacional; tem a inovação como um de seus valores e busca se manter competitiva no mercado nacional com a aquisição contínua de novos negócios de saúde e, ainda, fortalece a tese de Kooistra (2018), pela qual os hospitais empreendedores mudam para serem inovadores.

A partir dessa análise, é possível responder à questão central da presente pesquisa:

"Qual o papel da Cultura Organizacional no processo de adaptação das Organizações de Saúde brasileiras à LGPD?"

Diante de tantas evidências, foi possível verificar que a Cultura Organizacional das Organizações de Saúde foi uma facilitadora do processo de

adequação ao regramento da LGPD, visto que, antes mesmo do início dos debates acerca da nova lei, já eram implementadas regras mínimas de segurança da informação, sigilo e ética, com fundamento em legislação esparsa, sobretudo a CRFB, o Código Civil, o CDC e o Código de Ética Médica.

Ocorre que a LGPD, embora transpareça para algumas Organizações como apenas um limitador burocrático, consolidou suas recomendações em um único documento legal e, em sua menor atuação, pode servir para facilitar a consulta por quem ainda tem dúvida de como é possível tratar dados pessoais.

Do mesmo modo, não obstante os entrevistados sustentarem suas Culturas como fortes, pequenos detalhes expostos nos depoimentos levam a crer que, mesmo que seja realmente forte, a Cultura Organizacional de Saúde ainda apresenta brechas que podem ser fatais e ações, despertadas a partir da LGPD, que parecem pequenas, como excluir o número do CPF do paciente da etiqueta exposta e adesivada na roupa; troca periódica de senha; substituição dos prontuários de papel por eletrônicos; anonimização de dados e investimento em ferramentas de segurança, mostram-se essenciais para a sobrevivência do negócio.

5 Conclusão

Não obstante severas resistências, o mundo corporativo está mudando e passou a reconhecer que ter a adequação à LGPD como parte da Cultura Organizacional significava ter mais chance de sobreviver em um cenário altamente competitivo.

Com o passar dos anos, considerável parte da privacidade humana desapareceu. Porém, nas últimas décadas, novas ameaças passaram a assombrá-la, na medida em que a tecnologia ficou mais acessível, permitindo, inclusive, a prática remota de atividades que, até então, eram realizadas apenas de modo off-line, como a telemedicina, obrigando a disponibilização de dados pessoais desmedidamente e com os olhos vendados pelo desconhecimento das políticas de tratamento das informações.

É evidente que as tomadas de decisão do mundo presente impactarão as gerações futuras, sobretudo no que tange ao avanço da medicina e ao estabelecimento de políticas públicas para a saúde. Neste sentido, como o que estão em jogo é a vida privada e a intimidade dos indivíduos, protegidos como direitos primários e fundamentais, seus titulares devem ter clareza acerca de como estão sendo tratados seus dados, bem como devem ser capazes de ditar as regras, de direcionar o modo como o tratamento de suas informações se dará pelos detentores, e, ainda, devem autorizar (ou não) a sua disponibilização a quem, onde e por quanto tempo quiserem.

Porém, o controle de suas próprias vidas pelos titulares dos dados somente será possível com medidas efetivas de segurança da informação e de monitoramento do cumprimento dos ditames estabelecidos por uma Lei Geral, como o GDPR e a LGPD.

Episódios recorrentes de vazamento de dados precisam ser observados com a devida e máxima cautela, de modo que não seja a mera adoção de barreiras tecnológicas tida por suficiente. Isso porque, boa parte das falhas na segurança, inclusive o registro identificado em Organização de Saúde entrevistada, resulta de ação humana, o que tem impacto direto na Cultura Organizacional que deve, constantemente, reafirmar seus valores e ideologias aos empregados.

Além disso, o processo de adequação da Cultura Organizacional das

Organizações de Saúde à LGPD deve equalizar a rigidez normativa com o avanço tecnológico e social, de modo a não estabilizar novos modelos de negócios; possibilitar a construção de mecanismos de desburocratização e ascensão de processos de atendimento e estar em *compliance*, por exemplo, com normativos complementares, como o relativo ao uso do nome social, sempre cuidando para gerar confiança necessária ao titular dos dados e garantir o respeito ao princípio da dignidade da pessoa humana.

Por considerar que a LGPD determina que sejam utilizadas 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 e difusão desses dados; e por vislumbrar uma Cultura Organizacional frágil das Organizações de Saúde, embora o universo pesquisado a considere uma cultura forte, recomenda-se, como uma proposta para trabalho futuro, analisar, mais especificamente, o núcleo das pequenas Organizações de Saúde, como Consultórios Médicos, de modo a permitir melhor compreensão acerca da resistência à adesão à Regra Geral, instituída por Lei, para tratamento de dados pessoais.

