UNIVERSIDADE DO VALE DO RIO DOS SINOS – UNISINOS
UNIDADE ACADÊMICA DE PESQUISA E PÓS-GRADUAÇÃO
PROGRAMA DE PÓS-GRADUAÇÃO EM DIREITO
NÍVEL MESTRADO PROFISSIONAL

TAIANE MEIRELLES ALFONSIN

GESTÃO DE *COMPLIANCE* ADEQUADA À LEI GERAL DE PROTEÇÃO DE DADOS NA ÁREA DA SAÚDE

Porto Alegre
2022

TAIANE MEIRELLES ALFONSIN

GESTÃO DE *COMPLIANCE* ADEQUADA À LEI GERAL DE PROTEÇÃO DE DADOS NA ÁREA DA SAÚDE

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito, pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientador: Prof. André Rafael Weyermuller

Porto Alegre

2022

Ficha Catalográfica

A388 Alfonsin, Taiane Meirelles

Gestão de compliance adequada à Lei Geral de Proteção de Dados na área da saúde / Taiane Meirelles Alfonsin – Porto Alegre, 2022.
112 f. : il.

Dissertação (Mestrado) – Programa de Mestrado Profissional em Direito – Universidade do Vale do Rio do Sinos – UNISINOS, 2022.
Orientador: Prof. Dr. André Rafael Weyermuller.

1. Lei Geral de Proteção de Dados. 2. Compliance. 3. Área da Saúde. I. Weyermuller, André Rafael. II. Título.

CDU 347.122

Bibliotecária Responsável: Marianna de Almeida Cunha
CRB 10/2525

TAIANE MEIRELLES ALFONSIN

GESTÃO DE *COMPLIANCE* ADEQUADA À LEI GERAL DE PROTEÇÃO DE DADOS NA ÁREA DA SAÚDE

Dissertação apresentada como requisito parcial para obtenção do título de Mestre em Direito, pelo Programa de Pós-Graduação em Direito da Universidade do Vale do Rio dos Sinos (UNISINOS).

Aprovada em: _____ de _____ de _____.

BANCA EXAMINADORA

_____

Componente da Banca Examinadora – Instituição a que pertence

_____

Componente da Banca Examinadora – Instituição a que pertence

_____

Componente da Banca Examinadora – Instituição a que pertence

AGRADECIMENTOS

Reservo esse momento para agradecer principalmente ao meu marido, por sempre me apoiar em todas as minhas decisões e por ser a voz da minha consciência, e aos meus filhos gêmeos, os que me acompanharam por nove meses de aulas na minha barriga e o meu outro bebê que virou um anjinho no decorrer das aulas. Aos meus pais, obrigada por todos os ensinamentos, espero um dia poder retribuir, pelo menos um pouco, tudo que já fizeram por mim. Gostaria de agradecer a minha irmã, por ser uma fonte de inspiração, espero ter pelo menos a metade da força e garra que ela tem. Por fim, mas não menos importante, gostaria de agradecer a todos os professores que já passaram pela minha vida e a minha colega e amiga Rafaella, que me passou leveza e tranquilidade em muitos momentos que precisei. Os ensinamentos que aprendi e, até mesmo, as lições de vida que me foram dadas são algo que vou levar para sempre.

A todos, os meus singelos agradecimentos.

Muito obrigada!

RESUMO

O presente trabalho tem como objetivo apresentar a relação entre o *Compliance* e a Lei Geral de Proteção de Dados (LGPD) na área da saúde. Para o desenvolvimento deste texto serão analisados os aspectos gerais da LGPD e seus princípios norteadores, discorrendo-se sobre os efeitos e as principais disposições da referida lei. Além disso, serão abordados os impactos econômicos e empresariais da LGPD, correlacionando-os com o sistema de *Compliance*. Inicialmente, apresentar-se-á o conceito de dados pessoais e de tratamento à luz da Lei Geral de Proteção de Dados Pessoais, com exposição de overview da referida regulamentação. Na sequência, abordar-se-ão privacidade e a proteção de dados aplicadas à área da saúde, com análises estruturais, seguidas pela inclusão da proteção de dados junto aos sistemas de compliance e governança corporativa. Serão sugeridas medidas concretas de implementação de políticas na área da saúde, com a realização de avaliação de riscos no setor da saúde e aplicação da proteção de dados. Busca-se, nas conclusões deste trabalho, apresentar-se-á resposta para a seguinte questão: como adequar uma empresa da área da saúde às normas da LGPD em conformidade com o *Compliance*? Por fim, apontar-se-ão mecanismos de implementação da LGPD na área da saúde, por meio dos quais serão propostas maneiras para que a gestão das empresas da área da saúde consolide um sistema mais responsável no que diz respeito ao compartilhamento de dados pessoais. Conclui-se que é necessário condutas gerais que devem ser seguidas dentro das organizações e que possam produzir efeitos concretos para a proteção e segurança dos dados pessoais na área da saúde. Ainda, para robustecer a implementação da Lei Geral de Proteção de Dados, sugere-se um trabalho simultâneo de *Compliance* de dados, o qual deverá ocorrer de forma multidisciplinar, preventiva e com procedimentos de *checklists* diários. Assim há necessidade que a proteção de dados deve fazer parte da cultura empresarial, e sua importância deve ser compreendida por todos os segmentos. Contudo, não é possível falar em um único modelo de programa de *Compliance*, na medida que sua efetividade depende da observância das especificidades de cada organização e da revisão constante dos riscos envolvidos no negócio. O desafio das empresas é justamente construir um modelo sob medida, adequado às suas especificidades e sem se descuidar das diretrizes da lei. O novo cenário brasileiro é voltado às empresas com culturas mais seguras, éticas e transparentes.

Palavras-chave: Lei Geral de Proteção de Dados; *Compliance*; área da saúde. Implementação.

ABSTRACT

This article aims to discuss about the relationship between Compliance and the General Data Protection Law (LGPD) in the health care area. For the development of this text, the general aspects of the LGPD and its guiding principles will be analyzed, discussing the effects and main provisions of the referred law. In addition, the economic and business impacts of the LGPD will be addressed, correlating them with the Compliance system. Initially, the concept of personal data and treatment will be presented in the light of the General Law for the Protection of Personal Data, with an overview of the aforementioned regulation. Next, privacy and data protection applied to the health area will be addressed, with structural analyses, followed by the inclusion of data protection in compliance and corporate governance systems.Concrete measures will be suggested for the implementation of such policies in the health care area, with the assessment of risk in the health care sector and the application of data protection. At the conclusion, we seek to present an answer to the following question: how to adapt a company or office in the health care area to the LGPD standards in accordance with Compliance? Finally, mechanisms for implementing the LGPD on this sector are pointed out, through which health companies will manage to consolidate a more responsible system in regard to personal data sharing. It is concluded that it is mandatory to adopt general conducts within organizations that can generate concrete effects in order to safely protect personal data in the health care area. Also, to strengthen the implementation of the General Data Protection Law, simultaneous data compliance work is suggested, which should take place in a multidisciplinary, preventive manner and with daily checklist procedures. Thus, there is a need for data protection to be part of the corporate culture, and its importance must be understood by all segments. However, it is not possible to speak of a single Compliance program model, as its effectiveness depends on observing the specificities of each organization and the constant review of the risks involved in the business. The challenge for companies is precisely to build a tailored model, suited to their specificities and without neglecting the guidelines of the law. The new Brazilian scenario is aimed at companies with safer, more ethical and transparent cultures

LISTA DE SIGLAS E ABREVIATURAS

ANPD	Autoridade Nacional de Proteção de Dados
ANS	Agência Nacional de Saúde Complementar
ANVISA	Agência Nacional de Vigilância Sanitária
CF	Constituição Federal
GDPR	General Data Protection Regulation
DPO	Data Protection Officer
IBGC	Instituto Brasileiro de Governança Corporativa
IoT	Internet of Things
LGPD	Lei Geral de Proteção de Dados Pessoais, Lei 13.709 de 2018.
MCI	Marco Civil da Internet, Lei 12.965 de 2014.
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
OMS	Organização Mundial da Saúde
PbD	Privacy By Design
RGPD	Regulamento Geral sobre a Proteção de Dados
RIPD	Relatório de Impacto à Proteção dos Dados Pessoais
SUSEPE	Superintendência dos Serviços Penitenciários

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

O presente estudo destacará a importância da elaboração de um plano de governança de dados e da adoção de medidas eficientes de *Compliance* para evitar consequências jurídicas. Por oportuno, acrescenta-se que o alinhamento das empresas aos preceitos da Lei Geral de Proteção de Dados poderá ser visto como um investimento de ganho imediato, pois a necessidade de alteração das políticas internas (*Compliance*) em sintonia com a LGPD é uma oportunidade para a realização de novos modelos de negócios e para aumentar o nível de privacidade, segurança e gerenciamento da empresa.

Em linhas gerais, para o desenvolvimento deste trabalho serão analisados os aspectos gerais da LGPD e os seus princípios norteadores. Ainda, discorre-se sobre os efeitos e as principais disposições da referida lei. Também serão abordados os impactos econômicos e empresariais da LGPD, correlacionando-os com o sistema de *Compliance*. Além disso, serão sugeridas medidas concretas de implementação de políticas na área da saúde, com a realização de avaliação de riscos no setor da saúde e com a aplicação da proteção de dados. Ao final, serão apresentadas algumas conclusões.

A questão de pesquisa a ser respondida no presente trabalho é: quais as diretrizes que devem ser seguidas pelas organizações da área da saúde para suprir as necessidades de cumprimento da LGPD, e quais as dificuldades e os problemas dessa implementação?

Essa é uma linha que merece ser estudada e desenvolvida com mais intensidade, especialmente por conta da duplicidade de interlocução entre *Compliance* e saúde e entre proteção de dados e saúde.

Para responder ao problema de pesquisa foram elencados como objetivo geral analisar e conhecer a Lei Geral de Proteção de Dados, verificando, dentro das normativas regulamentadoras de *Compliance,* quais serão as ferramentas úteis para que a referida lei se torne aplicável e efetiva dentro das organizações da área da saúde.

Quanto aos objetivos específicos deste estudo, por sua vez, consistem em: conhecer os principais aspectos gerais norteadores da LGPD; analisar os impactos econômicos da LGPD; conhecer a origem e as ferramentas úteis para a

implementação de *Compliance*; estabelecer as diretrizes de aplicação da LGPD; necessidade de avaliar os riscos e propor uma forma de mitigá-los; propor diretrizes para um sistema de *Compliance* efetivo na aplicação da LGPD; conhecer os desafios no bojo da dinâmica corporativa contemporânea; conhecer a estrutura da saúde e as principais regulamentações na área da saúde; Risco de privacidade e integração da proteção de dados na área da saúde no sistema de gestão de Compliance.

Conduz-se este estudo no âmbito dos métodos dedutivo e dialético, como técnica de pesquisa, elegendo-se o procedimento bibliográfico e a interpretação das legislações e regulamentos pertinentes ao assunto, que restaram organizadas em três capítulos.

Com relação ao primeiro capítulo serão abordados o conceito de dado pessoal e suas implicações, bem como será realizado um *overview* da LGPD. A Lei Geral de Proteção de Dados (LGPD) ganha forte reforço com avanços tecnológicos como a utilização diária da internet e outros relacionados a fenômenos contemporâneos. Diante disso, o conceito de privacidade passou a ser não apenas o de direito de evitar interferências na vida privada das pessoas, mas também o de saber como estão sendo utilizados os dados dos indivíduos.

Ao final do primeiro capítulo serão tratados aspectos econômicos e o tratamento dos dados sensíveis.

No segundo capítulo, abordar-se-á a repercussão da proteção dos dados na área da saúde, no qual serão propostas alternativas a uma outra relação jurídica no que diz respeito aos dados dos pacientes, cuja importância aumentou em escala exponencial em tempos de COVID-19. O presente estudo não abrange nem esgota todos os aspectos e as diretrizes decorrentes da LGPD. Entretanto, torna-se essencial sua veiculação neste momento para que essa lei comece a ser aplicada de forma equilibrada, homogênea e de forma a inspirar credibilidade entre a população.

O início da vigência da LGPD é um marco significativo para a consolidação dos direitos e das garantias fundamentais do indivíduo, com forte impacto sobre todos os setores da sociedade. O setor de saúde, por envolver um enorme fluxo de tratamento de dados pessoais sensíveis, merece um olhar aprofundado e específico sobre o tema.

Os seres humanos serem cada vez mais dependentes dos instrumentos tecnológicos, sujeitando-se a um permanente estado de insegurança. O presente

projeto tem relevância a partir do momento em que, com a vigência da LGPD, empresas serão fiscalizadas e deverão se renovar diante dos novos parâmetros legais e mercadológicos. Mais do que nunca, o mercado passará a exigir que os seus agentes, além de protegerem a privacidade do cidadão, fomentem a inovação e promovam seus negócios com maior segurança, inclusive jurídica.

Ao final do segundo capítulo, serão avaliados os programas de Compliance na área da saúde, eis que, com o advento da LGPD, inúmeras empresas deverão alterar algumas políticas para estarem em conformidade com a nova legislação. Assim, a Política de *Compliance* das organizações, por exemplo, deverá ser modificada, pois, com a chegada da nova LGPD, muitas das políticas já implementadas nas empresas deverão ser atualizadas e padronizadas de acordo com essa novidade legislativa.

No último capítulo, o enfoque será a proteção de dados aplicadas aos programas de *Compliance* e governança corporativa. Como garantir que as normas estão sendo seguidas por terceiros, a importância da análise de riscos de impactos que possam vir a ser causados de forma direta ou indireta aos direitos humanos, sendo que a LGPD tem como fundamento a proteção a privacidade e outros direitos. Portanto, destaca-se, no presente estudo, a importância de se elaborar um plano de governança de dados, de se adotar medidas eficientes de *Compliance* de dados pessoais para evitar consequências jurídicas e de se definir quais instrumentos organizacionais serão suficientes para suprir as necessidades da implementação da LGPD. Mesmo com todos os cuidados, a LGPD reserva ainda mais proteção a um grupo específico de dados: aqueles que receberam o nome de “sensíveis”. Dentro dessa categoria, conforme a LGPD existem os dados de caráter político, religioso, filosófico ou moral, racial, dados de opção sexual, dados genéticos, de filiação sindical e todos aqueles dados relacionados à saúde.

Assim, um sistema de gestão de *Compliance* na área da saúde se torna imprescindível, pois qualquer deslize coloca em xeque a proteção do próprio bem da vida, o qual é protegido pela área da saúde.

Este estudo contribui para ampliar a discussão sobre a aplicabilidade e os ganhos do efetivo *Compliance* como instrumento de governança para a gestão de risco na formação de um ambiente em conformidade com a defesa de valores intrínsecos para a transformação da realidade organizacional. Parte-se da hipótese

de que pode ser criado um comitê específico para tratar dos temas, com reuniões de frequência preestabelecidas a fim de que possam ser definidas quais diretrizes devem ser tomadas para que seja efetiva a aplicação das políticas de *Compliance*, sem ferir as normas da LGPD. Ainda, para se obter uma resposta adequada para os desafios sociais atuais, é primordial que a teoria do direito se reconstrua e se reinterprete a ponto de compreender e solucionar os novos problemas enfrentados pelo homem na era da informação.

> São necessárias técnicas de anonimização e pseudonimização, políticas de privacidade, DPO (data protection officer/executivo de proteção de dados), armazenamento de dados pessoais, transparência algorítmica, selos/certificação de privacidade e medidas de PbD (privacy by design) para mitigar riscos e implicações legais identificadas. Além disso, é preciso consolidar uma dogmática sobre proteção de dados pessoais que delineie os contornos e as formas de garantia desse direito fundamental, sendo necessária a fiscalização constante dos atos dos responsáveis pelo processamento de dados, de modo a observar se estão em consonância com esse direito fundamental.

Para que isso seja possível, faz-se necessária a criação de novas regras e de procedimentos consignados tanto no código de conduta quanto na normatização interna no sentido de que sejam feitos *upgrades* periódicos e atualizados para fins de garantir que as normas de *Compliance* sejam efetivamente cumpridas. Desse modo, é necessário um programa de governança e um monitoramento contínuo.

Esse monitoramento contínuo, em muitos casos, é chamado de “Comitê de *Compliance*”, o qual é constituído por profissionais de diversas áreas da empresa, principalmente pelos da área de tecnologia, os quais nortearão a elaboração das novas normas e a implementação das novas políticas.

Ademais, as ferramentas de *Compliance* permitirão que as organizações cumpram suas obrigações de proteção de dados enquanto protegem os direitos de privacidade das pessoas. Esses compromissos podem ser demonstrados por meio de documentação interna e treinamento de funcionários em relação aos mandatos associados à LGPD – por exemplo, por meio de políticas internas escritas.

2 PROTEÇÃO DE DADOS

A presente pesquisa pretende avaliar o impacto da LGPD na saúde. Para tanto, inicia com o conceito de dados pessoais e tratamento, bem como suas implicações, para que isso possa servir de base para os próximos capítulos.

2.1 DADOS PESSOAIS e PRIVACIDADE: TRATAMENTO, CONCEITO E IMPLICAÇÕES

Esse estudo pretende avaliar o impacto da LGPD na área da saúde. Para isso, é importante primeiramente conceituar questões pontuais sobre o tratamento de dados pessoais e as suas implicações.

Tendo em vista que os seres humanos estão cada vez mais dependentes de instrumentos tecnológicos, percebe-se um permanente estado de insegurança. Em razão disso, foi sancionada, em agosto de 2018, a Lei Geral de Proteção de Dados, Lei n.º 13.709/2018[1], que estabelece regras sobre coleta, tratamento, armazenamento e compartilhamento de dados pessoais gerenciados pelas organizações.

A LGPD foi inspirada em uma outra lei igualmente conhecida no Brasil por sua sigla, a GDPR – General Data Protection Regulation[2] (em português, RGPD – Regulamento Geral sobre a Proteção de Dados), norma que regulamenta a proteção de dados pessoais no âmbito da União Europeia.

A respeito da personalidade, tema importante abordado na GDPR, Amaral ensina:

> [...] é na filosofia grega que se encontra a maior contribuição para a teoria dos direitos da personalidade, com o surgimento do dualismo nas fontes jurídicas, um direito natural como ordem superior criada pela natureza, e um direito positivo, as leis estabelecidas na cidade, (*ius in civitate positum*), sendo o homem a origem e a razão de ser da lei e do direito.[3]

---

[1] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 out. 2022.

[2] EUROPEAN UNION. Regulamento (UE) 2016/679, de 27 de abril de 2016. General Data Protection Regulation. **Official Journal of the European Union**, Brussels, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL. Acesso em: 22 jun. 2022.

[3] AMARAL, Francisco. **Direito Civil**. São Paulo: Saraiva, 2018. p. 251.

Uma das novidades da GDPR é a “do princípio da responsabilidade, pelo qual o referido regulamento imputa às empresas e à administração pública a responsabilidade civil pela coleta, armazenagem e proteção dos dados.”[4] Nesse aspecto, em caso de violação ou vazamento de dados, além do reparo aos proprietários dos dados, o RGPD prevê a notificação obrigatória à autoridade de proteção de dados, o que deve ocorrer no prazo máximo de 72 horas.

Em uma sociedade cada vez mais informatizada, na qual o fluxo de dados se tornou um componente crucial para o comércio, as comunicações e as interações sociais, a proteção de dados pessoais passou a ser uma preocupação para grande parte dos países. Nesse contexto, muitos países têm adotado novas regras de proteção de dados ou modernizado as que já tinham, como Coreia do Sul, Chile, Tailândia, Índia, Indonésia e Brasil. Atualmente, já são mais de cem países com marcos regulatórios para proteção de dados pessoais em todo o mundo.[5]

Em agosto de 2018, foi sancionada a Lei n.º 13.709[6], popularmente conhecida como Lei Geral de Proteção de Dados Pessoais – ou simplesmente LGPD –, para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo.

A dignidade humana foi fator crucial para a distinção dos direitos da personalidade, visto que tais direitos foram ganhando tanto mais relevo quando se distinguiu, na pessoa humana, elemento incorpóreo de dignidade, afinal a proteção da dignidade humana é objetivo desses direitos.[7] Ainda, preceitua Clóvis Beviláqua, que “[...] pessoa é o ser a quem se atribuem direitos e obrigações, e Personalidade é

---

[4] Um dos fundamentos do RGPD é o de que a proteção de dados deve ser uma das bases da “economia digital”, porquanto as pessoas têm direito à preservação dos próprios dados, sendo vedado o intercâmbio de dados entre empresas sem o consentimento dos titulares. (BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021. p. 79.)

[5] CONSUMERS INTERNATIONAL. **Consumers International**: Strategy. [*S. l.*]: Consumers International, 2018. Disponível em: https://www.consumersinternational.org/media/155232/strategy-eng.pdf. Acesso em: 7 jul. 2021. p. 4.

[6] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

[7] FERMENTÃO, Cleide Aparecida Gomes Rodrigues. Os direitos da personalidade como direitos essenciais e a subjetividade do direito. **Revista Jurídica CESUMAR**, Maringá, v. 6, n. 1, p. 241-266, 2006. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/313. Acesso em: 28 jun. 2022.

a aptidão reconhecida pela ordem jurídica a alguém para exercer e contrair obrigações".[8]

Pontes de Miranda ensina: "Quem pode ter um direito é pessoa".[9] Logo, a dignidade aglomera os direitos da personalidade, os direitos fundamentais do indivíduo e reconhece a afirmação da integridade física e espiritual do homem, a garantia do desenvolvimento de sua personalidade e a defesa de sua autonomia individual.[10]

A LGPD versa sobre o tratamento de dados pessoais dispostos em meio físico ou digital, feitos por pessoa física ou jurídica de direito público ou privado e engloba um amplo conjunto de operações efetuadas em meios manuais ou digitais.[11]

O desenvolvimento tecnológico experimentado pela sociedade nos últimos anos não deixa transparecer toda a trajetória histórica até que a privacidade pudesse ser reconhecida como um bem jurídico. Essa trajetória foi atribuída aos juristas norte-americanos Samuel D. Warren e Louis D. Brandeis com a sua primeira produção científica, que tratou o tema *Right to Privacity,* em 1890.[12]

Com discussão iniciada em 1890 por meio do artigo de Louis D. Brandeis e Samuel D.Warren, o conceito de privacidade foi revigorado com a Declaração Universal de Direitos Humanos prevendo que nenhuma pessoa poderia sofrer interferências arbitrárias sobre sua privacidade, família, residência e correspondência. A partir daí, surgem diversas legislações ao redor do mundo sobre o tema.[13]

Entretanto, é pacífica a conclusão de que o direito à proteção de dados pessoais não é absoluto e deve ser equilibrado com outros direitos fundamentais em conformidade com a Constituição Federal (CF)[14], como o da privacidade e o princípio da proporcionalidade.

---

[8] BEVILÁQUA, Clóvis. **Teoria Geral do Direito Civil**. São Paulo: Servanda, 2015. p. 70.
[9] MIRANDA, Pontes de. **Tratado de direito privado**. São Paulo: Revista dos Tribunais, 2012. p. 153.
[10] CANOTILHO, J. J. Gomes. **Direito Constitucional e teoria da Constituição**. Coimbra: Almedina, 2017. p. 363.
[11] GUIA de Boas Práticas - Lei Geral de Proteção de Dados (LGPD). *In:* BRASIL. **Governo Digital.** [Brasília, 2020]. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 31 ago. 2020. p.12.
[12] WARREN, Samuel D.; BRANDEIS, Louis D. Right to privacity. **Harvard Law Review**, Boston, v. 4, n. 5, 1890. p. 193-220.
[13] WARREN, Samuel D.; BRANDEIS, Louis D. Right to privacity. **Harvard Law Review**, Boston, v. 4, n. 5, 1890. p. 193-220.
[14] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jan. 2022.

Samuel D. Warren e e Louis D. Brandeis assim definiram privacidade:

> We must therefore conclude that the rights, so protected, whatever their exact nature, are not rights arising from contract or from special trust, but are rights against the world; and, as above stated, the principle which has been applied to protect these rights is in reality not the principle of private property, unless that world be used in an extended and unusual sense. The principle which protects personal writings and any other productions of the intellect or of the emotions, is the right to privacy, and the law has no new principle to formulate when it extends this protection to the personal appearance, sayings, acts and to personal relation, domestic or otherwise.[15]

A referida LGPD trará uma mudança de paradigma, com aspetos relevantes à atividade empresarial, sobretudo considerando a Quarta Revolução Industrial, que tem como características primordiais a velocidade, a amplitude, a profundidade e o impacto sistêmico.[16]

Segundo Bauman e Lyon:

> Los desafíos que plantea esta situación son tremendos. De entrada, la nueva vigilancia, basada en el procesamiento de la información, más que en lo que afirmaba Foucault, permite una nueva transparencia en la que no solamente los ciudadanos como tal sino todos nosotros, en cada uno de los roles que asumimos en nuestra "vida cotidiana, somos constantemente controlados, observados, examinados, evaluados, valorados y juzgados. Pero no ocurre lo mismo en el sentido contrario. A medida que los detalles de nuestra vida cotidiana se hacen más transparentes para los organismos que nos vigilan, más difícil resulta discernir cuáles son sus propias actividades. A medida que el poder se mueve con la velocidad de las señales electrónicas en la fluidez de la modernidad líquida, el grado de transparencia crece para unos y disminuye para otros.[17]

---

[15] "Devemos, portanto, concluir que os direitos assim protegidos, qualquer que seja sua natureza exata, não são direitos decorrentes de contrato ou de confiança especial, mas são direitos contra o mundo; e, como dito acima, o princípio que foi aplicado para proteger esses direitos não é, na realidade, o princípio da propriedade privada, a menos que esse mundo seja usado em um sentido extenso e incomum. O princípio que protege os escritos pessoais e quaisquer outras produções do intelecto ou das emoções é o direito à privacidade, e a lei não tem nenhum princípio novo a formular quando estende essa proteção à aparência pessoal, ditos, atos e à relação pessoal, doméstica ou outro." (WARREN, Samuel D.; BRANDEIS, Louis D. Right to Privacy. **Harvard Law Review**, Boston, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/ cs5436/warren-brandeis.pdf?. Acesso em: 16 jun. 2021. p. 213.)

[16] SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016. p.90.

[17] "Os desafios colocados por esta situação são enormes. Desde logo, a nova vigilância, baseada no tratamento da informação, e não no que Foucault afirmava, permite uma nova transparência em que não só os cidadãos como tais, mas todos nós, em cada um dos papéis que assumimos no nosso "Cotidiano", somos constantemente controlados, observados, examinados, avaliados, valorizados e julgados. Mas o mesmo não acontece na direção oposta. À medida que os detalhes de nossas vidas diárias se tornam mais transparentes para as agências que nos monitoram, fica

Ademais, a Lei n.º 14.460, de 25 de outubro de 2022 transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados.[18]

A ANPD é indispensável para a efetividade da LGPD sendo responsável por garantir seu cumprimento e efetivação e por estabelecer e manter padrões persistentes de aplicação.[19]

Todavia, em razão da efervescência do debate, esse assunto já chegou aos tribunais brasileiros, que têm analisado a (i)legalidade do tratamento de dados no Brasil. Um exemplo foi a decisão do Plenário do STF que suspendeu a MP 954[20] que, durante o período de pandemia pelo coronavírus, liberou o compartilhamento de dados pessoais por empresas de telefonia com o IBGE (ADIs 6.387, 6.388, 6.389, 6.390 e 6.393)[21]. Ainda que anterior à vigência da LGPD, essa norma foi considerada inconstitucional por violar o direito à privacidade dos cidadãos. Com o crescimento exponencial da utilização de dados pessoais tanto pelo setor privado quanto pelos órgãos públicos, surgiram, no mundo, várias legislações visando à tutela da proteção de dados pessoais. O Brasil possuía uma série de normas setoriais sobre o assunto, com dispositivos que podem ser aplicados à proteção de dados e que estão espalhados pela Constituição Federal, pelo Código de Defesa do Consumidor, pelo Código Civil, pela Lei de Acesso à Informação, pela Lei do Cadastro Positivo e pelo Marco Civil da Internet.[22]

Esse cenário, entretanto, sofreu alteração em 14 de agosto de 2018 com a

---

mais difícil discernir quais são suas próprias atividades. À medida que o poder se move com a velocidade dos sinais eletrônicos na fluidez da modernidade líquida, o grau de transparência aumenta para alguns e diminui para outros." (BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Argentina: Paidós, 2013. p. 32-33.)

[18] BRASIL. Lei n.º 14.460, de 25 de outubro de 2022. Transforma a Autoridade Nacional de Proteção de Dados (ANPD) em autarquia de natureza especial e transforma cargos comissionados. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2022/Lei/L14460.htm. Acesso em: 20 nov. 2022.

19 MENDES, Laura Schertel Ferreira; DONEDA, Danilo César Maganhoto. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da Proteção de Dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, nov./dez. 2018. p. 24-25.

[20] BRASIL. MP 954 e 17 de Abril de 2020. Brasília, DF: Presidência da República, 2020. Disponível em https://www.planalto.gov.br/CCIVIL_03/_Ato2019-2022/2020/Mpv/mpv954.htm. Acesso em: 20 nov. 2022.

[21] VALENTE, Fernanda. STF barra MP que previa compartilhamento de dados pessoais com IBGE. **Consultor Jurídico**, São Paulo, 7 maio 2020. Disponível em: https://www.conjur.com.br/2020-mai-07/stf-barra-mp-previa-compartilhamento-dados-pessoais-ibge. Acesso em: 11 set. 2022.

[22] BIONI, Bruno Ricardo. **Proteção de dados pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

sanção da Lei n.º 13.709/2018[23], que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.[24]

Além de ser a primeira lei geral nacional sobre o tema, a importância da LGPD está na apresentação de regras para o tratamento de dados pessoais. Essas regras vão desde os princípios que disciplinam a proteção de dados pessoais, passando pelas bases legais aptas para justificar o tratamento de dados até a fiscalização e a responsabilização dos envolvidos no tratamento de dados pessoais.

A LGPD também prevê a possibilidade de a pessoa natural a quem se referem os dados pessoais requerer informações, como a confirmação da existência de tratamento dos seus dados pessoais, o acesso aos dados, a correção de dados incompletos, a eliminação de dados desnecessários e a portabilidade de dados pessoais a outro fornecedor de produtos e serviços.[25]

A esse respeito, “dados pessoais são aquelas informações que permitem identificar a pessoa a quem dizem respeito. A sua proteção tem como objeto (1) o direito à intimidade e (2) o direito à identidade pessoal. O primeiro importa na autodeterminação informativa”[26], e o segundo, por sua vez, tem como objetivo barrar que a identidade da pessoa seja modificada, seja por informações incompletas ou incorretas.[27]

A proteção de dados pessoais tem como fundamentos alguns princípios: o respeito à privacidade; a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e

---

[23] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

[24] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 1.º.

[25] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 11.

[26] Para um exame mais detalhado sobre o direito à autodeterminação informativa, ver LAEBER, Márcio Rafael Silva. Proteção de dados pessoais: o direito à autodeterminação informativa. **Revista de Direito Bancário e do Mercado de Capitais**, São Paulo, n. 37, jul. 2007. p. 59.

[27] PROTEÇÃO de dados pessoais: privacidade *versus* avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. (Cadernos Adenauer xx, n. 3).p. 25.

da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor; e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[28]

A LGPD contém exceções que devem ser interpretadas taxativamente (*numerus clausus*) e nas quais não se aplica o tratamento de dados pessoais: realizado por pessoa natural para fins exclusivamente particulares e não econômicos; realizado para fins exclusivamente: a) jornalístico e artísticos ou b) acadêmicos; realizado para fins exclusivos de: a) segurança pública, b) defesa nacional, c) segurança do Estado ou d) atividades de investigação e repressão de infrações penais (esse tratamento será regido por legislação específica); ou proveniente de fora do território nacional e que não seja 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.[29]

Os princípios elencados devem nortear a atividade da coleta de dados e de seu tratamento, sendo que, nos procedimentos de tratamento de dados, devem ser respeitados os direitos constitucionais e fundamentais dos titulares dos dados, preservando a sua intimidade, vida privada, honra e imagem.

A nova legislação inaugura uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e acerca dos seus reflexos em direitos fundamentais, como a liberdade, a privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2.2 SISTEMA DE PROTEÇÃO DE DADOS E *OVERVIEW* DA LGPD

A fim de garantir melhor compreensão para esse debate, passa-se à análise do sistema de proteção de dados, com visão geral da Lei Geral de Proteção de Dados

---

[28] PROTEÇÃO de dados pessoais: privacidade *versus* avanço tecnológico. Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. (Cadernos Adenauer xx, n. 3).p.19.

[29] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 4.º, IV.

Pessoais. Em razão da dualidade que envolve o tratamento de dados, principalmente no que diz respeito à privacidade e ao fomento da economia, criou-se uma espécie de sistema de proteção por meio do surgimento de diversas legislações e regulamentos não só no ordenamento jurídico brasileiro, mas no âmbito mundial.

Primeiramente, dada a importância da compreensão do contexto histórico sobre a privacidade e proteção de dados, em 28 de janeiro de 1981, foi assinada a Convenção 108, que foi o primeiro tratado internacional juridicamente vinculativo que tratou da privacidade e proteção de dados.[30]

A Lei Geral de Proteção de Dados representa o marco de uma nova cultura de tutela da privacidade e dos dados pessoais. Caminhando ao encontro do Regulamento europeu, a norma institui modelo preventivo de proteção de dados, baseado na ideia de que todo dado pessoal possui relevância e valor por representar projeção da pessoa humana.[31]

Assim, os dados pessoais são armazenados por mais tempo do que o necessário, sendo acessados sem controle nem responsabilidade por diversas pessoas – não necessariamente relacionadas ao tratamento – e, muitas vezes, sem a autorização de seus titulares e/ou sem finalidades delimitadas. Visto que tais dados passaram a ser coletados, acessados e armazenados por meio digitais, a disseminação e acesso indevidos são cada vez mais recorrentes. Essa é a razão pela qual aumenta a preocupação com a forma com que as empresas utilizam dados pessoais. Não restam dúvidas, portanto, sobre a relevância do tema e, por conseguinte, sobre a necessidade impositiva de as empresas se adequarem às exigências implementadas pela nova legislação no âmbito da proteção de dados pessoais.[32]

A adequação capaz de legitimar o tratamento de dados pessoais enfrentará

---

[30] Convenção 108 na Europa: Disponível em: http://www.encarregadodaprotecaodedados.com/2021/05/20/convencao-108-do-conselho-da-europa/. Acesso em 22 de nov. de 2022. n.p.

[31] TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, v. 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 28 jun. 2021.p.15.

[32] Na primeira década do século XXI, o número de pessoas conectadas à Internet passou de 350 milhões para 2 bilhões. Além disso, neste mesmo período, o número de pessoas com celulares passou de 750 milhões para 5 bilhões. A expectativa para o ano de 2025 é de a maior parte da população mundial estar com acesso à informação instantânea, sendo que, se for mantido o ritmo de crescimento de pessoas conectadas à Internet, ter-se-á, na mencionada data, 8 bilhões de pessoas *online*. (SCHMIDT, Eric; COHEN, Jared. **The New Digital Age**: Reshaping the Future of People, Nations and Business. London: John Murray, 2014. p. 15.)

desafios práticos complexos diante da atual praxe empresarial – por exemplo, farmácias estabelecidas em território nacional que ofertam descontos em medicamentos por meio da exigência de cadastro com CPF[33] e outros dados pessoais dos usuários. Por se tratar de dados sensíveis, por vezes pode haver necessidade de consentimento do uso desses dados por parte dos titulares. Esse consentimento deverá ser livre, explícito e informado, específico e destacado[34], sendo expressamente vedado pela LGPD o compartilhamento desses dados entre empresas visando unicamente vantagens econômicas. Esse é um dos inúmeros desafios a serem enfrentados pelas empresas diante da nova legislação de proteção de dados pessoais, sendo imperiosa a adequação dessas empresas fim de fomentar o desenvolvimento dessa legislação em uma sociedade cada vez mais digital.

Para que uma informação seja considerada dado pessoal e esteja sujeita ao regime previsto na LGPD, necessariamente deve ser relacionada a uma pessoa natural. Logo, a LGPD não se aplica à informação de pessoas jurídicas. Além disso, as pessoas naturais devem ser identificadas ou identificáveis.[35]

A Lei 13.709/18 ainda estabelece um regime específico de proteção para os dados pessoais sensíveis. Por dados pessoais sensíveis entende-se informações a respeito de "origem racial ou étnica, convicção religiosa, opiniões políticas, filiação a sindicato, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos"[36]. O processamento desse tipo de dados demanda maior cautela e enquadramento a uma base legal específica, incluindo-se, entre elas, o consentimento prévio do titular de forma livre, inequívoca, informada, expressa e específica.