No mesmo sentido, propõe-se análise mais direcionada aos riscos reais de vazamento de dados, a fim de contribuir com as Organizações de Saúde na identificação dos obstáculos à integralidade dos arquivos médicos.

Por fim, cogita-se como tópico relevante para pesquisa futura a identificação das razões que levam empresas familiares e/ou com forte apego à figura pessoal do fundador a apresentarem resistência aos processos formais de adequação à LGPD.

6 Referências Bibliográficas

TOMEI, Patricia Amelia. O que é Cultura Organizacional / Raquel Rolnik. São Paulo: Brasiliense, 2012. (Coleção Primeiros Passos)

MALDONADO, Viviane Nóbrega et al., Comentário ao GDPR [livro eletrônico]: Regulamento Geral de Proteção de Dados da União Europeia. 2. ed. São Paulo: Editora Thomson Reuters Brasil, 2020

CUNHA, Daniel Alves da; HIERRO, Ana e SILVA, Diogo Rodrigues. Guia de Processo de Adequação ao Regulamento Geral de Proteção de Dados. Coimbra: Editora Almedina, 2020

TOSCANO, Manuel Castilleja, GDPR – LOPDGDD Sistema de Cumplimiento de la normativa de privacidad, 1. ed. Edita Privacy Driver

PEREIRA, Gustavo Nojosa, O Direito Fundamental à Privacidade nos Meios Digitais. Editora: Gustavo Nojosa Pereira. 05 de junho de 2021

ZANINI, Leonardo Estevam de Assis. O surgimento e o desenvolvimento do right of privacy nos Estados Unidos. Revista de Doutrina TRF4. 2015. Disponível em https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao064/Leonardo_Zanini.html. Acessado em 28.06.2022

WARREN, Samuel D. e BRANDEIS, Louis D. “The Right to Privacy”. Harvard Law Review. Vol. IV. December 15, 1890. Nº. 5. Disponível em http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html. Acessado em 28.06.2022

KOCH, Richie. LGPD: a versão brasileira do regulamento europeu. 2019. Disponível em https://www.serpro.gov.br/lgpd/noticias/lgpd-versao-brasileira-gdpr-dados-pessoais. Acessado em 27.06.2022

https://gdpr.eu/gdpr-vs-lgpd/. Acessado em 27.06.2022

https://carnegieindia.org/2019/05/15/will-gdpr-style-data-protection-law-work-for-india-pub-79113. Acessado em 28.06.2022

Temas em Saúde Coletiva. Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde, 2015

Privacidade Hoje – Anais do I Seminário de Direito Civil da PUC-Rio no ano de 2017. Organização: Maria Celina Bodin de Moraes e Caitlin Mulholland. Middletown, DE: s.n., 2018

GRISWOLD v. CONNECTICUT, 381 US 479 (1965). Disponível em: https://supreme.justia.com/cases/federal/us/381/479/. Acessado em:

29/06/2022

D'AVILA, Ana Vitória Germani, SILVA, Bruna Fabiane da e ARAUJO, Thiago Volpi de. LGPD muito além da Lei. Gvtech Soluções em Tecnologia da Informação Ltda. 2021

BARBOSA, Carla e LOPES, Dulce, na obra coletiva LGPD na Saúde. Coordenação de Analluza Bolivar Dallari e Gustavo Ferraz de Campos Monaco. 1. ed. São Paulo: Revista dos Tribunais. 2021
Nota à imprensa do Hospital Israelita Albert Einstein. Disponível em: https://www.einstein.br/sobre-einstein/imprensa/press-release/nota-a-imprensa-26112020#:~:text=%E2%80%8BO%20Hospital%20Israelita%20Albert,sistemas%20sem%20a%20prote%C3%A7%C3%A3o%20adequada. Acessado em 25.07.2022

https://www.publico.pt/2018/10/22/sociedade/noticia/hospital-barreiro-contesta-judicialmente-coima-400-mil-euros-comissao-dados-1848479. Acessado em 23.07.2022

https://research.checkpoint.com/2019/11th-november-threat-intelligence-bulletin/. Acessado em 24.07.2022

https://research.checkpoint.com/2022/10th-january-threat-intelligence-report/. Acessado em 24.07.2022

https://unit42.paloaltonetworks.com/infusion-pump-vulnerabilities/. Acessado em 25.07.2022

https://conteudo.axur.com/pt-br/relatorio-da-atividade-criminosa-online-no-brasil-2021. Acessado em 27.07.2022