---

[33] DERMARTINI, Felipe. O que as farmácias fazem com o seu CPF? Governo questiona uso de dados. **Canaltech**, [*s. l.*], 17 nov. 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-as-farmacias-fazem-com-o-seu-cpf-governo-questiona-uso-de-dados-201966/. Acesso em: 13 out. 2022.p.2.

[34] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 out. 2022. Art. 5.º, inciso XII.

[35] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Thomson Reuters, 2019. p. 17.

[36] Os dados genéticos são considerados sensíveis, pois constituem informações acerca das características hereditárias dos indivíduos, obtidas por meio da análise de ácidos nucleicos e outras análises científicas, que levam à ideia de um "homem transparente" ou "de cristal". Acerca de dados genéticos, importante ressaltar que é a singularidade da informação genética que determina a necessidade de um tratamento específico desses dados. Para aprofundar o tema verificar: BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021. p. 184.

Insta registrar que a liberdade de disposição dos dados pessoais encontra limitação nos direitos da personalidade previstos na CF/88 em seu art. 5.º, X.[37] De acordo com Maria Helena Diniz[38], os direitos da personalidade são absolutos, intransmissíveis, indisponíveis, ilimitados, imprescritíveis e expropriáveis (inatos, adquiridos no instante da concepção e protegidos mesmo após o falecimento). Ainda no âmbito da Constituição Federal, tem-se a Emenda Constitucional n.º 115, de 10 de fevereiro de 2022, que alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais:

> Art. 1.º O caput do art. 5.º da Constituição Federal passa a vigorar acrescido do seguinte inciso LXXIX: [...]
> Art. 5.º. LXXIX - é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais[39].

A Constituição Federal, ao assegurar a proteção de dados pessoais como garantia fundamental, concedeu relevância à Lei Geral de Proteção de Dados, o que reforça o respeito à liberdade, intimidade e proteção de dados dos cidadãos brasileiros.

Na lição de Sarlet, a carga positiva deste direito fundamental "assegura à proteção de dados a condição de direito fundamental autônomo, com âmbito de proteção próprio", além de ser inquestionável a aplicação do regime constitucional ao direito fundamental em estudo, seja no seu sentido formal, seja no material.[40]

A LGPD ainda refere 10 princípios que, além de orientarem a aplicação das normas previstas no referido diploma legal, deverão nortear as atividades de

---

[37] "Art. 5.º - 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 à indenização pelo dano material ou moral decorrente de sua violação." (BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jan. 2022.)

[38] DINIZ, Maria Helena. **Curso de direito civil brasileiro**. 26. ed. São Paulo: Saraiva, 2010.p.88.

[39] BRASIL. **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/Emendas/Emc/emc115.htm. Acesso em: 2 ago. 2022.

[40] SARLET, Ingo. Fundamentos constitucionais: o direito à proteção de dados. In: DONEDA, Danilo *et al.* Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021, p. 37e 38.

tratamento de dados. Os agentes deverão, portanto, no âmbito de suas competências, formular regras de boas práticas e de governança que garantam aplicação dos referidos princípios no âmbito das ações organizacionais relativas ao tratamento de dados.[41]

A proteção de dados é vista como cidadania do novo milênio, pois resulta da soma de um conjunto de direitos, tendo se tornado uma ferramenta essencial para o livre desenvolvimento da personalidade.[42] Com o acelerado avanço tecnológico e a consolidação de espaços públicos virtuais, a gestão da informação sobre si própria tornou-se algo fundamental.

Ademais, a LGPD possui dois mecanismos institucionais de proteção de dados pessoais. O primeiro mecanismo é a instituição de agentes de proteção de dados pessoais, nas figuras do controlador e do operador, além da figura do encarregado pelo tratamento de dados pessoais. O segundo mecanismo é a criação de uma Autoridade Nacional de Proteção de Dados (ANPD) com a função principal de zelar pela proteção de dados pessoais por meio do exercício de competências normativa, deliberativa, fiscalizadora e sancionatória.[43]

Logo, revela-se impossível "cogitar de proteção integral à liberdade, à privacidade ao desenvolvimento da pessoa natural sem que se lhe garanta eficaz defesa e controle de seus próprios dados".[44] É por isso que, na LGPD, há expressa previsão de que a proteção conferida tem o objetivo de "proteger os direitos fundamentais da liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural"[45] (art. 1.º), premissa que deve orientar a interpretação de toda a LGPD.

Muito mais do que apenas impedir o acesso indesejado às informações pessoais, a LGPD preocupa-se também, conforme previsto em seu art. 2.º, inciso II, em manter a autodeterminação informativa como fundamento, a qual, embora não enunciada na Constituição Federal, pode ser visualizada no conjunto dos princípios e

---

[41] FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Thomson Reuters, 2019, p. 30-31.

[42] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p.11

[43] DEODATO, Sérgio. **A proteção dos dados pessoais de saúde**. Lisboa: Universidade Católica, 2017. p. 48.

[44] DONEDA, Danilo. **Manual de proteção de dados pessoais**. Brasília: SDE/DPDC, 2010.p.27

[45] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

dos seus outros direitos constitucionais expressos e nada mais é que ter a faculdade de o particular determinar e controlar a utilização dos seus dados pessoais.

Para que a LGPD seja efetivamente aplicada, é importante os programas de *Compliance,* que assumem esse papel. Pode-se definir o termo *Compliance* como "conjunto de ações a serem adotadas no ambiente corporativo para que se reforce anuência da empresa à legislação vigente, de modo a prevenir a ocorrência de infrações ou, já tendo ocorrido o ilícito, propiciar o imediato retorno a contexto de normalidade e legalidade".[46]

Uma vez que a LGPD possui diversos conceitos abertos que precisam ser contextualizados diante da realidade de cada agente econômico, do contexto social e econômico e do avanço tecnológico, é fundamental que, ao lado do papel da agência nacional de regulação, os agentes possam também ter a iniciativa de dar concretude aos preceitos legais, adaptando-se a sua realidade e aos esclarecimentos ditados pelo Estado.[47]

Estão expressamente estabelecidos na LGPD em seu artigo 2º os seguintes fundamentos:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.[48]

A LGPD está dividida em 10 capítulos e 65 artigos, sendo o Capítulo I dedicado às disposições gerais, em que são encontrados os princípios que fundamentam a proteção de dados pessoais (art. 2.º), o âmbito de aplicação territorial da lei (art. 3.º) e os conceitos básicos (art. 5.º). Entre os conceitos apresentados pela LGPD, destaca-

---

[46] FRAZÃO, Ana. Programas de *Compliance* e critérios de responsabilização de pessoas jurídicas por ilícitos administrativos. *In*: ROSSETTI, Maristela Abla; PITTA, André Grunspun. **Governança corporativa**: avanços e retrocessos. São Paulo. Quartier Latin, 2017. p. 42.

[47] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral De Proteção De Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.p.80

[48] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

se o de dados pessoais, que são informações relacionadas à pessoa natural identificada ou identificável (art. 5.º, I). Assim, a LGPD[49] protege não só a informação que identifica uma pessoa natural, mas também aquela que, cruzada com outras, permite a identificação da pessoa natural.

Há, ainda, os dados pessoais sensíveis, que são dados pessoais "sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou à 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". Titular dos dados, por sua vez, é pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.[50]

Já tratamento é qualquer ação que se faça com os dados pessoais ou os dados pessoais sensíveis. A LGPD aponta como tratamento

> [...] toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.[51]

No Capítulo II, são apresentados os requisitos para o tratamento de dados pessoais, dados pessoais sensíveis, dados pessoais de criança e de adolescente, bem como as hipóteses de término do tratamento de dados. Os direitos dos titulares são apresentados no Capítulo III, com a descrição dos prazos e das formas para o atendimento das requisições dos titulares.[52]

O Capítulo IV é dedicado ao tratamento de dados pessoais pelo Poder Público e à sua responsabilização em caso de infração à LGPD. O Capítulo V trata da

---

[49] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

[50] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 5.º, I e II.

[51] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. (art. 5.º, X).

[52] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 16/22.

transferência internacional de dados, e o Capítulo VI ocupa-se dos agentes de tratamento de dados pessoais, da responsabilidade dos agentes e do ressarcimento de danos. Os agentes de tratamento de dados pessoais são três: o controlador, o operador e o encarregado pelo tratamento de dados pessoais.[53]

Conforme os conceitos apresentados pela própria LGPD[54], o controlador é a "pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". Já o operador é a "pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador".[55]

O encarregado pelo tratamento de dados pessoais, por seu turno, é a "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)".[56]

O Capítulo VII cuida da segurança e das boas práticas a serem adotadas no tratamento de dados pessoais. O capítulo VIII trata da fiscalização da proteção de dados pessoais, com destaque para o rol de sanções administrativas que podem ser aplicadas pela ANPD.[57]

A Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal integrante da Presidência da República, e o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade são especificados no Capítulo IX. Por fim, o Capítulo X é dedicado às disposições finais e transitórias.[58]

---

[53] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 37/45.

[54] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 37/45.

[55] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 5.º, VII.

[56] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art.41.

[57] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 52/54.

[58] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais

Como visto, a Lei Geral de Proteção de Dados Pessoais apresenta conceitos, princípios e diretrizes para o tratamento de dados no Brasil e pontua os agentes de tratamento, orientando-os conforme suas funções. Incumbe à Agência Nacional de Proteção de Dados promover a aplicação da lei em comento, com padronização de diretivas e posicionamentos, além da fiscalização e aplicação de sanções quando justificadas.

Entretanto, para que o enquadramento à legislação seja considerado efetivo, não basta o simples cumprimento dos seus artigos, uma vez que, para efetivação dos seus princípios e diretrizes, mostra-se necessária a implementação de uma cultura de tratamento de dados, o que pode ser melhor obtido por meio de um Programa de *Compliance*. Esse programa deve prever não só o cumprimento às regras, mas também a sua aplicação dentro do contexto econômico-empresarial de forma preventiva e com promoção de políticas específicas, treinamentos e investigações.

A Lei Geral de Proteção de Dados Pessoais está atrelada não só à proteção da pessoa natural, mas também a aspectos econômicos e empresariais na medida em que não só se deve preservar o desenvolvimento individual, como também se deve permitir o desenvolvimento econômico e tecnológico, motivo pelo qual se passa, agora, à análise de tais questões.

2.3 ASPECTOS ECONÔMICOS E EMPRESARIAIS DA LGPD

A LGPD entrou em vigor em agosto de 2020 em meio à maior crise sanitária dos últimos cem anos, a qual causou impactos econômicos ainda imensuráveis, mas certamente enormes. Nesse contexto, a maioria das empresas lutam pela sobrevivência, especialmente os microempreendedores individuais e as micro e pequenas empresas.[59]

A LGPD criou a Autoridade Nacional de Proteção de Dados – ANPD, que é o órgão responsável pela supervisão da LGPD por elaborar as diretrizes para a Política

(LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 60/64**.**

[59] PINTO, Gabriel Nogueira Portella Nunes. LGPD e o impacto nas micro e pequenas empresas. **Revista Governança e *Compliance***, Rio de Janeiro, v. 4, n. 8, p. 16-17, abr. 2021. Disponível em: https://acrj.org.br/wp-content/uploads/2021/04/revista_governanca_*Compliance*_abr_2021_14_04.pdf. Acesso em: 7 jun. 2021.

Nacional de Proteção de Dados Pessoais e Privacidade e por promover a regulamentação dos setores que lidam com dados pessoais. Entre as funções da ANPD está a de coordenar ações com os órgãos e as entidades responsáveis por setores específicos da atividade econômica para promover o adequado funcionamento da LGPD, conforme as disposições regulamentares e a legislação.[60]

A par da sua inquestionável relevância da LGPD, independentemente do setor em que as empresas atuam, essa lei impõe adequação das atividades empresariais, devendo as organizações cumprir normas legais e regulamentares.

Algumas medidas de segurança da informação são capazes de promover, em agentes de tratamento de pequeno porte, um ambiente institucional mais seguro quanto ao tratamento de dados pessoais. Em relação a empresas de pequeno porte, a Agência Nacional de Proteção de Dados editou o guia orientativo de boas práticas, por meio do qual apresentou diretrizes voltadas, principalmente, à segurança da informação e ao aumento da confiança dos titulares de dados. Nesse documento, ressalta-se a importância da conscientização de funcionários e colaboradores por meio de treinamentos e campanhas, bem como por fomento à reflexão sobre obrigações e responsabilidades, de forma individual e conjunta, a respeito do tratamento de dados pessoais. O guia, ainda, sugere o repasse de algumas orientações aos funcionários, entre elas:

> [...] como utilizar controles de segurança dos sistemas de TI relacionados ao trabalho diário; como evitar de se tornarem vítimas de incidentes de segurança corriqueiros, tais como contaminação por vírus ou ataques de phishing, que podem ocorrer, por exemplo, ao clicar em links recebidos na forma de pop-up de ofertas promocionais ou em links desconhecidos que chegam por e-mail;
> [...] manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas; não compartilhar logins e senhas de acesso das estações de trabalho; bloquear os computadores quando se afastar das estações de trabalho, para evitar o acesso indevido de terceiros; seguir as orientações da política de segurança da informação.[61]

---

[60] CONFEDERAÇÃO NACIONAL DE SAÚDE. Código de Boas Práticas: proteção de dados para prestadores privados de serviços em saúde. [*S. l.: s. n.*], 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 02 set. 2022. p.4.

[61] BRASIL. Autoridade Nacional de Proteção de Dados. **Segurança da informação para agentes de tratamento de pequeno porte.** Brasília, DF: ANPD, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 2 ago. 2022. p. 7,

A ANPD ainda sugere que haja uma política de segurança da informação, tais como: cópias de segurança; uso de senhas; acesso à informação; compartilhamento de dados; atualização de *softwares*; uso de correio eletrônico; uso de antivírus; *etc*.

A disseminação da cultura de proteção dos dados entre os funcionários deve ser realizada mediante treinamentos e campanhas, por meio dos quais os funcionários serão orientados a incutir, no dia a dia, obrigações relacionadas ao tratamento de dados. Essas obrigações reforçarão pontos de controles de segurança, evitando, assim, que esses funcionários se tornem vítimas de incidentes, pois sabe-se que funcionários são as maiores vítimas de incidentes como contaminação por vírus ou ataques de *phishing*. Nesses treinamentos, os funcionários também serão orientados a manter documentos físicos que contenham dados pessoais dentro de gavetas, e não sobre as mesas, e a não compartilhar *logins* e senhas de acesso das estações de trabalho.[62] O objetivo desses treinamentos é fazer com que os agentes de pequeno porte sejam capazes de agir em conformidade e com boas práticas, alcançando assim o desenvolvimento de suas atividades em um ambiente mais seguro com o devido tratamento dos dados pessoais.

Há muitas indagações sobre a LGPD, afinal os dados pessoais, muitas vezes coletados de forma ilícita, sem a ciência e a autorização dos titulares, estão se tornando os novos insumos da nova economia, o que pode comprometer não apenas a privacidade dos usuários, mas também a identidade pessoal, a autodeterminação informativa, a liberdade, as oportunidades e perspectivas do presente e do futuro das pessoas e a própria democracia.

A referida lei trouxe importantes avanços, os quais implicarão significativas modificações para a atividade empresarial e para toda a sociedade. Estima-se que a total adaptação das empresas não será tarefa fácil, assim como não será simples resolver todos os problemas interpretativos que decorrem da LGPD. Na atualidade, os dados pessoais possuem enorme valor agregado e são estratégicos para ações comerciais e políticas mundo contemporâneo.[63]

9.

[62] PAIVA, Maria Teresa Pacheco Sampaio de. A Importância da Disseminação da Cultura da Proteção de Dados. **Âmbito Jurídico**, São Paulo, 1 maio 2022. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/a-importancia-da-disseminacao-da-cultura-da-protecao-de-dados-2/ Acesso em: 13 out. 2022.

[63] PINTO, Gabriel Nogueira Portella Nunes. LGPD e o impacto nas micro e pequenas empresas.

As instituições, tanto as públicas quanto as privadas, deverão se adequar à nova legislação, porquanto uma importante figura inserida pela LGPD é a previsão de sanções administrativas no caso de descumprimento da lei, as quais vão de advertência, multa até proibição das atividades:

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) 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 (cinquenta milhões de reais) por infração;
> III - multa diária, observado o limite total a que se refere o inciso II;
> IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;
> V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
> VI - eliminação dos dados pessoais a que se refere a infração;
> X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador. (Incluído pela Lei n.º 13.853, de 2019)
> XI- suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei n.º 13.853, de 2019)
> XII – proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei n.º 13.853, de 2019).[64]

Tendo como objetivo compreender de que maneira as organizações no Sul de Minas Gerais estavam se adaptando à nova legislação, estudo publicado em 2019 envolvendo sete instituições de diferentes áreas e portes concluiu que as integrantes da pesquisa, na maioria dos casos, desconheciam totalmente a existência da LGPD, sequer tendo conhecimento dessa. Na época dos estudos, os pesquisadores chegaram à conclusão de que as organizações necessitariam de enormes transformações no que tange à gestão dos negócios referente à própria segurança das informações. Dentre as inúmeras dificuldades encontradas, pode-se citar a

---

Revista Governança e *Compliance*, Rio de Janeiro, v. 4, n. 8, p. 16-17, abr. 2021. Disponível em: https://acrj.org.br/wp-content/uploads/2021/04/revista_governanca_*Compliance*_abr_2021_14_04.pdf. Acesso em: 7 jun. 2021.

[64] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 out. 2022. Art. 52.

ausência ou dificuldade de recursos tecnológicos e o total desconhecimento das boas práticas.[65]

Cumpre registrar que, em pesquisa realizada entre fevereiro e março de 2019 pela empresa Serasa Experian com um total de 1.564 pessoas, foi identificado que, para 75% delas, a LGPD é um tema desconhecido ou pouco conhecido. Já entre as 508 empresas pesquisadas nessa mesma pesquisa, 66% afirmaram que seu conhecimento sobre a lei é médio.[66]

As discussões acerca do assunto ora proposto ainda estão em âmbito teórico e preventivo, sendo necessário delimitar quais práticas efetivamente deverão ser seguidas – por exemplo, como melhorar a atuação das organizações, principalmente com a LGPD, e como as empresas irão atuar na privacidade dos dados pessoais. Entende-se nesse sentido, que a LGPD é de salutar relevância e deve ater-se também a área da saúde, a um tema que envolve, diretamente, a vida da população brasileira e seu direito à proteção de dados sensíveis por se tratar de dados de saúde.

No mundo corporativo, estar de acordo com o que determina a lei em todos os seus detalhes, etapas e processos recebe o nome de *Compliance.* Para evitar futuras consequências jurídicas, as empresas devem se antecipar para se adequarem às determinações legais de proteção de dados. As empresas que entendem e já adotaram o conceito de *Compliance* têm vantagens práticas em relação ao cumprimento da LGPD, assunto que será tratado nos próximos capítulos.

2.4 TRATAMENTO DE DADOS SENSÍVEIS

Procede-se à análise dos dados referentes à saúde da pessoa. Esses dados são denominados sensíveis, e isso significa que devem ser amplamente protegidos, inclusive para que sejam banidas atitudes de caráter discriminatório e lesivo. Nesse

---

[65] PIURCOSKY, Fabrício Peloso *et al*. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma neg**., Bogotá, v. 10, n. 23, p. 89-99, dez. Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2215-910X2019000300089&lng=en&nrm=iso. Acesso em: 5 maio 2022.

[66] O QUE os consumidores e as empresas sabem sobre LGPD e o que estão fazendo a respeito?. **Serasa experian**, São Paulo, 16 jul. 2019. Disponível em: https://www.serasaexperian.com.br/conteudos/protecao-de-dados/pesquisa-o-que-os-consumidores-e-as-empresas-sabem-sobre-lgpd-e-o-que-estao-fazendo-a-respeito/. Acesso em: 25 out. 2022.

sentido, serão analisados os conceitos de dados pessoais e dados sensíveis pela GDPR (General Data Protection Regulation) e pela LGPD e os princípios que legitimam as bases autorizadoras.

Há um grande estudo sobre o que são dados pessoais e, entre eles, quais seriam dados sensíveis e de que forma podem ser utilizados – se haveria alguma flexibilidade de uso ou se essas informações são blindadas e não podem ser utilizadas para nenhuma finalidade sem autorização do seu titular.

Nas palavras de Stefano Rodotà, “os dados sensíveis abrangem informações que, caso sejam conhecidas e processadas, podem ser utilizadas de forma discriminatória ou particularmente lesiva e que apresentaria maiores riscos potenciais que a média, para a pessoa e até mesmo para uma coletividade”.[67]

Não há dúvidas de que “tais benesses não vieram desacompanhadas de perigos, que se manifestam claramente, quando se pensa na maior facilidade para se violar a privacidade e a imagem alheias, bem como nos direitos de monitorar quem monitora, de deletar dados pessoais e de proteger a identidade online, aspectos esses que devem ser tutelados como pilares de garantia da eficácia do direito fundamental à privacidade em sentido amplo.”[68]

Segundo Doneda, “o paradigma inicial para uma reflexão doutrinária partiu justamente da reação a estes projetos, para logo depois fundamentar as primeiras iniciativas legislativas na matéria”[69]. Os projetos a que Doneda se refere são os

[67] RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 11.

[68] COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Violação dos direitos de personalidade no meio ambiente digital: a influência da jurisprudência europeia na fixação da jurisdição/competência dos tribunais brasileiros. **Civilistica.com,** Rio de Janeiro, v. 8, n. 1, 2019. Disponível em: http://civilistica.com/violacao-dos-direitos-de-personalidade/. Acesso em: 5 set. 2022. p. 9.

[69] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 205.

criados pelo governo, como os do “National Data Center”[70] ou o “SAFARI”[71].

'A partir de 1970, surgiram várias normas que visavam à tutela dos dados pessoais. A doutrina classificou com a “primeira geração” de leis de proteção de dados as seguintes leis: a Hessisches Datenschutzgesetz (Lei de Proteção de Dados Hessiana), em 1970; a Data Legen 289 (ou Datalag), em 1973, na Suécia; e o Privacy Act, nos Estados Unidos da América, em 1974."[72]

Ocorre que, com o avanço tecnológico, três gerações de leis restaram atrofiadas, e com isso surgiu a “quarta geração” em matéria de proteção de dados. Na quarta geração, incluem-se as normas trazidas pela Carta dos Direitos Fundamentais da União Europeia[73], bem como a Diretiva 95/46/EC, que tratou especificamente da proteção de dados pessoais.[74]

Sem incorrer no equívoco da “Convenção para Proteção dos Indivíduos com Respeito ao Processamento Automático de Dados Pessoais”, que havia entrado em vigor em 1985, e seguindo a mesma linha das “Diretrizes sobre proteção da

---

[70] A ideia de formar um centro de dados nacional (National Data Center) surgiu na década de 1960, quando cientistas sociais norte-americanos sentiram a necessidade de obter maior acesso a microdados mantidos pelo governo federal. Como resultado, em 1965, recomendaram que o governo federal desenvolvesse um Data Center nacional que armazenasse e disponibilizasse aos pesquisadores os dados coletados por várias agências estatísticas, recomendação feita através de relatório do Comitê sobre a Preservação e Uso de Dados Econômicos para o Conselho de Pesquisa em Ciências Sociais, conhecido como “Relatório Ruggles”. Vide, sobretudo: KRAUS, R. S. **Statistical Déjà Vu**: The National Data Center Proposal of 1965 and Its Descendants. Miami: [*s. n.*], 2011. Disponível em: https://www.census.gov/history/pdf/kraus-natdatacenter.pdf. Acesso em: 29 jun. 2022. E também: RUGGLES, R. *et al.* **Report of the Committee on the Preservation and Use of Economic Data (1965)**. [*S. l.: s. n.*]. Disponível em: https://ia800200.us.archive.org/31/items/ReportOfTheCommitteeOnThePre servationAndUseOfEconomicData1965/Ruggles_econdata_1965.pdf. Acesso em: 29 jun. 2022.

[71] SAFARI, sigla de sistema automatizado para arquivos administrativos e o diretório de indivíduos (Système Automatisé Pour Les Fichiers Administratifs Et Le Répertoire Des Individus), foi criado em 1974, na França, com o mesmo intento do National Data Center norte-americano. O sistema envolvia a criação de um banco de dados centralizado da população, usando o arquivo da previdência social como o identificador comum de todos os arquivos administrativos. Confrontado com o clamor generalizado provocado por esse projeto, o jornal *Le Monde* publicou matéria intitulada “SAFARI, ou caça aos franceses”. Isso levou a uma forte oposição popular, levando o governo a criar a Comissão Nacional de Informática e Liberdades. O projeto SAFARI, lançado durante a presidência de Georges Pompidou, não viu a luz do dia. Vide, sobretudo: SAFARI. **La chasse aux Français 40 ans après**. [*S. l.*], 2018. Disponível em: https://donneesouvertes.info/2018/01/26/safari-la-chasse-aux-francais-40-ans-apres. Acesso em: 29 jun. 2022.

[72] SIMITIS, S. Il contesto giuridico e político della tutela della privacy. **Rivista Critica del Diritto Privato**, [*s. l.*], 1997. p. 565-566.

[73] Carta dos Direitos Fundamentais da União Europeia. https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 22 nov. 2022.

[74] REINALDO FILHO, Demócrito. A Diretiva Europeia sobre a proteção de dados pessoais. **Jus Navigandi**, Teresina, 6 fev. 2013. Disponível em: https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais. Acesso em: 12 set. 2022.

privacidade e o fluxo transnacional de informações pessoais", publicada pela OECD no início dos anos 1980, a Diretiva 95/46/EC[75] trouxe, no seu art. 2.º, uma série de conceitos e princípios.[76]

Consta, no art. 2.º da referida Diretiva, que dado pessoal é "qualquer informação relativa a uma pessoa singular identificada ou identificável"[77], o que nos permite concluir que alcança não somente informações textuais, mas também fotografias, imagens audiovisuais, registros de sons e tudo o mais que puder identificar uma pessoa, estando ela viva ou não, sem que se retirem desses aspectos as suas características de direitos autônomos também.[78]

Em face do avanço tecnológico desses 20 anos, a Diretiva 95/46/EC também se tornou obsoleta e foi substituída pelo novo regulamento geral de proteção de dados (GDPR – General Data Protection Regulation) em 25/05/2018. Após inúmeros casos que chegaram ao Parlamento Europeu e ao Conselho Europeu, verificou-se a necessidade de regras mais rígidas para regulamentar a proteção de dados dos cidadãos.[79]

Assim, a GDPR trouxe inúmeras inovações ao expandir a concepção anterior constante da Diretiva 95/46/EC acrescentando outras definições. Com relação aos dados pessoais, a GDPR dispõe:

> Dados pessoais: informações relativas a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular.[80]

---

[75] Diretiva 95/46/EC. https://www.conjur.com.br/dl/diretiva-europeia.pdf. Acesso em 22 nov. 2022.

[76] MONTEIRO, António Pinto. A proteção do consumidor em Portugal e na União Europeia: o olhar de um europeu. *In:* INSTITUTO ÍTALO-IBERO-BRASILEIRO DE ESTUDOS JURÍDICOS. [*S. l., s. n.*], 12 jul. 2022. Disponível em: https://institutoiib.org/protecao-do-consumidor/. Acesso em: 11 set. 2022.

[77] Diretiva 95/46/EC. https://www.conjur.com.br/dl/diretiva-europeia.pdf. Acesso em 22 nov. 2022.

[78] FACHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à Privacidade e Novas Tecnologias: Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa. **Revista Internacional Consinter de Direito**, [*s. l.*], n. 7, p. 19-40, 2.º semestre de 2018. p. 30.

[79] PARLAMENTO EUROPEU. **Directiva 95/46/CE, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial, Luxemburgo, n.º L 281 de 23/11/1995 p. 0031 – 0050. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046. Acesso em: 21 jun. 2022.

[80] EUROPEAN UNION. Regulamento (UE) 2016/679, de 27 de abril de 2016. General Data Protection

Também digno de destaque é o disposto no art. 10, que se refere ao tratamento de categorias especiais de dados pessoais, isto é, aos chamados dados sensíveis:

> O tratamento de dados pessoais que revelem a origem racial ou étnica, as opiniões políticas, as convicções religiosas ou filosóficas, a filiação sindical, o tratamento de dados genéticos, dados biométricos destinados a identificar uma pessoa singular de forma inequívoca, dados relativos à saúde ou dados relativos à vida sexual ou à orientação sexual, só é autorizado se for estritamente necessário, se estiver sujeito a garantias adequadas dos direitos e liberdades do titular dos dados, e se: a. For autorizado pelo direito da União ou de um Estado-Membro; Direito à Privacidade e Novas Tecnologias b. Se destinar a proteger os interesses vitais do titular dos dados ou de outra pessoa singular; ou c. Estiver relacionado com dados manifestamente tornados públicos pelo titular dos dados [...].[81]

Percebe-se, aqui nessa diretiva, que o legislador já trata os dados atinentes à saúde como dados pessoais sensíveis, considera sua respectiva e poderosa importância no domínio dos tratamentos e se preocupa com a sua constante proteção. Portanto, tratando-se de dados sensíveis, as regras são ainda mais rigorosas, uma vez que se destina à tutela das características essenciais da pessoa humana.[82]

Quanto ao tratamento de dados, a GDPR apoiou os seguintes princípios: “(i) licitude, lealdade e transparência; (ii) limitação das finalidades; (iii) minimização dos dados; (iv) exatidão; (v) limitação do prazo de conservação; (vi) integridade e confidencialidade; e, por fim, (vii) responsabilidade.” (artigo 5.º)[83]

A GDPR introduziu mecanismos de certificação e marcas de proteção de dados, permitindo que os titulares dos dados avaliem rapidamente o nível de proteção de dados empregado pelos produtos e serviços em questão. Uma lista de organizações certificadas estará, portanto, disponível publicamente. Códigos de conduta e mecanismos de certificação aprovados também ajudarão os controladores

---

Regulation. **Official Journal of the European Union**, Brussels, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL. Acesso em: 22 jun. 2022. Art. 4.º.

[81] EUROPEAN UNION. Regulamento (UE) 2016/679, de 27 de abril de 2016. General Data Protection Regulation. **Official Journal of the European Union**, Brussels, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL. Acesso em: 22 jun. 2022. Art. 10.º.

[82] KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da lei n.º 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 460.

[83] UNIÃO EUROPEIA. **Regulamento Geral de Proteção de Dados da União Europeia.** Disponível em:. https://gdpr-info.eu/. Acesso em: 22 nov. 2022.

a identificar os riscos relacionados ao seu tipo de processamento e a aderir às melhores práticas.[84]

Assim, a GDPR deu novas diretivas em relação ao regulamento de 95/46/EC, que previu a necessidade rígida de proteger os dados dos titulares com o intuito de gerar segurança jurídica e segurança prática nesse mercado que passou a fomentar o desenvolvimento da economia digital de pequenas, médias e grandes empresas, trazendo obrigações, responsabilidades e sanções.

Em matéria de dados pessoais, a Lei Geral de Proteção de Dados (LGPD), sob o n.º 13.709 de 2018, vem como importante regulação a ser aplicada em produtos e serviços que utilizam inteligência artificial, bem como na concepção, no desenvolvimento e na execução de suas atividades. A confiança está diretamente ligada à eticidade, concretizada pelo princípio da boa-fé objetiva. E tal fato se confirma na própria redação do dispositivo legal, que reúne o *framework* principiológico em matéria de proteção de dados pessoais, na medida em que a boa-fé está enunciada no cabeçalho do artigo 6.º da LGPD: “As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios.”[85]

Conforme artigo 6.º da LGPD (Lei 13.709/2018), estão previstos, a referida lei, 10 princípios, os quais têm como foco legitimar as bases legais para se realizar o tratamento de dados. São eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização.

Porém, para dados pessoais sensíveis, esse rol é bem mais restritivo, uma vez que se está diante de dados de cunho íntimo, que podem apresentar potencial discriminatório. Por esse motivo, seu tratamento só é permitido quando há coleta de consentimento do titular ou, ainda, quando essa coleta é enquadrada nas alíneas do artigo 11, inciso II, da LGPD:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:

---

[84] COUTINHO, Francisco Pereira; MONIZ, Graça Canto (coord.). **Anuário da proteção de dados**. Lisboa: CEDIS, 2019. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2019/06/anuario-da-protecao-de-dados-2019.pdf. Acesso em: 7 jul. 2021. p. 22.

[85] COLOMBO, Cristiano; GOULART, Guilherme Damasio. Inteligência artificial aplicada a perfis e publicidade comportamental: proteção de dados pessoais e novas posturas em matéria de discriminação abusiva. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CERQUEIRA, Joaquim Portes de. (org.). **Inteligência artificial aplicada ao processo de tomada de decisões**. São Paulo: D'Plácido, 2020. p. 293.

> I- quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
> II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei n.° 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9.° desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.[86]

Nos termos do artigo 5.º, inciso II, da Lei Geral de Proteção de Dados Pessoais[87], dados referentes à saúde dos titulares são considerados dados pessoais sensíveis.[88]

A escolha das hipóteses autorizadoras deve ser pautada nas particularidades do controlador, no seu ramo de atuação e nos objetivos de tratamento. Sugere-se, desde logo, a realização de mapeamento para que sejam verificadas as necessidades, as finalidades e os interesses do controlador, cuja análise é imprescindível para a implementação correta da LGPD.[89] A finalidade de mapear

---

[86] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Grifo nosso.

[87] "Art. 5.º. Para os fins desta Lei, considera-se: [...] II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural. [...]" (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.)

[88] "A grande inovação que a LGPD operou no ordenamento jurídico brasileiro pode ser compreendida na instituição de um modelo *ex ante* de proteção de dados, baseado no conceito de que não existem mais dados irrelevantes diante do processo eletrônico e ubíquo de dados na sociedade da informação." (MENDES, Laura Schertel Ferreira; DONEDA, Danilo César Maganhoto. Comentário à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da Proteção de Dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 555-587, nov./dez. 2018.

[89] GUIA de Boas Práticas - Lei Geral de Proteção de Dados (LGPD). *In:* BRASIL. **Governo Digital**. [Brasília, 2020]. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-

dados sensíveis auxiliará a identificar quais controles de segurança devem ser adotados na proteção dessas informações.

Em todos os casos, optando o controlador pelo tratamento de dados pessoais sensíveis pautado no consentimento, faz-se necessário o cumprimento de todos os requisitos legais elencados no artigo 8.º da Lei 13.709/2018.[90] Incumbe ao controlador comprovar que a coleta do consentimento se deu conforme as determinações legais, de forme livre, informada e inequívoca, para uma finalidade determinada.[91]

Sempre que possível, esses dados pessoais sensíveis devem ser anonimizados, conforme preceitua o artigo 16 da LGPD, pelas empresas para a preservação do indivíduo e, consequentemente, para proteção de sua vida ou da sua incolumidade física ou de terceiros envolvidos.[92]

O consentimento deverá ser fornecido livremente pelo titular por escrito ou por outro meio que demonstre sua manifestação de vontade, por meio de uma atitude assertiva. Em caso de coleta de consentimento por meio de instrumento contratual, as cláusulas de tratamento deverão ser apresentadas de forma destacada. Ainda, o consentimento deverá apresentar finalidades específicas e determinadas, sendo vedada a autorização genérica de tratamento, sob pena de nulidade. Havendo alteração de finalidade, o titular deve ser imediatamente informado. Quanto ao prazo,

---

dados/guias/guia_lgpd.pdf. p. 22. Acesso em: 31 ago. 2020.

[90] "Art. 8.º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.
§ 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais.
§ 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.
§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.
§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas.
§ 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.
§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 9º desta Lei, o controlador deverá informar ao titular, com destaque de forma específica do teor das alterações, podendo o titular, nos casos em que o seu consentimento é exigido, revogá-lo caso discorde da alteração." (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.).

[91] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 4.º.

[92] CARLOTO, Selma. Manual Prático de Adequação à LGPD: Com enfoque nas relações de trabalho. (2021).: LTr Editora.p.13.

a legislação não apresenta validade específica. Em contrapartida, permite a revogação do consentimento, pelo titular, a qualquer tempo, mediante procedimento gratuito e facilitado, podendo o último, ainda, solicitar sua eliminação.[93]

Em relação à tutela de saúde, recorte dado no presente estudo, a análise da hipótese autorizadora contida na alínea “f”, inciso II, do artigo 11, também merece melhor destaque. Com efeito, é permitido o tratamento de dados pessoais sensíveis para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Sendo assim, médicos, hospitais e clínicas podem, em uma primeira análise, utilizar esse permissivo para o exercício de suas atividades.