VÉRIZ, Carissa. Privacidade é Poder. 1. ed. São Paulo: Editora Contracorrente. 2021

CHAZARO, Octavio F. Torres. Formando Culturas Organizacionales: El caso de clínicas y hospitales. .1 ed. Spain, 2015

Constituição do Império do Brasil de 1824, disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao24.htm

Constituição da República de 1891, disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao91.htm

Constituição da República de 1934, disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao34.htm

Constituição da República de 1937, disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao37.htm

Constituição da República de 1946, disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao46.htm

Constituição da República de 1967, disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao67.htm

Constituição da República de 1969, disponível em http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao67EMC69.htm

https://www.iso.org/about-us.html. Acessado em 27.07.2022

https://www.security.ufrj.br/noticias/senhas2021/. Acessado em 27.07.2022

PERRET, Véronique. Elliott JAQUES. De l'organisation comme moyen de lutte contre l'anxiété à la "Requisite Organization". Les grands auteurs en Management, EMS Management & Société, pp.464- 479, 2009.

CURRIE, Graeme; DINGWALL, Robert; KITCHENER, Martin e WARING, Justin. Let's dance: Organization studies, medical sociology and health policy. Social Science & Medicine 74 273 e 280. Elsevier, 2012.

SCHEIN, Edgar H, The role of the founder in creating organizational culture. Organizational Dynamics, Summer, 13–28.

SCHEIN, Edgar H, Organizational Culture and Leadership. 2. ed. San Francisco: JosseyBass, 1992.

FRITH L, Sinclair M, VEHVILÄINEN-JULKUNEN K, BEECKMAN K, LOYTVED C, LUYBEN A., Organisational culture in maternity care: a scoping review. Evidence Based Midwifery, 2014.

ROCHA FLR, Marziale MHP, Carvalho MC, Id SFC, Campos MCT, A Cultura Organizacional de um hospital público brasileiro. Rev Esc Enferm USP 2014; 48(2):308-14.

VEGRO TC, Rocha FLR, Camelo SHH, Garcia AB. Cultura Organizacional de um hospital privado. Rev Gaúcha Enferm. 2016 jun; 37(2):e49776.

NYSTROM PC. Organizational cultures, strategies, and commitments in health care organizations. Health Care Manage Rev. 1993 Winter;18(1):43-9. PMID: 8444614.

RADOLIFFE-BROWN, Alfred Reginald, 1881. Estrutura e função na sociedade primitiva; tradução de Nathanael C. Caixeiro. Petrópolis, Vozes, 1973, 272p. (Antropologia, 2).

KOOISTRA, Trijntje Jannie (Reina). Isomorphism and organizational culture: how hospitals adapt to the General Data Protection Regulation. Master's thesis MSc BA - Organizational & Management Control University of Groningen, Faculty of Economics and Business. 2018.

ARISTÓTELES, 384-322 a.C. A política / Aristóteles; introdução de Ivan Lins; tradução de Nestor Silveira Chaves. – Ed. Especial. - Rio de Janeiro: Nova Fronteira, 2011.

ROCHA, Fernanda Ludmilla Rossi Rocha; MARZIALE, Maria Helena Palucci; CARVALHO, Michele Cristina de; CARDEAL ID, Samira de Fátima; CAMPOS, Monica Chiodi Toscano de. A Cultura Organizacional de um hospital público brasileiro. Rev Esc Enferm USP. 2014; 48(2):308-14

Parlamento Europeu. https://www.europarl.europa.eu/about-parliament/pt/home. Acessado em 29.08.2022.

Tratado de Roma (1957), disponível em https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=LEGISSUM:xy0023

Lei de Hesse, Alemanha, versão 2021, disponível em https://www.rv.hessenrecht.hessen.de/bshe/document/jlr-DSIFGHEpG24.

FORTES, Paulo Antônio de Carvalho. Reflexões sobre a bioética e o consentimento esclarecido. Revista Bioética. Conselho Federal de Medicina. v. 2, n. 2. 1994.

Convenção Americana sobre Direitos Humanos (Pacto de San José da Costa Rica), disponível em http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm#:~:text=1.-,Toda%20pessoa%20tem%20o%20direito%20de%20que%20se%20respeite%20sua,dignidade%20inerente%20ao%20ser%20humano.

LEI DE PROPRIEDADE INDUSTRIAL, disponível em http://www.planalto.gov.br/ccivil_03/leis/l9279.htm.