Conforme já mencionado, é imprescindível a análise das particularidades de cada caso antes da escolha da base autorizadora para tratamento. Todavia, a Lei Geral de Proteção de Dados Pessoais é clara ao autorizar o tratamento de dados pessoais sensíveis para a tutela de saúde sem obrigatoriedade de coleta de consentimento.[94]

O consentimento, desde que manifestado de forma livre, informada e inequívoca e ainda que seja apresentado como a principal base, apresenta inúmeros desafios, pois não é simples provar que foi lido de forma livre e inequívoca. Termos escritos de forma clara e direta, acessados rapidamente e facilmente, ainda assim, podem não ser lidos.

Sem a necessidade de consentimento, são possíveis as bases previstas no artigo 11 da Lei 13.709/2018, como o cumprimento de obrigação legal ou regulatória, que seria inexistente se não fosse feito o tratamento do dado; tratamento compartilhado para que sejam executadas políticas públicas previstas em lei ou regulamento para realização de pesquisa para exercício regular de direitos; para proteção da vida ou tutela da saúde, realizada por profissional de saúde; e garantia da prevenção à fraude.[95]

---

[93] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 8º, parágrafo 5º.

[94] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 7.º, VIII.

[95] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em:

Fins econômicos possuem ressalva legal específica, exceto quando houver pedido de portabilidade pelo titular e para prestação de serviços de saúde, de assistência farmacêutica e de assistência de saúde, sempre em benefício do titular. Seleção de riscos em cálculo de plano de saúde está expressamente vedada. Mesmo a privacidade, a confidencialidade e a integridade já sendo centrais à saúde, a LGPD trouxe benefícios e graus de proteção ainda maiores.[96]

A LGPD permite que o caminho do dado que está sendo utilizado seja percorrido, eis que o titular pode pedir relatório de impacto, conforme previsto na lei, o qual deve conter como a empresa teve acesso aos dados, quando e com quem os compartilhou e como os tratou, podendo ainda o titular exigir que os dados sejam alterados, corrigidos e até mesmo apagados ou bloqueados de forma total ou parcial.

Assim, a proteção de dados aplicada à área da saúde merece melhor atenção, uma vez que envolve majoritariamente o tratamento de dados sensíveis, cujo tratamento é diferenciado e demanda maior cautela por parte dos agentes de tratamento.

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 11, II, f, g.

[96] CARLINI, Angélica; SAAVEDRA, Giovani Agostini. ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 113.

3 PRIVACIDADE E PROTEÇÃO DE DADOS NA ÁREA DA SAÚDE

O maior patrimônio que uma empresa possui, na era da sociedade da informação e do conhecimento, são os dados pessoais, os quais podem se tornar ativos ou passivos de uma empresa dependendo da forma como são tratados. Desse modo, neste capítulo, será apresentado um breve panorama geral sobre o conceito de dados e privacidade, sobre como os dados serão aplicados em favor da saúde e sobre quais são seus regulamentos. Ao final, será abordado o tema de *Compliance* na área da saúde, o qual é especialmente importante nos dias atuais, em que os serviços de saúde são exigidos em seu grau máximo.

A privacidade, já tratada no capítulo anterior, merece várias abordagens, haja vista que o direito à privacidade permite afastar a interferência alheia sobre a vida íntima de cada um. Em uma sociedade contemporânea, com aumento exponencial do fluxo de dados, o "direito à privacidade deve se propor a algo mais que àquela finalidade inicial restrita à proteção da vida íntima".[97] Ele deve abarcar também o direito da pessoa humana de controlar o uso e a coleta dos seus dados pessoais, ainda mais quando são dados sensíveis. Assim, o direito à privacidade abrange não apenas a vida íntima das pessoas, mas também a proteção de seus dados pessoais.

Nessa perspectiva, é crucial que se tenha em mente, em que pese a proteção de dados seja sempre atrelada ao direito de privacidade, o âmbito de proteção é bem mais amplo, porquanto, abarca todos os dados que dizem respeito a uma pessoa, podendo ser em diversas esferas da vida: íntima, privada, familiar, social).[98]

Dados coletados de modo autorizado ou não podem guiar decisões e ações estratégicas para construir perfis de consumidores, de segurados e assim por diante. Logo, é preciso proteger dados de pessoas naturais que são acessados pelas empresas, sejam os titulares pacientes, terceiros, fornecedores ou funcionários. Essa ação encontra respaldo na LGPD.

Embora atual e coerente, não é fácil de essa proteção ser implementada, pois requer um trabalho atento aos detalhes, uma análise rigorosa de riscos e a criação de

---

[97] SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014. p. 137.

[98] BARZOTTO, Luciane Cardoso; COSTA, Ricardo H. Martins (org.). *Estudos sobre a Lei Geral de Proteção de Dados*: doutrina e aplicabilidade no âmbito laboral. Porto Alegre: Tribunal Regional do Trabalho, 2022.

políticas específicas, com fiscalização constante, especialmente dos dados de saúde, considerados pela lei como dados pessoais sensíveis.

Interessante notar que a LGPD não traz um conceito de saúde, assim como ocorre na GDPR a LGPD faz menção tão somente aos conceitos de “dado pessoal” e “dado pessoal sensível”. Assim, a definição do conceito de “dados de saúde” é possível a partir da legislação europeia, qual seja:

> [...] todos os dados relativos ao estado de saúde de um titular de dados que revelem informações sobre a sua saúde física ou mental no passado, no presente ou no futuro. Inclui informações sobre a pessoa singular recolhidas durante a inscrição para a prestação de serviços de saúde, ou durante essa prestação.[99]

Dados, se não protegidos adequadamente, podem se tornar um passivo perigoso e não somente um dado jurídico, mas também econômico-financeiro e reputacional, afinal nenhuma instituição de saúde gostaria de ver sua imagem alinhada com desrespeito aos direitos dos pacientes.[100]

Trazer transparência para o uso de dados ajuda a proteger a sociedade, obstando que sejam realizadas condutas inadequadas com os dados. Mesmo com todos os cuidados, a LGPD reserva ainda mais proteção a um grupo específico de dados, aqueles que receberam a denominação "sensíveis". Dentro dessa categoria, de acordo com a LGPD existem os dados de caráter religioso, filosófico, político, racial/étnico, de opinião política, genético, biométrico e todos aqueles referentes à saúde.

Dentro dessa categoria, de acordo com a lei, existem os dados de caráter religioso, filosófico, político, racial/étnico, de opinião política, genético, biométrico e todos aqueles referentes à saúde. Especificamente na prática médica, tem o Ato Médico[101], que é absoluto em repetir sobre a confidencialidade e a relação de confiança entre médico e paciente.[102]

---

[99] MENDES, Laura Schertel *et al.* (coord.). **Proteção de dados para prestadores privados em saúde**. [*S. l.*]: Confederação Nacional de Saúde, 2021.p.46.

[100] CARLINI, Angélica; SAAVEDRA, Giovani Agostini. ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 112.

[101] BRASIL. **Lei n.º 12.842, de 10 de julho de 2013**. Dispõe sobre o exercício da Medicina. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12842.htm. Acesso em: 20 jun. 2022.

[102] PRIVACY. *In:* STANFORD Encyclopedia of Philosophy Archive. [*S. l.*], Spring 2018. Disponível em: https://plato.stanford.edu/archives/spr2018/entries/privacy/. Acesso em: 20 jun. 2022.

O armazenamento, o manuseio e a transmissão de dados digitais têm acentuado a necessidade de proteção de dados, seja por empresas privadas ou por entes públicos. Deve haver uma transformação cultural para que qualquer empresa esteja em conformidade com a LGPD. Faz-se necessário assimilar que os titulares dos dados pessoais possuem soberania e autonomia para decidir. Além disso, deve ser garantido ao titular que todos os seus direitos poderão ser executados caso seja essa a sua vontade, sendo importante fundamentar, de forma sólida e estruturada, todos os tratamentos de dados existentes em bases legais, afinal, hoje em dia, dados são como chaves que exigem especial proteção, sob pena de ameaçarem a intimidade, a privacidade e os demais direitos humanos.

Todas essas ações devem penetrar em todos os funcionários, terceiros, pacientes, médicos e fornecedores. A transparência e a ética, essenciais ao *Compliance,* permeiam os elementos da LGPD.

A área da saúde é a única área da vida das pessoas que ainda permaneceu altamente sensível e privada. Porém, dados constantes em exames, consultas, diagnósticos e outros são geralmente amplamente compartilhados, sendo que, na maioria das vezes, o paciente não tem conhecimento sobre como essas informações são coletadas, armazenadas, distribuídas ou divulgadas.

Por isso, são importantes os mecanismos para proteção dos dados pessoais tratados dentro da área da saúde, pois poderão acarretar passivos para as empresas em caso de descumprimento da Lei Geral de Proteção de Dados, devendo os dados pessoais, serem tratada como direito fundamental, instrumento de proteção à vida privada e à intimidade, que são objetos tanto da Constituição Federal[103] quanto do Código Civil (Arts. 11 ao 21).[104]

3.1 APLICAÇÃO EM FAVOR DA SAÚDE

Nos termos do artigo 196 da Constituição Federal[105], a saúde é direito de todos

---

[103] BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988. https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 22 nov. 2022.

[104] BRASIL. Lei n. 10.406, de 10 de Janeiro de 2002. Dispõe sobre Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 22 nov. 2022.

[105] BRASIL. **Constituição (1988). Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988. https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 22 nov. 2022. Art. 196.

e dever do Estado, devendo ser garantida por meio de políticas sociais e econômicas que visem à redução do risco de doença e de outros agravos e ao acesso universal e igualitário a ações e serviços para sua promoção, proteção e recuperação.

No âmbito doutrinário, a Organização Mundial de Saúde (OMS) definiu saúde como “um estado de completo bem-estar físico, mental e social e não somente ausência de afecções e enfermidades”.[106] A saúde, é um direito fundamental, reafirmado pela Lei n.º 8.080/90, que dispõe sobre as condições para promoção, proteção e recuperação da saúde.[107]

Na área da saúde, no mínimo a relação é triangular, pois envolve um profissional da área da saúde, plano da saúde ou seguro saúde, hospital, e até a pessoa chegar a resolver o problema, os dados de saúde dessa pessoa já passaram por muitas outras pessoas. Os dados pessoais de saúde versam sobre condições clínicas de pessoa natural identificada ou identificável e incluem prontuários, receituários, atestados, resultados de exames e demais diagnósticos, uso de biometria para identificação de paciente (em substituição da carteira do plano), etc. Referidos dados apresentam potencial discriminatório na medida em que, a título de exemplificação, um indivíduo pode sofrer rejeição por ser portador de doença sexualmente transmissível ou de alguma condição psiquiátrica. Por esse motivo, a proteção de dados — amplamente relacionada com os conceitos de privacidade e intimidade — deve ser reforçada em relação a esse tipo de dado. [108]

Assim, quando um dado é classificado como sensível, há a necessidade de garantias reforçadas de proteção. A título exemplificativo, esse tipo de proteção “refere-se à vedação ao seu acesso, bem como o tratamento em arquivos automatizados, sem que haja o consentimento do sujeito”.[109]

A exemplo do prontuário médico, os direitos aos dados do prontuário são do paciente, porém quem o gera é o médico, ficando a guarda do referido documento

---

[106] MARQUES, Antônio Jorge de Souza *et al.* **Direito à saúde, cobertura universal e integralidade possível**. [*S. l.: s. n.*], 2016. Disponível em: https://www.almg.gov.br/export/sites/default/acompanhe/eventos/hotsites/2016/encontro_internacional_saude/documentos/textos_referencia/00_palavra_dos_organizadores.pdf. Acesso em: 3 set. 2022.

[107] BRASIL. **Lei n.º 8.080, de 19 de setembro de 1990**. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 14 jun. 2022.

[108] PINHEIRO, Patrícia Peck. **Direito Digital.** São Paulo: Saraiva Educação, 2021. p. 370-376.

[109] BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021. p. 100.

com os agentes da saúde. No entanto, é só um paciente precisar do seu prontuário que a batalha judicicial começa. Os dados constantes nos prontuários são extremamentes sigilosos e sensíveis. Assim, de que forma um banco de dados seria utilizado? Há muitos intresses divergentes na área da saúde e, por isso, ela acaba sendo uma área muito delicada. A saúde digital confere muitos benefícios para médicos e pacientes, porém há que se ter capacitação para que sejam preservadas a segurança e a privacidade dos dados dos pacientes, dados esses que deveriam ter nível de acesso controlado e restrito.[110]

Tudo isso é um desafio para o setor da saúde, pois demandará treinamento a fim de capacitar profissionais para o uso de computadores e envolverá uma questão de mudança de cultura, eis que na área da saúde o vazamento de dados pode ocorrer em diversos momentos, pois a cadeia de pessoas envolvidas é extensa.

Outro aspecto diz respeito à privacidade. Os dados de saúde de uma pessoa são extremamente sigilosos e sensíveis, visto o grau de impacto que podem causar. A Constituição Federal não faz distinção entre os conceitos de privacidade e intimidade. Na doutrina, a privacidade pode ser compreendida como a tipificação dos direitos de personalidade, estando amplamente relacionada com a dignidade da pessoa humana:

> O direito à privacidade é considerado como “tipificação dos direitos da personalidade, que são inerentes ao próprio homem e têm por objetivo resguardar a dignidade da pessoa humana. Surgem como uma reação à teoria estatal sobre o indivíduo e encontram guarida em documentos como a Declaração dos Direitos do Homem e do Cidadão, de 1789, a Declaração Universal dos Direitos do Homem, de 1948 (art. 12), a 9.ª Conferência Internacional Americana, de 1948 (art. 5.º), a Convenção Europeia dos Direitos do Homem, de 1950 (art. 8.º), a Convenção Panamericana dos Direitos do Homem, de 1959, a Conferência Nórdica sobre o Direito à Intimidade, de 1967, além de outros documentos internacionais. Vale ressaltar que a matéria é objeto tanto da Constituição Federal de 1988 quanto do Código Civil brasileiro de 2002 (arts. 11 ao 21), o que provocou o seu tratamento mais aprofundado e amplo pela doutrina nacional”.[111]

Apesar de serem inter-relacionados, o conceito de privacidade não se confunde com o conceito de dados pessoais. Para as finalidades deste trabalho, será utilizado

---

[110] PINHEIRO, Patrícia P. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018. p. 372.

[111] DIREITO à privacidade., *In:* ENCICLOPÉDIA Jurídica da PUCSP. São Paulo, 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 23 jun. 2022. Cap. 1.

o conceito de privacidade defendido pelo jus-filósofo italiano Stefano Rodotà, qual seja "o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir sua própria esfera particular".[112]

Com relação ao conceito de proteção de dados pessoais, será utilizado o enquadramento teórico de Danilo Doneda, que define a proteção de dados pessoais como uma garantia de caráter instrumental derivada da tutela da privacidade, mas que não se limita por essa, fazendo referência a todo o leque de garantias fundamentais que se encontram no ordenamento brasileiro.[113]

No relatório elaborado para a Escola Nacional de Defesa do Consumidor, assim restou pontuado sobre a proteção de dados pessoais:

> A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantêm uma ligação concreta e viva com a pessoa titular destes dados. Os dados pessoais são a pessoa e, portanto, como tal devem ser tratados, justificando o recurso ao instrumental jurídico destinado à tutela da pessoa e afastando a utilização de um regime de livre apropriação e disposição contratual destes dados que não leve em conta seu caráter personalíssimo. Também destas suas características específicas deriva a consideração que, hoje, diversos ordenamentos jurídicos realizam, de que a proteção de dados pessoais é um direito fundamental — uma verdadeira chave para efetivar a liberdade da pessoa nos meandros da Sociedade da Informação.[114]

Os dispositivos da IoT (Internet of Things), ao coletarem uma quantidade imensa de dados referentes a incontáveis aspectos da vida dos usuários, os colocam em um novo patamar de riscos,[115] sobretudo porque a lei brasileira de proteção de dados pessoais (Lei n.º 13.709/18) ainda é recente.

Em tempos de COVID-19, muitos dados pessoais estão sendo coletados de

---

[112] RODOTÀ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.p.57

[113] DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.p. 323.

[114] MAGRANI, Eduardo. **Entre Dados e Robôs**: Ética e Privacidade na Era da Hiperconectividade. [*S. l.*]: Arquipelago Editorial, 2019. (Pautas Em Direito Vol. 5). p. 57.

[115] BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Brasília: SDE/DPDC, 2010. p. 61.

forma incontrolável e sem limite com justificativas de que serviriam para prevenir surtos e de que seriam essenciais na identificação e resposta a futuras epidemias, municiando autoridades públicas de saúde com informações.[116]

Nessa linha, a Inteligência Artificial vem ganhando espaço cada vez maior, inclusive com a coleta de dados de interpretações de exames e de dados clínicos, já possibilitando a busca de informações pessoais de pacientes, de reações a medicamentos, de tempo de internação, de dados genéticos. A partir de um número grande de dados, os algoritmos são utilizados por meio de processos de gestão a partir da Inteligência Artificial[117], gerando protocolos e metodologias de operações em hospitais, apontando diagnósticos e medidas terapêuticas, além de medidas de prevenção para novas contaminações.[118]

No setor de saúde, em face ao perigo de contágio, no período da pandemia, as pessoas passaram a utilizar mais websites e aplicativos, muitos dos quais já tomam conhecimento de medidas preliminares antes mesmo do atendimento presencial físico, no caso de a pessoa estar infectada. Sendo que essas alterações, podem ser transitórias ou permanentes.

Registre-se, ainda, que, em 20 de março de 2020, a Portaria n.º 467 de 2020, do Ministério da Saúde, dispôs sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência, reduzindo ainda mais o deslocamento geográfico ao hospital de referência pelos

---

[116] GALVANI, Nathalia. Google anuncia plataforma de coleta de dados em tempo real sobre a COVID-19. **Estado de Minas**, [*s. l.*], 26 fev. 2021. Tecnologia. Disponível em: https://www.em.com.br/app/noticia/tecnologia/2021/02/26/interna_tecnologia,1241263/google-anuncia-plataforma-de-coleta-de-dados-em-tempo-real-sobre-a-covid-19.shtml. Acesso em: 22 jun. 2022.

[117] No âmbito do direito brasileiro, cumpre assinalar que tramita, no Congresso Nacional, o Projeto de Lei n.º 21/20, que estabelece diretrizes para o desenvolvimento de Inteligência Artificial (AI) no Brasil. Em seu art. 2.º, conceitua AI como um sistema baseado em processo computacional que, "a partir de um conjunto de objetivos definidos por humanos, pode, por meio do processamento de dados e de informações, aprender a perceber e a interpretar o ambiente externo, bem como a interagir com ele, fazendo predições, recomendações, classificações ou decisões". Cumpre assinalar que não será abordado o tema da Inteligência Artificial nesse estudo. (BRASIL. **Projeto de Lei n.º 21/2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Brasília: Senado Federal, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 15 ago. 2022.)

[118] COLOMBO, Cristiano ; ENGELMANN, W. Inteligência Artificial em favor da saúde: proteção de dados pessoais e critérios de tratamento em tempos de pandemia. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CÈSAR, Joaquim Portes de Cerqueira (org.). **Inteligência Artificial aplicada ao processo de tomada de decisões**. Belo Horizonte: Editora D'Plácido, 2020. v. 1. p. 229.

pacientes.[119]

> Tais práticas se revelam positivas, representando redução da demanda fisica em clínicas e hospitais, sendo a comunicação mediada pela internet, contudo, neste modelo, os usuários fornecem seus dados pessoais, ficando submetidos aos cookies, conhecidos como "testemunhas de conexão", onde são identificados os usuários e a geolocalização, ou mesmo, como *trade off* preenchendo cadastros pela oferta dos serviços.[120]

Em todo o mundo, a situação emergencial vivida com a COVID-19 virou pretexto para acesso, coleta e tratamento de dados pessoais de forma indiscriminada. No entanto, isso não pode resultar na utilização desses dados sem quaisquer limites. Os exemplos acerca do tratamento de dados pessoais de forma inadequada, pela administração pública, em alguns casos, são pitorescos, como é o caso da indonésia Sita Tyasutami, que declarou à BBC News: "O presidente revelou meu diagnóstico de covid-19 ao vivo na TV".[121] Widodo, governante da Indonésia, não revelou o nome da paciente, todavia referiu a sua idade (31) e a de sua mãe (64). Ele também divulgou que elas estavam em um hospital de Jacarta e descreveu com detalhes seu perfil, seus sintomas e a exata evolução de seu histórico de contatos, que originaram seu contágio. Sita, que assistia à televisão, no hospital, enquanto estava aguardando o resultado do exame, ficou incrédula, com raiva e confusa.

Outro exemplo, relacionado especificamente a farmácias e drogarias, é o da informação do número do CPF. A principal situação em que isso ocorre no Brasil é a da exigência do CPF para a realização de compras em farmácias e drogarias (muitas vezes, para a obtenção de um desconto ou uma promoção). Ao relacionar o CPF de uma pessoa às compras de medicamentos e outros produtos ou serviços relacionados

---

[119] BRASIL. Ministério da Saúde. **Portaria n.º 467, de 20 de março de 2020**. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3.º da Lei n.º 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19. Brasília, DF: Gabinete do Ministro, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/Portaria/PRT/Portaria%20n%C2%BA%20467-20-ms.htm. Acesso em: 22 jun. 2022.

[120] COLOMBO, Cristiano; ENGELMANN, W. Inteligência Artificial em favor da saúde: proteção de dados pessoais e critérios de tratamento em tempos de pandemia. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CÈSAR, Joaquim Portes de Cerqueira (org.). **Inteligência Artificial aplicada ao processo de tomada de decisões**. Belo Horizonte: Editora D'Plácido, 2020. v. 1. p. 231.

[121] NEVETT, Joshua. Coronavírus: o presidente revelou meu diagnóstico de covid-19 ao vivo na TV. **BBC**, São Paulo, 6 maio 2020. Disponível em: https://www.bbc.com/portuguese/internacional-52561909. Acesso em: 22 jun. 2022. [Não paginado].

à sua saúde, esse dado passa a ser enquadrado no conceito dedado pessoal sensível, conforme o art. 5º, II, da LGPD. A informação do número do CPF deve ter uma base legal. Por envolver um dado pessoal, que se torna sensível nesse caso, a sua coleta deve ter prioritariamente o consentimento do titular (art. 11, I, da LGPD).

Para Helena Nissenbaum:

> In a health care context, for example, patients expect their physicians to keep personal medical information confidential, yet they accept that it might be shared with specialists as needed. Patients' expectations would be breached and they would likely be shocked and dismayed if they learned that their physicians had sold the information to a marketing company. In this event, we would say that informational norms for the health care context had been violated.[122]

Logo, muitas medidas de segurança administrativas de dados pessoais devem ser adotadas por médicos, que são controladores de dados. Porém, o estabelecimento dessas políticas de segurança vai depender de cada atuação médica, a fim de que seja verificado quais instrumentos devem ser utilizados para que tanto esses profissionais quanto *os que propiciam um sistema de Compliance de dados pessoais* se adaptem à LGPD*.*

Aconselha-se que profissionais da área da saúde formulem suas regras de boas práticas e de governança de dados de acordo com sua atividade, sua estrutura, sua finalidade e riscos envolvidos, tendo em vista a imposição de sanções administrativas em caso de não utilização dessas regras (art. 50 e 52 da LGPD).[123]

Assim, nasce a necessidade de o médico-controlador obter o consentimento livre e esclarecido do paciente para um fim específico, com exceção aos art. 7.º, 8.º e 11 da LGPD, que envolvem tutela da saúde, sendo de grande importância a implantação de um sistema de governança e *Compliance* digital.[124]

---

[122] "Em um contexto de cuidados de saúde, por exemplo, os pacientes esperam que seus médicos mantenham suas informações médicas confidenciais, ainda que aceitem que elas possam ser compartilhadas com especialistas conforme necessário. As expectativas dos pacientes seriam violadas, e eles provavelmente ficariam consternados se soubessem que os médicos venderam suas informações para uma empresa de marketing. Neste caso, diríamos que normas informativas para o contexto assistencial haviam sido violadas." (NISSENBAUM, Helen. **Privacy in Context Technology, Policy, and the Integrity of Social Life**. [*S. l.*]: Stanford Law Books, 2009. p. 33, tradução nossa.)

[123] CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance* e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 1122-1123.

[124] CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance* e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 1124.

De todo modo, dados pessoais relacionados à área da saúde necessitam de ampla proteção, razão pela qual, na próxima seção abordam-se as principais regulamentações na área da saúde.

3.2 ESTRUTURA DA SAÚDE E PRINCIPAIS REGULAMENTAÇÕES NA ÁREA DA SAÚDE

A LGPD é uma lei transversal e, como tal, tem que aproximar todos os setores. Desse modo, se faz imprescindível analisar, em síntese, a estrutura da saúde no Brasil.

A área da saúde representa 9,6% do PIB do Brasil dentro da estrutura econômica do país (dados de 2019)[125] – o famoso "primo pobre" da economia. O Brasil gasta em saúde 9,2% do PIB (soma de todas as riquezas produzidas), um pouco acima da média dos 37 países-membros da OCDE, os quais, na sua maioria ricos, gastam 8,8% do seu PIB. No caso do Brasil, boa parte dessas despesas são privadas. A fatia dos recursos públicos investidos nessa área representa apenas 4% do PIB, enquanto na média da organização ela é de 6,6% do PIB.[126]

Em 2019, a maior concentração de hospitais privados ocorre nas regiões Sudeste, Nordeste e Sul, mais especificamente nos estados de São Paulo (859 hospitais), de Minas Gerais (543 hospitais), da Bahia (352 hospitais), do Paraná (331 hospitais), do Rio de Janeiro (310 hospitais) e do Rio Grande do Sul (294 hospitais).[127]

De acordo com estudo feito, o número de médicos no Brasil, em 2016, era de 2,1 médicos para cada mil habitantes[128], por sua vez o número de médicos cresce mais que o da população.

Ademais, com relação ao mercado farmacêutico, segundo dados apresentados

---

[125] Agência Brasil. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2022-04/ibge-despesas-com-saude-chegaram-r-7114-bilhoes-em-2019. Acesso em 22 de nov. 2022.

[126] FERNANDES, Daniela. Pandemia evidencia que Brasil gasta pouco e mal em saúde pública, diz diretor da OCDE. **UOL**, São Paulo, 24 jul. 2020. Disponível em: https://economia.uol.com.br/noticias/bbc/2020/07/24/pandemia-evidencia-que-brasil-gasta-mal-em-saude-publica-diz-diretor-da-ocde.htm. Acesso em: 4 nov. 2021.

[127] FEDERAÇÃO BRASILEIRA DE HOSPITAIS. **Cenário dos hospitais no Brasil 2019**. [*S. l.: s. n.*], 2019. Disponível em: http://cnsaude.org.br/wp-content/uploads/2019/05/CenarioDosHospitaisNoBrasil2019CNSaudeFBH.pdf. Acesso em: 4 nov. 2021.

[128] WORLD BANK WDI 2.12 - Health Systems. *In:* KAGGLE. [*S. l.*], 2020. Disponível em: https://www.kaggle.com/danevans/world-bank-wdi-212-health-systems. Acesso em: 4 nov. 2021.

no Abradimex Conecta 2020-2021[129], o Brasil está entre os países com maior demanda de medicamentos do mundo. Em 2019, alcançava a 10.ª posição no *ranking* mundial, demonstrando alto consumo de medicamentos pelos brasileiros.[130]

No setor público, onde está 75% da população, estão as pessoas que não possuem plano de saúde e que, portanto, serão atendidas pelo SUS. O governo federal faz, nesse setor, um pequeno investimento de 3,8% do PIB, ou seja, aproximadamente R$ 123 bilhões são destinados pelo Governo Federal para a área da saúde pública.[131]

Os problemas da saúde no Brasil já se arrastam por muitos anos, tais como: distorções sistêmicas, inflação médica, concorrência, produtividade e balança comercial. A respeito das distorções sistêmicas, há os desvios, uso do dinheiro que deveria ir para a área da saúde, mas que acaba não sendo utilizado nessa esfera, e, ainda, as alocações ineficientes, em que a verba é mal utilizada.[132]

No SUS, tem-se problemas como tabelas de valores de exames, procedimentos e consultas defasadas, má aplicação dos recursos, com desperdícios e desvios, atenção primária precária, concentração em grandes centros, número excessivo de hospitais atuando no mesmo nível de complexidade, acesso limitado de novas tecnologias (cirurgias por vídeo, por exemplo, o SUS não paga) e corte de verbas parlamentares.[133]

Para resolver esses problemas relacionados à área da saúde, é necessária uma revisão de toda a política de saúde pública, com centralização regional de especialidades, atenção primária focada – por exemplo, a saúde da família –, mudança do modelo atual de distribuição de verbas, parcerias público-privadas (PPP),

---

[129] Disponível em: https://www.abradimex.com.br/index.php?option=com_k2&view=item&id=148:os-6-pa%C3%ADses-que-mais-consomem-medicamentos-no-mundo&Itemid=141. Acesso em 22 de nov. 2022.

[130] BRASIL. Consumo de medicamentos: Um autocuidado perigoso. **Conselho Nacional de Saúde**, Brasília, s.d. Disponível em: http://www.conselho.saude.gov.br/ultimas_noticias/2005/medicamentos.htmAcesso em: 4 nov. 2021.

[131] VERDÉLIO, Andreia. Brasil gasta 3,8% do PIB em saúde pública. **Agência Brasil**, Brasília, 1 nov. 2018. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2018-11/brasil-gasta-38-do-pib-em-saude-publica. Acesso em: 4 nov. 2021.

[132] BRASIL. Câmara dos Deputados. Saúde pública no Brasil ainda sofre com recursos insuficientes. **Agência Câmara de Notícias**, Brasília, 8 jan. 2015. Disponível em: https://www.camara.leg.br/noticias/448436-saude-publica-no-brasil-ainda-sofre-com-recursos-insuficientes/. Acesso em: 9 fev. 2022.n.p.

[133] BRASIL. Ministério da Saúde. **Transformação digital para o SUS**. Disponível em: https://datasus.saude.gov.br/. Acesso em: 8 nov. 2021.

adesão a novas tecnologias sedimentadas (VP), revisão da tabela SUS, integração de dados paciente/sistema público e privado, criação de modelos focados em pacientes crônicos e idosos, avaliação da qualidade de serviços e ampliação da formação de profissionais em todas as áreas da saúde, ou seja, é necessário melhorar a qualidade dos profissionais que estão à frente da área da saúde.[134]

A Constituição Federal traz, na Seção II, os artigos de 196, até 200 que tratam sobre garantias da saúde. Especificamente, o artigo 196 retrata que a saúde é direito de todos, sendo dever do Estado garanti-lo por meio de políticas sociais e econômicas que visam a reduzir o risco de doenças e outros agravos, tais como ter alimentação, condições de viver e habitar, emprego, acesso à educação, condições de higiene, *etc*. Por fim, e não menos importante, é um direito que deve ser promovido de uma forma universal.[135]

No artigo 197, diz que cabe ao Poder Público sobre a regulamentação e fiscalização o controle dessas ações, devendo ocorrer de maneira regionalizada e hierarquizada (art.198). O artigo 199 da CF[136] prevê a participação da iniciativa privada.[137]

A Lei 8.080, de 19 de setembro de 1990, dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Também dispõe sobre a vigilância sanitária a que ficam sujeitos os medicamentos, as drogas, os insumos farmacêuticos e correlatos, cosméticos, saneantes e outros produtos, e dá outras providências.[138] Assim, a referida lei traz os objetivos do Sistema Único de Saúde – SUS.

---

[134] GIOVANELLA, Ligia *et al.* Saúde da família: limites e possibilidades para uma abordagem integral de atenção primária à saúde no Brasil. **Ciência da Saúde Coletiva**, [*s. l.*], v. 14, n. 3, jun. 2009. Disponível em: https://www.scielo.br/j/csc/a/XLjsqcLYxFDf8Y6ktM4Gs3G/?lang=pt. Acesso em: 14 jun. 2022.

[135] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jan. 2022. Art. 196.

[136] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jan. 2022. Art. 199.

[137] BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jan. 2022.

[138] BRASIL. **Lei n.º 8.080, de 19 de setembro de 1990**. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 14 jun. 2022.

A Lei 8.080/90 traz o que cabe em nível Federal, Estadual e Municipal em ações de saúde, conforme quadro a seguir:

Quadro 1 – Competências normativas

Esfera de governo	Formulação de políticas e planejamento	Financiamento	Regulação, coordenação, controle e avaliação	Execução direta de serviços
Federal	• Identificação de problemas e definição de prioridades no âmbito nacional. • Papel estratégico e normativo. • Manutenção da unicidade, respeitando a diversidade. • Busca da equidade. • Apoio e incentivo para o fortalecimento institucional e de práticas inovadoras de gestão estadual e municipal. • Planejamento e desenvolvimento de políticas estratégicas nos campos de tecnologias, insumos e recursos humanos.	• Garantia de recursos estáveis e suficientes para o setor saúde. • Peso importante dos recursos federais. • Papel redistributivo. • Definição de prioridades nacionais e critérios de investimentos e alocação entre áreas da política e entre regiões/estados. • Realização de investimentos para redução de desigualdades. • Busca da equidade na alocação de recursos.	• Regulação de sistemas estaduais. • Coordenação de redes de referência de caráter interestadual/nacional. • Apoio à articulação interestadual. • Regulação da incorporação e uso de tecnologias em saúde. • Normas de regulação sanitária no plano nacional. • Regulação de mercados em saúde (planos privados, insumos). • Regulação das políticas de recursos humanos em saúde. • Coordenação dos sistemas nacionais de informações em saúde. • Avaliação dos resultados das políticas nacionais e do desempenho dos sistemas estaduais.	• Em caráter de exceção. • Em áreas/ações estratégicas.
Esfera de governo	**Formulação de políticas e planejamento**	**Financiamento**	**Regulação, coordenação, controle e avaliação**	**Execução direta de serviços**
Estadual	• Identificação de problemas e definição de prioridades no âmbito estadual. • Promoção da regionalização. • Estímulo à programação integrada. • Apoio e incentivo ao fortalecimento institucional das secretarias municipais de saúde.	• Definição de prioridades estaduais. • Garantia de alocação de recursos próprios. • Definição de critérios claros de alocação de recursos federais e estaduais entre áreas da política e entre municípios. • Realização de investimentos para redução de desigualdades. • Busca da equidade na alocação de recursos.	• Regulação de sistemas municipais. • Coordenação de redes de referência de caráter intermunicipal. • Apoio à articulação intermunicipal. • Coordenação da PPI no estado. • Implantação de mecanismos de regulação da assistência (ex.: centrais, protocolos). • Regulação sanitária (nos casos pertinentes). • Avaliação dos resultados das políticas estaduais. • Avaliação do desempenho dos sistemas municipais.	• Em caráter de exceção. • Em áreas estratégicas: serviços assistenciais de referência estadual/ regional, ações de maior complexidade de vigilância epidemiológica ou sanitária. • Em situações de carência de serviços e de omissão do gestor municipal.
Esfera de governo	**Formulação de políticas e planejamento**	**Financiamento**	**Regulação, coordenação, controle e avaliação**	**Execução direta de serviços**

Municipal	• Identificação de problemas e definição de prioridades no âmbito municipal. • Planejamento de ações e serviços necessários nos diversos campos. • Organização da oferta de ações e serviços públicos e contratação de privados (caso necessário).	• Garantia de aplicação de recursos próprios. • Critérios claros de aplicação de recursos federais, estaduais e municipais. • Realização de investimentos no âmbito municipal.	• Organização das portas de entrada do sistema. • Estabelecimento de fluxos de referência. • Integração da rede de serviços. • Articulação com outros municípios para referências. • Regulação e avaliação dos prestadores públicos e privados. • Regulação sanitária (nos casos pertinentes). • Avaliação dos resultados das políticas municipais.	• Peso importante na execução de ações/ prestação direta de serviços assistenciais, de vigilância epidemiológica e sanitária. • Gerência de unidades de saúde. • Contratação, administração e capacitação de profissionais de saúde.

Fonte: A autora, 2022.

A Lei Orgânica de Saúde – Lei Federal n.º 8.080 de 1990 (Brasil, 1990) – define que a direção do SUS é única em cada esfera de governo e estabelece como órgãos responsáveis pelo desenvolvimento das funções de competência do Poder Executivo na área de saúde:[139]

1. Ministério da Saúde, no âmbito nacional;
2. As secretarias de saúde, no âmbito estadual;
3. As secretarias de saúde, no âmbito municipal.