LEI SOBRE DIREITOS AUTORAIS, disponível em http://www.planalto.gov.br/ccivil_03/leis/l9610.htm.

LEI DA INTERCEPTAÇÃO TELEFÔNICA, disponível em http://www.planalto.gov.br/ccivil_03/leis/l9296.htm.

CÓDIGO CIVIL, disponível em http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm.

CÓDIGO DE ÉTICA MÉDICA, disponível em https://portal.cfm.org.br/images/stories/biblioteca/codigo%20de%20etica%20medica.pdf.

RESOLUÇÃO CFM Nº 1.605, DE 15 DE SETEMBRO DE 2000, disponível em https://www.cremesp.org.br/library/modulos/legislacao/versao_impressao.php?id=3051.

RESOLUÇÃO CFM Nº 1.821, DE 11 DE JULHO DE 2007, disponível em https://sistemas.cfm.org.br/normas/visualizar/resolucoes/BR/2007/1821.

PROCESSO-CONSULTA CFM Nº 1.401/2002 PC/CFM/Nº 30/2002, disponível em https://sistemas.cfm.org.br/normas/visualizar/pareceres/BR/2002/30.

CÓDIGO PENAL, disponível em https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm.

LEI GERAL DAS TELECOMUNICAÇÕES, disponível em http://www.planalto.gov.br/ccivil_03/leis/l9472.htm.

LEI DO HABEAS DATA, disponível em http://www.planalto.gov.br/ccivil_03/leis/l9507.htm.

LEI DO CADASTRO POSITIVO, disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm.

LEY 19628 SOBRE PROTECCION DE LA VIDA PRIVADA, CHILE, disponível em https://www.bcn.cl/leychile/navegar?idNorma=141599&idParte=864270.

Ley 25.326 PROTEÇÃO DE DADOS PESSOAIS, ARGENTINA, disponível em https://observatoriolegislativocele.com/pt/dados-pessoais/.

LEY FEDERAL DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE LOS PARTICULARES – DOF 05/07/2010, disponível em https://dof.gob.mx/nota_detalle.php?codigo=5150631&fecha=05/07/2010#gsc.tab=0.

Ley N° 29733 - Ley de Protección de Datos Personales do Peru, disponível em https://www.gob.pe/institucion/congreso-de-la-republica/normas-legales/243470-29733.

LEY ESTATUTARIA 1581 DE 2012, COLÔMBIA, disponível em https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981.

LEY N° 18331 - LEY DE PROTECCION DE DATOS PERSONALES, URUGUAI, disponível em https://www.impo.com.uy/bases/leyes/18331-2008.

CONSOLIDAÇÃO DAS LEIS TRABALHISTAS – CLT, disponível em

http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm.

CÓDIGO DE PROCESSO PENAL, disponível em http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm.

DALLARI, Analluza Bolivar e MONACO, Gustavo Ferraz de Campos. LGPD na Saúde. Editora Revista dos Tribunais; Nova Edição. 2021.

Diferença entre Hackers, Crackers, White Hat, Black Hat, Gray Hat, entre outros. Disponível em https://egov.ufsc.br/portal/conteudo/saiba-diferen%C3%A7a-entre-hackers-crackers-white-hat-black-hat-gray-hat-entre-outros

O que é um vazamento de dados? Disponível em https://getprivacy.com.br/perguntas-respostas-lgpd-vazamento-de-dados/#:~:text=Um%20vazamento%20de%20dados%20%C3%A9,e%20usadas%20para%20fins%20diversos.

MADRUGA, Roberto. Employee Experience, Gestão de Pessoas e Cultura Organizacional. Editora Atlas. 2021

SCHEIN, Edgar H. e SCHEIN, Peter. Organizational Culture and Leadership. 5ª ed. Wiley. 2017.

LOPES, Isabel Maria e OLIVEIRA, Pedro. Aplicabilidade do Regulamento Geral de Proteção de Dados em Clínicas de Saúde. RISTI – Revista Ibérica de Sistemas e Tecnologias de Informação. 2018. p. 118-129. Disponível em: https://www.proquest.com/docview/2041141522/fulltextPDF/3B4872CF39F436CPQ/1?accountid=26649

Erasmus MC lekt mailadressen jonge hiv-patiënten. Disponível em https://www.rtlnieuws.nl/tech/artikel/4007671/erasmus-mc-lekt-mailadressen-jonge-hiv-patienten

Conceitos e Definições em Saúde. Disponível em https://bvsms.saude.gov.br/bvs/publicacoes/0117conceitos.pdf

ACAR, A. Z., & ACAR, P. (2012). The effects of organizational culture and innovativeness on business performance in healthcare industry. Procedia-Social and Behavioral Sciences.