Assim, mais do que um administrador, o gestor do SUS é a “autoridade sanitária”, em cada esfera de governo, cuja ação política e técnica deve estar pautada pelos princípios da reforma sanitária brasileira. O gestor de saúde tem duas dimensões indissociáveis da atuação dos gestores da saúde: política e técnica.[140]

A existência dessas dimensões ajuda a compreender a complexidade e os dilemas no exercício dessa função pública de autoridade sanitária, bem como a natureza dessa atuação e as possíveis tensões relativas à direcionalidade da política de saúde em um dado governo e ao longo do tempo.

Em primeiro lugar, cabe lembrar que o cargo de ministro ou de secretário de saúde tem significado político importante. Seu ocupante é designado pelo chefe do

---

[139] BRASIL. **Lei n.º 8.080, de 19 de setembro de 1990**. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 14 jun. 2022. Art. 9.º, I, II, III.

[140] SER gestor municipal do SUS. [*S. l.: s. n.*], abr. 2021. Disponível em: https://gestaosus.suprema.edu.br/ser-gestor-sus.pdf. s.n. Acesso em: 13 set. 2022.

Executivo, democraticamente eleito em cada esfera do governo (presidente, governador ou prefeito).[141]

Isso situa o gestor da saúde como integrante de uma equipe que tem responsabilidade por determinado “projeto de governo” e que terá de dar respostas ao chefe político em cada esfera e interagir com outros órgãos de governo. Por outro lado, a autoridade sanitária tem a responsabilidade de conduzir as políticas de saúde segundo as determinações constitucionais e legais do SUS, as quais constituem um dado modelo de política de Estado para a saúde que não se encerra no período de um governo.[142]

A interação projeto de governo e política de Estado setorial tem de ser considerada na reflexão sobre a atuação dos gestores do SUS, visto que, muitas vezes, essa interação pode expressar tensões que influenciam a possibilidade de continuidade e consolidação das políticas públicas de saúde.[143]

Ainda se tem as seguintes leis de regulamentações:

Lei 6.360, de 23 de setembro de 1976: dispõe sobre a vigilância sanitária a que ficam sujeitos os medicamentos, as drogas, os insumos farmacêuticos e correlatos, cosméticos, saneantes e outros produtos, e dá outras providências.[144]

Lei 9.782, de 26 de janeiro de 1999: define o Sistema Nacional de Vigilância Sanitária. Cria a Agência Nacional de Vigilância Sanitária e dá outras providências.[145]

Lei 9.961, de 28 de janeiro de 2000: cria a Agência Nacional de Saúde Suplementar e dá outras providências.[146]

---

[141] JANKAVSKI, André. Novo ministro da Saúde é escolhido: quanto essas trocas afetam a economia?. **CNN Brasil**, Brasília, 16 mar. 2021. n.p. Disponível em: https://www.cnnbrasil.com.br/business/novo-ministro-da-saude-e-escolhido-quanto-essas-trocas-afetam-a-economia/. Acesso em: 13 set. 2022.

[142] BRASIL. Ministério da Saúde. *In:* PORTAL brasileiro de dados abertos. Brasília, [2022]. Disponível em: https://dados.gov.br/organization/about/ministerio-da-saude-ms. Acesso em: 13 set. 2022.

[143] MACHADO, Cristiani Vieira; LIMA, Luciana Dias de; BAPTISTA, Tatiana Wargas de Faria. Princípios organizativos e instâncias de gestão do SUS. *In:* QUALIFICAÇÃO de gestores do SUS. [*S. l.: s. n.*]. p. 47-72. Disponível em: http://www5.ensp.fiocruz.br/biblioteca/dados/txt_339793983.pdf. Acesso em: 19 nov. 2021.

[144] BRASIL. **Lei n.º 6.360, de 23 de setembro de 1976**. Dispõe sobre a vigilância sanitária a que ficam sujeitos os medicamentos, as drogas, os insumos farmacêuticos e correlatos, cosméticos, saneantes e outros produtos, e dá outras providências. Brasília, DF: Presidência da República, 1976. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6360.htm. Acesso em: 1 dez. 2021.

[145] BRASIL. **Lei n.º 9.782, de 26 de janeiro de 1999**. Define o Sistema Nacional de Vigilância Sanitária, cria a Agência Nacional de Vigilância Sanitária e dá outras providências. Brasília, DF: Presidência da República, 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9782.htm. Acesso em: 1 dez. 2021.

[146] BRASIL. **Lei n.º 9.961, de 28 de janeiro de 2000**. Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências. Brasília, DF: Presidência da República, 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9961.htm. Acesso em: 1 dez. 2021.

A respeito das relações institucionais e governamentais, tem-se:

> O ato de reivindicar, por diferentes grupos da sociedade, pressupõe pluralidade de interesses econômicos, políticos, sociais, culturais e étnicos. [...] As atividades de lobby são uma delas.[147]

Sobre a definição de *lobby*/*advocacy* pode-se dizer que:

> "É toda atividade organizada, exercida dentro da lei e da ética, por um grupo de interesses definidos e legítimos, com o objetivo de ser ouvido pelo poder público para informá-lo e dele obter determinadas medidas, decisões, atitudes. [...] O lobbying é o processo pelo qual os grupos de pressão buscam participar do processo estatal de tomada de decisões, contribuindo para a elaboração das políticas públicas de cada país".148

No sistema de saúde brasileiro, existem os atores (*players*), que participam todos os dias das relações institucionais e governamentais. A cadeia de *stakeholders* da saúde suplementar é extensa e envolve, como afirmam Camarinha, Costa e Vieira, grupos ou pessoas cujos interesses podem afetar ou ser afetados por uma organização.[149] Assim, os atores do sistema de saúde brasileiro, por exemplo, são: pacientes, profissionais da saúde, Estado (representado pelo SUS), hospitais privados, beneficentes e santas casas, operadoras de planos de saúde, cooperativas, indústrias (farmacêutica, dispositivos médicos), poder Executivo (Ministérios, Agências e Autarquias), Poder Legislativo (Câmara, Senado, TCU), Poder Judiciário (TJs, Ministério Público, STJ/STF), sociedades médicas (conselhos federais e regionais, órgãos de classe), *etc.*[150]

Embora o conceito de gestão da cadeia de suprimentos seja relativamente recente, o gerenciamento de cadeias de suprimentos existe desde um longo período

---

[147] FARHAT, Saïd. **Lobby**: o que é, como se faz - ética e transparência junto a governos. São Paulo: Aberje, 2007. p. 69.

[148] OLIVEIRA, Andréa Cristina de Jesus. Breve histórico sobre o desenvolvimento do lobbying no Brasil. **Revista de Informação Legislativa**, Brasília, v. 42, n. 168, p. 29-43, out. 2005. Disponível em: https://pergamum.tjrs.jus.br/pergamumweb/vinculos/00000d/00000d2e.pdf. Acesso em: 2 ago. 2022.

[149] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. n.p.

[150] COSTA, Márcio Roberto; TORRES JÚNIOR, Noel. Gestão da Cadeia de Suprimentos de Serviços: uma análise das atividades operacionais logísticas de empresas exibidoras de filmes de longa-metragem de Belo Horizonte. **Gestão da Produção, Operações e Sistemas**, Bauru, Ano 9, n. 3, p. 61-78, jul./set. 2014. Disponível em: https://revista.feb.unesp.br/index.php/gepros/article/viewFile/1050/589. Acesso em: 28 jun. 2020.

de tempo na história econômica da humanidade, visto que sempre existiram demandas por produtos. Essas demandas geram um conjunto de atividades e processos para que os insumos sejam adquiridos e transformados em bens que serão transportados e entregues ao consumidor final. No entanto, foi apenas nas últimas décadas que começou a ser enfatizada a importância da gestão da cadeia de suprimentos como um meio para a redução de custos e melhoria do nível de serviços. Tornou-se corrente a acepção de que uma gestão eficaz e eficiente da cadeia de suprimentos traz uma série de benefícios para as organizações.[151] Apesar do crescente interesse pelo tema, existe uma grande variedade de definições e de problemas na sua conceituação. Os diversos conceitos existentes foram desenvolvidos e aplicados às indústrias de transformação. Portanto, esses não são amplamente consistentes com as características dos serviços, e isso impõe a necessidade de reconceituar a gestão da cadeia de suprimentos, tendo-se em conta o setor de serviços e suas especificidades[152]

[151] BALLOU, Ronald H. **Gerenciamento da Cadeia de Suprimentos/Logística Empresarial.** São Paulo: Bookman, 2006. n.p.

[152] BALTACIOGLU *et al.,* 2007 *apud.* COSTA, Márcio Roberto; TORRES JÚNIOR, Noel. Gestão da Cadeia de Suprimentos de Serviços: uma análise das atividades operacionais logísticas de empresas exibidoras de filmes de longa-metragem de Belo Horizonte. **Gestão da Produção, Operações e Sistemas**, Bauru, Ano 9, n. 3, p. 61-78, jul./set. 2014. Disponível em: https://revista.feb.unesp.br/index.php/gepros/article/viewFile/1050/589. Acesso em: 28 jun. 2020.

3.3 PROGRAMAS DE *COMPLIANCE* NA AREA DA SAÚDE

O termo *Compliance* deriva da expressão em inglês *"to comply"*, que significa "cumprir" ou, de forma mais ampla, "conformidade", em relação a leis, normas, regulamentos, entre outros. Nessa linha de pensamento, ensina Block que estar em conformidade é o dever de cumprir e fazer cumprir regulamentos internos e externos impostos às atividades de uma instituição de forma a expressar que as normas internas são cumpridas de forma ética, conferindo idoneidade às atitudes humanas. Equivale a conhecer as normas da organização, seguir os procedimentos recomendados, agir em conformidade e sentir o quanto são fundamentais a ética e a idoneidade em todas as atitudes humanas e empresariais.[153]

A área da saúde é conhecida por muitos escândalos de problemas que já existiram – por exemplo, a máfia das próteses.[154] Assim, essa área precisa se defender e mostrar que tem práticas de mercado adequadas para garantir benefício ao paciente e ao consumidor final, dependendo do produto. Foi a partir da máfia das próteses que os planos de saúde e seguradoras começaram a criar procedimentos para evitar fraudes, acabando assim que os dados das pessoas são mais compartilhados.

É fundamental que os agentes econômicos se adaptem à nova realidade por meio de um sistema de gestão de *Compliance* com a certificação da ISO 37301[155]. Sob essa perspectiva, percebem-se diversas vantagens atribuídas aos programas de *Compliance.* São elas: (i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento e auxilia na prevenção do ilícito; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; (iv) servir potencialmente como atenuante no caso de punições administrativas. Podem-se enumerar, ainda,

---

[153] BLOCK, Marcella. ***Compliance* e Governança Corporativa.** Rio de Janeiro: Freitas Bastos, 2017. p.67.

[154] BRASIL. Câmara dos Deputados. **CPI – Máfia das órteses e próteses no Brasil**. Brasília, DF: Câmara dos Deputados, 2015. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-mafia-das-orteses-e-proteses-no-brasil. Acesso em: 13 set. 2022. n.p.

[155] Certificação ISO 37301 – Sistema de Gestão de Compliance Disponível em: https://www.qmsbrasil.com.br/blog/certificacao-iso-37301-sistemas-de-gestao-de-compliance-3/. Acesso em 22 de nov. 2022.

benefícios, mesmo que indiretos, no tocante ao desenvolvimento em qualidade e inovação, além de incremento na reputação.[156]

Para que as vantagens acima enumeradas sejam efetivas e materializadas, é necessário um programa de *Compliance* efetivo, e não de fachada, ainda que penalidades maiores podem ocorrer caso não haja nem um programa apenas no papel. Um programa mal concebido, que não envolva suficientemente as lideranças corporativas ou que careça do suporte financeiro para seu regular desempenho, dissemina entre os funcionários a ideia de que o programa é um embuste.[157]

Desse modo, existem elementos mínimos para a estruturação de um programa de *Compliance* efetivo, quais sejam: (i) avaliação contínua de riscos e atualização do programa; (ii) elaboração de Códigos de Ética e Conduta; (iii) organização compatível com o risco da atividade; (iv) compromisso da alta administração; (v) autonomia e independência do setor de *Compliance*; (vi) treinamentos periódicos; (vii) criação de uma cultura corporativa de respeito à ética e às leis; (viii) monitoramento constante dos controles e processos, inclusive para fins de atualização de programas; (ix) canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes; (x) detecção, apuração e punição de condutas contrárias ao programa de *Compliance.*[158] O *Compliance* assume importante papel a fim de rever as condutas estabelecidas para o cumprimento de outras normas. Por exemplo, as normas trabalhistas deverão estar em conformidade com a LGPD, evitando-se a coleta de dados desnecessários dos empregados, entre outras situações, a fim de obstar um uso de dados que possa ser considerado discriminatório.[159]

Para as empresas que já possuem um programa de *Compliance* será mais fácil. As que não o possuem, no entanto, terão que se adaptar diante da sua realidade. O primeiro passo será fazer um projeto de planejamento da adequação da empresa em conformidade com a LGPD. Posteriormente, é necessária a formalização de um *assessment* (avaliação sobre quais ações já foram feitas e o que precisa ser feito para

---

[156] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral De Proteção De Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 677- 710.

[157] BASRI, Carole. **Corporate *Compliance***. North Carolina: Carolina Academic Press, 2017. *E-book.*

[158] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral De Proteção De Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.p.711-718

[159] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral De Proteção De Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019.p.719-780.

estar em conformidade plena com a LGPD). Por fim, é preciso treinamento dos colaboradores para sua conscientização geral e engajamento. Também é indispensável que o controlador indique o encarregado pelo tratamento de dados. Esse encarregado atuará como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.[160]

A LGPD busca estimular: a aplicação de seus dispositivos em caráter preventivo, ou seja, exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de *Compliance* digital; investimento; atualização de ferramentas de segurança de dados; revisão documental; melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria; e, acima de tudo, mudança de cultura.[161]

A formação de um comitê gestor de proteção de dados pessoais é uma estratégia essencial para o cumprimento da Lei n.º 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). Esse comitê deverá ser formado por uma equipe multidisciplinar, composta por funcionários, diretores e gestores que cumulam as suas atividades ordinárias com aquelas do comitê. O comitê será responsável pela avaliação dos mecanismos de tratamento e proteção dos dados existentes e pela proposição de ações voltadas ao seu aperfeiçoamento.

Por fim, deverá constar claramente, no sítio do controlador, todos os dados para contato, conforme previsão legal do artigo 41, §1.º, da LGPD: "A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador."[162]

Os riscos de *Compliance*, quando não mitigados, mas sim materializados, trazem consequências negativas, que nem sempre são fáceis de se mensurar por se tratarem também de ativos intangíveis.[163]

---

[160] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 5, VIII.

[161] PINHEIRO, Patrícia P. **Proteção de dados pessoais**: comentários à lei n. 13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.152 p.

[162] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

[163] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 44.

4 A PROTEÇÃO DE DADOS APLICADA AOS PROGRAMAS DE *COMPLIANCE* E GOVERNANÇA CORPORATIVA

No presente capítulo, o objetivo será introduzir os elementos principais dos alicerces da governança corporativa na área da saúde e abordar a necessidade da realização da avaliação de riscos, bem como a importância de mapeá-los. Esses objetivos serão direcionados, especificamente, para a área da saúde, em que há muitos riscos – por exemplo, em um hospital, os riscos são inúmeros, tendo em vista a cadeia de pessoas e colaboradores envolvidos que acessam os dados dos pacientes. Visto que o objeto deste estudo também são os riscos relacionados aos dados pessoais, o enfoque será nessa particularidade. Ainda, será abordada a implementação de padrões de ética e conduta, políticas que servirão de reforço à aderência às normas internas citadas, canais de denúncia e treinamento. Ao final, e não menos importante, serão abordados os elementos centrais do *Compliance* no segmento da saúde, bem como as diretrizes para implementação de um programa efetivo.

O *Compliance* se correlaciona com a LGPD, pois para que haja a adequação da LGPD dentro de uma empresa é implementado um sistema de gestão de *Compliance.* Em regra, a implantação de um sistema de *Compliance* de dados é semelhante à implantação de um sistema de gestão de *Compliance*, eis que obedece passos semelhantes, porém com algumas especificidades da proteção de dados.

Os programas de *Compliance* podem ser conhecidos como programas de conformidade, de cumprimento ou de integridade. São instrumentos de governança corporativa tendentes a garantir a implementação das políticas públicas de forma mais eficiente.[164] Além disso, são compostos de mecanismos para que sejam prevenidos os riscos de responsabilidade empresarial decorrentes do descumprimento de obrigações legais, regulatórias, normas éticas e padrões de conduta propostos pelos *stakeholders.*

Compliance pode significar, em português, conformidade, mas também integridade. Segundo o Decreto 8.420/2015:

> Programa de integridade consiste, no âmbito de uma pessoa jurídica, no conjunto de mecanismos e procedimentos internos de integridade,

[164] CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance***: Perspectivas e Desafios dos programas de conformidade. Belo Horizonte: Fórum, 2019. p. 53.

> auditoria e incentivo à denúncia de irregularidades e na aplicação efetiva de códigos de ética e de conduta, políticas e diretrizes com objetivo de detectar e sanar desvios, fraudes, irregularidades e atos ilícitos praticados contra a administração pública, nacional ou estrangeira.[165]

Os requisitos básicos do programa de *Compliance* são:

> a) padrões de conduta e política e procedimentos escritos;
> b) designação de um *Compliance Officer* e/ou Comitê de *Compliance*;
> c) educação e treinamento para fornecer conhecimento de forma efetiva;
> d) canal de comunicação anônima de eventuais problemas de *Compliance*;
> e) monitoramento proativo de processos específicos e documentados para fins de *Compliance* e ajuda na redução de problemas identificados;
> f) comunicação efetiva e ações disciplinares e corretivas.[166]

Em linhas gerais, a principal função dos programas de *Compliance* é a de proteger, orientar e garantir qualidade e fomento à inovação. Por fim, mas não menos importante, tem-se a função de monitoramento e a de criação de uma cultura dentro da empresa para que haja efetividade do programa, o qual, desse modo, não se sustentará apenas por meio da criação de normas, mas também guiando a cultura das pessoas.[167]

As finalidades dos programas de *Compliance* se confundem com os riscos jurídicos enfrentados pelas empresas, que são: *Compliance criminal* e, especificadamente, o direito antitruste, as leis anticorrupções, a lavagem de dinheiro, o direito do trabalho, o direito de proteção de dados pessoais, o direito e proteção da propriedade intelectual, o direito tributário, o direito ambiental, bem como o direito do consumidor.[168] Neste tópico, será abordado apenas o direito de proteção de dados pessoais devido ao enfoque do estudo.