CARLSTRÖM, E. D., & EKMAN, I. (2012). Organisational culture and change: implementing person-centred care. Journal of health organization and management.

JACOBS, R., MANNION, R., DAVIES, H. T., HARRISON, S., KONTEH, F., & WALSHE, K. (2013). The relationship between organizational culture and performance in acute hospitals. Social science & medicine.

MANDAL, S. (2017). The influence of organizational culture on healthcare supply chain resilience: moderating role of technology orientation. Journal of Business & Industrial Marketing.

QUINN, R. E., & ROHRBAUGH, J. (1983). A spatial model of effectiveness criteria: Towards a competing values approach to organizational analysis. Management science.

SHORTELL, S. M., O'BRIEN, J. L., CARMAN, J. M., FOSTER, R. W., HUGHES, E. F., BOERSTLER, H., & O'CONNOR, E. J. (1995). Assessing the impact of continuous quality improvement/total quality management: concept versus implementation. Health services research.

WAGNER, C., MANNION, R., HAMMER, A., GROENE, O., ARAH, O.A., Dersarkissian, M., & SUÑOL. (2014). The associations between organizational culture, organizational structure and quality management in European hospitals. International Journal for Quality in Health Care Advance Access.

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR PONTOS DE ACESSO AO PRONTUÁRIO ELETRÔNICO DO PACIENTE. PESQUISA 2021. Disponível em https://cetic.br/en/tics/saude/2021/estabelecimentos/B7/

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR FUNCIONALIDADES DE TROCA DE INFORMAÇÕES EM SAÚDE DISPONÍVEIS EM SISTEMA. PESQUISA 2021. Disponível em https://cetic.br/en/tics/saude/2021/estabelecimentos/B6/

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR FORMA DE MANUTENÇÃO DAS INFORMAÇÕES CLÍNICAS E CADASTRAIS NOS PRONTUÁRIOS DOS PACIENTES. PESQUISA 2021. Disponível em https://cetic.br/en/tics/saude/2021/estabelecimentos/B1/

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR TIPO DE DADO SOBRE O PACIENTE DISPONÍVEL ELETRONICAMENTE. PESQUISA 2021. Disponível em https://cetic.br/en/tics/saude/2021/estabelecimentos/B2/

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR TIPO DE FERRAMENTA DE SEGURANÇA DA INFORMAÇÃO UTILIZADA. PESQUISA 2021. Disponível em https://www.cetic.br/pt/tics/saude/2021/estabelecimentos/A10/

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR MEDIDAS ADOTADAS EM RELAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. PESQUISA 2021. Disponível em https://www.cetic.br/pt/tics/saude/2021/estabelecimentos/A12/

TIC SAÚDE 2022 Congresso Brasileiro de 02 de dezembro de 2022

Informática em Saúde - CBIS LANÇAMENTO DOS RESULTADOS. Disponível em https://cetic.br/media/analises/TIC-Saude-2022_apresentacao-de-lancamento_Final_rev2.pdf

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR MEDIDAS ADOTADAS EM RELAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS. PESQUISA 2022. Disponível em https://cetic.br/pt/tics/saude/2022/estabelecimentos/A12/

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR TIPO DE FERRAMENTA DE SEGURANÇA DA INFORMAÇÃO UTILIZADA. PESQUISA 2022. Disponível em https://cetic.br/pt/tics/saude/2022/estabelecimentos/A10/.

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR FORMA DE MANUTENÇÃO DAS INFORMAÇÕES CLÍNICAS E CADASTRAIS NOS PRONTUÁRIOS DOS PACIENTES. PESQUISA 2022. Disponível em https://cetic.br/pt/tics/saude/2022/estabelecimentos/B1/.

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR TIPO DE DADO SOBRE O PACIENTE DISPONÍVEL ELETRONICAMENTE. PESQUISA 2021. Disponível em https://cetic.br/pt/tics/saude/2022/estabelecimentos/B2/.

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR FUNCIONALIDADES DE TROCA DE INFORMAÇÕES EM SAÚDE DISPONÍVEIS EM SISTEMA. PESQUISA 2021. Disponível em https://cetic.br/pt/tics/saude/2022/estabelecimentos/B6/.

CETIC BR. Pesquisa ESTABELECIMENTOS DE SAÚDE, POR PONTOS DE ACESSO AO PRONTUÁRIO ELETRÔNICO DO PACIENTE. PESQUISA 2022. Disponível em https://cetic.br/pt/tics/saude/2022/estabelecimentos/B7/.