---

[165] BRASIL. **Decreto n.º 8.420, de 18 de março de 2015**. Regulamenta a Lei nº 12.846, de 1º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências. Brasília, DF: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm. Acesso em: 22 jun. 2022. Art. 41.

[166] COIMBRA, Marcelo de Aguiar; MANZI, Vanessa A. **Manual de *Compliance***. Preservando a Boa Governança e a Integridade das Organizações. São Paulo: Atlas, 2010. p. 37-40.

[167] CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance***: Perspectivas e Desafios dos programas de conformidade. Belo Horizonte: Fórum, 2019. p. 57.

[168] CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance***: Perspectivas e Desafios dos programas de conformidade. Belo Horizonte: Fórum, 2019. p. 63.

Com a entrada em vigor da LGPD, as empresas tiveram que introduzir, em suas culturas, programas de conformidade que visem à proteção dos dados pessoais em resposta à necessidade de proteger efetivamente as pessoas na era atual, de rápidas mudanças e avanços tecnológicos.

Para que a LGPD tenha mais credibilidade e aderência, há a imposição de multa pecuniária, que pode chegar a 2% do faturamento da empresa – até o limite de R$ 50 milhões, suspensão parcial do funcionamento do banco de dados e das atividades do tratamento de dados, conforme alterado pela Lei 13.853/2019[169]. Em vista da alta pena pecuniária que poderá ser imposta e das demais consequências que podem afetar as atividades das empresas, o assunto de proteção de dados deve ser levado a sério. Inclusive, a depender do caso, pode ocorrer a proibição total das atividades relacionadas ao tratamento do dado pessoal.[170]

Diante dos riscos que todo esse impacto representa aos indivíduos, um dos objetivos da LGPD foi justamente delimitar as obrigações dos agentes de tratamento de dados e, com isso, fixar regime jurídico para sua responsabilização.[171] Afirmam ser possível identificar outros quatro eixos da LGPD: (i) unidade e generalidade da aplicação da lei; (ii) legitimação para o tratamento de dados; (iii) princípios e direitos do titular; e (iv) obrigações dos agentes de tratamento de dados. É inevitável, nesse "admirável novo mundo", cheio de riscos,[172] experimentar efeitos colaterais que

---

[169] BRASIL. Lei n. 13.843 de 8 de Julho de 2019. Brasília.Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm. Acesso em 23.nov de 2022.

[170] "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: (Vigência)I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) 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 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II; IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização; VI - eliminação dos dados pessoais a que se refere a infração; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; (Incluído pela Lei n.º 13.853, de 2019) XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei n.º 13.853, de 2019)." (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 out. 2022.)

[171] SCHERTEL, Laura Mendes; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista dos Tribunais**, São Paulo, v. 120, p. 469-483, 2018.

[172] MIRAGEM, Bruno. A internet das coisas e os riscos do admirável mundo novo. **Consultor Jurídico**. São Paulo, 29 mar. 2017. Disponível em: https://www.conjur.com.br/2017-mar-29/garantias-consumo-internet-coisas-riscos-admiravel-mundo. Acesso em: 7 jul. 2021.n.p.

deverão ser compensados e, preferencialmente, prevenidos.[173] A esse respeito, a seção sobre responsabilidade e ressarcimento de danos[174] desafia um exercício difícil de dogmática jurídica.

A gestão de riscos deixou de ser uma preocupação exclusiva das organizações financeiras e passou a ser também de interesse das empresas não financeiras, em especial aquelas líderes em seus segmentos de atuação.[175] O interesse dessas empresas tornou-se mais proeminente quando foram noticiados escândalos de grandes corporações, tanto norte-americanas quanto de outras nações, os quais ameaçaram a continuidade dos negócios, chamando a atenção de investidores, credores, gestores, governos e da academia.[176]

A avaliação e a análise de riscos são muito importantes para dar visibilidade à situação dos ativos, assim como para priorizar os investimentos e proteger os ativos da melhor maneira.[177]

Na legislação, na parte de sanções da Lei Geral de Proteção de Dados,[178] há a referência de que a adoção de um sistema de *Compliance* ou governança vai ter

---

[173] COSTA, Luiz. Privacy and the precautionary principle. **Computer Law & Security Review**, [*s. l.*], v. 28, p. 14-24, 2012.

[174] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Seção III, cap. VI.

[175] SAITO, R.; SCHIOZER, R. F. Uso de derivativos em empresas não-financeiras listadas em bolsa no Brasil. **RAUSP Management Journal**, [*s. l.*], v. 42, n. 1, p. 97-107, 2007.

[176] LOPES, Iago Franca; BEUREN, Ilse Maria; VICENTE, Ernesto Fernando Rodrigues. Associação da Evidenciação do Gerenciamento de Riscos com Governança Corporativa e Desempenho em Empresas com ADRs. **Revista Evidenciação Contábil & Finanças**, *[s. l.]*, v. 9, n. 1, p. 5–21, 2021. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/recfin/article/view/52215. Acesso em: 7 jul. 2021.

[177] DONDA, Daniel. **Guia prático de implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.p.45.

[178] "Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
[...]
§ 1º As sanções serão aplicadas 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 os seguintes parâmetros e critérios:
[...]VII - a cooperação do infrator;
VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;
IX - a adoção de política de boas práticas e governança;
X - a pronta adoção de medidas corretivas; [...]" (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2022.)

impacto na aplicação da multa. Com isso, a lei deixa claro que o fato de ter um sistema de *Compliance* ou um sistema de governança de dados não vai eximir a empresa de ser responsabilizada, mas servirá como um redutor de multa.

Outra disposição da referida lei que pode ser combinada com alguns elementos de *Compliance* está prevista no parágrafo 7.º:

> § 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo.[179]

Esse parágrafo estabelece uma conexão com o *Compliance* no sentido de que, se houver um vazamento de dados dentro de uma organização que tem um programa de *Compliance* efetivo e se for possível fazer uma investigação corporativa adequada, haverá a possibilidade de ser descoberto antes o vazamento de dados, podendo se antecipar e ser proposta conciliação direta com o titular de dados, evitando, assim, a aplicação de penalidades.

Ademais, o artigo 46 traz que os agentes de tratamento de dados - pessoas jurídicas ou físicas - devem adotar medidas de segurança, técnicas e administrativas aptas a protegerem os dados pessoais:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.[180]

A LGPD não estabelece medida-padrão de exigência de segurança. Ela trata, de forma genérica, sobre os critérios de melhores práticas do mercado. Para adotar medidas de segurança, é preciso recorrer às normas de ISO, que vão adequar essas medidas de segurança ao tamanho e à complexidade da empresa. No caso de eventuais incidentes de segurança, esses devem ser comunicados à ANPD.[181]

---

[179] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2022.

[180] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

[181] "Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.§ 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá

Quando se trata de boas práticas de governança, o artigo 50[182] da referida lei traz importantes informações detalhadas do que é necessário para a implementação da LGPD, pois, em caso de fiscalização da empresa, é crucial saber os pré-requisitos de um sistema de gestão de *Compliance*. O referido artigo traz regras de boas práticas e de governança, que estabelecem as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados à proteção de dados.

Na referida norma, resta claro que deverá ter um encarregado de dados, um comitê, *etc*. Deve também ter um canal para exigências, definições e pedidos dos titulares de dados, bem como ações educativas e padrões e normas de segurança para o tratamento de dados.

Sempre que forem definidas as melhores práticas, deverão ser observados os princípios da LGPD (finalidade, probabilidade e gravidade dos riscos e benefícios decorrentes do tratamento de dados do titular). A implementação do sistema de *Compliance* deve observar a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados. Aqui, está claro que se deve fazer uma avaliação de riscos e, em todos os casos, um estudo do impacto que essas medidas terão no direito dos titulares.[183]

---

mencionar, no mínimo:[...]" (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.)

[182] "Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais." (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.)

[183] "Art. 50

[...]

§ 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular.

O artigo 50, inciso I, alíneas de ‘a’ até ‘h’, trata ainda dos mínimos requisitos que devem estar presentes para implementação do sistema de gestão de *Compliance*.[184] É importante conseguir demonstrar as razões pelas quais o programa de *Compliance* é efetivo, e isso envolve ter uma gestão de indicadores que demonstrem claramente o que é considerado sucesso do programa de governança e privacidade. É necessário ter os KPIs (Key Performance Indicators) e que os indicadores do programa estejam adequados ao contexto da empresa (porte, riscos, *etc*.). Todas essas regras devem ser publicadas e atualizadas periodicamente.

Para que a adequação à LGPD ocorra, é preciso conhecer os dados que estão sendo tratados, conhecer os ativos de TI, saber quais *softwares* são utilizados para tratamento de dados, ter o apoio jurídico, integrando tudo isso no sistema de *Compliance* a fim de criar uma cultura de proteção de dados e privacidade, pois tudo que é feito guiará ações de pessoas.

O programa explanado deve estar alinhado com as políticas de governança e *Compliance*, que tem por escopo, no geral, realizar uma gestão de riscos (que serão analisados da próxima seção) - mediante boas práticas, observância da legislação e regulamentos internos - e criar controles internos.[185]

---

§ 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: [...]” (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.)

[184] “I - implementar programa de governança em privacidade que, no mínimo:
a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;
b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
g) conte com planos de resposta a incidentes e remediação; e
h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;” (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.)

[185] COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019. p. 198.

4.1 AVALIAÇÃO DE RISCOS E GERENCIAMENTO

O risco de vazamento de dados existe por toda a cadeia na área da saúde, e não é um risco abstrato, porque ele ocorre de verdade na prática. Assim, a avaliação e o gerenciamento dos riscos são essenciais, e toda vez que temos uma situação que de fato acontece, ou seja, no histórico operacional, trata-se de risco alto, então é preciso de ter mais controle, possibilitando assim a criação do sistema de gestão de compliance na avaliação de risco, e é sobre o que o presente tópico irá tratar.

À medida que se começou a avaliar a frequência (incidência e prevalência) com que pacientes sofriam danos provenientes do cuidado da saúde, percebeu-se que a magnitude desse problema atraiu a atenção de profissionais e gestores da saúde, bem como de pesquisadores, de grupos de direitos dos pacientes e da sociedade em geral.[186]

Assim, a detecção dos fatores de mitigação, as ações de melhoria e as ações empreendidas para reduzir riscos são de extrema importância. O termo “risco” tem como origem a palavra *risicu* ou *riscu*, em latim, que está relacionada a “ousar”, ou seja, risco tem a ver com a ousadia na consecução dos objetivos.[187]

Há alguns conceitos de risco na literatura. Um primeiro conceito identifica risco como o conjunto de eventos, externos ou internos, que podem impactar (positiva ou negativamente) os objetivos estratégicos da organização, inclusive os relacionados aos ativos intangíveis. Pode ser qualquer coisa que impeça as empresas de realizarem a continuidade do seu negócio.[188]

Ainda existe o conceito de risco como sendo as ameaças aos valores de uma organização, sejam esses econômicos, reputacionais, legais ou regulatórios, mercadológicos ou operacionais.[189]

O risco pode vir de fontes internas e externas. Riscos externos são aqueles que não estão no controle direto da administração. Incluem questões políticas, taxas de

---

[186] SOUSA, Paulo (org.). **Segurança do paciente**: conhecendo os riscos nas organizações de saúde 2. ed. Rio de Janeiro: Fiocruz, 2019. p. 21.

187 LEMOS, Ricardo. Gerenciamento de Riscos Corporativos. In: LAMBOY, Christian K. (coord.). Manual de Compliance. São Paulo: Via Ética, 2018. p. 449-470.

[188] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de Riscos Corporativos**: evolução em governança estratégia. São Paulo: IBCG, 2017. p. 41.

[189] BANDAROVSKY, Bruno Pires. *Compliance* Risk Assessment em 8 passos. s.n. *In:* LEC. Disponível em: https://conteudo.lec.com.br/*Compliance*-risk-assessment-em-8-passos. Acesso em: 14 jun. 2022.n.p.

câmbio, taxas de juros, catástrofes naturais e assim por diante. Riscos internos, por outro lado, incluem: não conformidade, vazamento de informações, acidentes numa planta, entre vários outros.[190]

A identificação de riscos de negócio é crucial para a subsistência empresarial. Com efeito, o mapeamento e gerenciamento de potenciais problemas permitem atuação preventiva, o que reduz efeitos e impactos negativos, tanto econômicos quanto sociais.[191]

Na esfera da Lei Geral de Proteção de Dados Pessoais, o risco do tratamento de dados também deve ser pontuado. Por esse motivo, sugere-se que, conjuntamente com a análise e o gerenciamento de riscos negociais e mercadológicos, também sejam incluídos os riscos relacionados à proteção de dados, principalmente no que diz respeito aos vazamentos e às invasões de sistemas.

Assim, verifica-se que o risco poderá estar presente em várias situações como, por exemplo, na coleção excessiva de dados, na falta de finalidade ao tratamento de dados, na falha de *hardwares*, na falta de permissão para copiar ou retirar dados, *etc*. A LGPD trouxe um avanço para que as normas de proteção de dados sejam cumpridas e para que haja responsabilização daqueles que a descumpram. Por isso, a adoção de medidas para que seja mitigado o risco é o que se impõe a fim de que sejam observadas e cumpridas as normas de proteção aos dados pessoais.

A prevenção de risco é o ponto convergente entre o *Compliance* e a proteção de dados, sendo que o *Compliance* aparece como fomentador para que as normas sejam cumpridas na mitigação dos riscos e eventuais danos.[192] Nesse sentido, o mapeamento de riscos é uma das principais ferramentas de prevenção.

4.1.1 Gerenciamendo risco

O gerenciamento de riscos é importante, em uma organização, para a

---

[190] TRILHO, Alvaro. **Gerenciamento de Riscos e o Papel do profissional de Riscos**. IBGC Análises & Tendências, [*s. l.*], 4. ed., jul. 2018. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2018/08/ibcg-analises-e-tendencias-gerenciamento-de-riscos-no-4-2018.pdf. Acesso em: 22 jun. 2022.n.p.

[191] HEALEY, Robert. **Data Mapping and GDPR *Compliance***: What your business needs to know. United Kingdom, Aug. 2022. Disponível em: https://formiti.com/data-mapping-and-gdpr-*compliance*-what-your-business-needs-to-know/. Acesso em: 13 out. 2022.n.p.

[192] CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance* e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 311-315.

continuidade do negócio, porque, sem ele, não podem ser definidos os objetivos de forma adequada. O objetivo do gerenciamento de riscos é garantir que a empresa priorize os riscos que a ajudarão a atingir seus objetivos; mantendo todos os outros sob controle. Dessa forma, se faz necessário identificar os riscos para que eles possam ser alocados de forma efetiva.[193]

Gerenciar riscos, atuais e futuros, é uma questão de, ao mesmo tempo, aproveitar oportunidades vantajosas e evitar riscos desvantajosos, pois o risco é inerente a qualquer atividade na vida pessoal, profissional ou organizacional. A cultura da administração dos riscos é um elemento-chave.[194]

O *Compliance Risk Assessment*[195] pretende identificar os riscos de *Compliance* aos quais a empresa está exposta, quais os fatores de risco existentes, qual o impacto potencial do risco na organização, qual a probabilidade de materialização desse risco, quais as medidas mitigatórias já existentes, quais devem ser aprimoradas ou adicionadas (bem como quais devem ser suprimidas), qual o plano de implementação dos ajustes às medidas mitigatórias e como esse plano será monitorado pela unidade de *Compliance*.[196]

Definidos o impacto e a probabilidade, é preciso entender quais recursos serão utilizados para que o risco não se concretize. Depois de definidas essas medidas de mitigação, será criado um plano de implementação e se dará continuidade ao monitoramento para evitar riscos eventuais.

A elaboração de um projeto de implementação de Programa de *Compliance* sem a realização de uma avaliação de riscos prévia é bastante temerária, pois será realizada sem conhecimento acerca dos riscos aos quais a companhia está exposta e, portanto, sem o conhecimento de quais são as medidas necessárias para mitigar esses riscos, envidando esforços, investimento de tempo e recursos para medidas que não trarão a segurança necessária para as operações da empresa. Assim, se faz

---

193 TRILHO, Alvaro. **Gerenciamento de Riscos e o Papel do profissional de Riscos**. IBGC Análises & Tendências, [*s. l.*], 4. ed., jul. 2018. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2018/08/ibcg-analises-e-tendencias-gerenciamento-de-riscos-no-4-2018.pdf. Acesso em: 22 jun. 2022.n.p.

194 LEMOS, Ricardo. Gerenciamento de Riscos Corporativos. *In:* LAMBOY, Christian K. (coord.). **Manual de *Compliance***. São Paulo: Via Ética, 2018.

195 UNITED STATES. Department of Justice. **Evaluation of Corporate *Compliance* Programs**. [*S. l.s.n*], June 2020. Disponível em: https://www.justice.gov/criminal-fraud/page/file/937501/download. Acesso em: 13 set. 2022.n.p.

196 BANDAROVSKY, Bruno Pires. *Compliance* Risk Assessment em 8 passos. *In:* LEC. Disponível em: https://conteudo.lec.com.br/*Compliance*-risk-assessment-em-8-passos. Acesso em: 14 jun. 2022.

necessária a realização de uma avaliação do risco antes da implementação de um sistema de gestão de *Compliance*.[197]

A organização precisa ter aspectos para controlar os riscos a que está exposta, e esse controle possui uma função se analisado sob três aspectos: (i) tamanho ou relevância do risco; (ii) possibilidade de ocorrência; (iii) como reagir ou responder a cada tipo de risco.[198]

A estrutura de uma implementação de LGPD segue os mesmos passos de um sistema de *Compliance*, porém, ao invés de ter somente o *Risk Assessment* (análise de risco), uma implementação de LGPD terá *Data mapping* (inventário e registro de dados, mapeamento dos dados da empresa), *Privacy Impact Assessment* – PIA (avaliação que discute os impactos para a privacidade de determinado produto, serviço ou atividade da empresa) e *Data Protection Impact Assessments* (DPIA).[199]

Na área da saúde o risco existe em diversas cadeias, seja dentro do hospital, na logística, todos esses terão acessos aos dados dos pacientes, ou seja, o risco de vazamento é alto.

No Brasil, ainda não se tem uma definição de circunstâncias nas quais esse relatório de impacto seja obrigatório. Caberá à ANPD tal definição em resolução específica sobre RIPD (Relatório de Impacto à Proteção dos Dados Pessoais) consoante inc. XIII do art. 55-J da LGPD.[200]

De acordo com o parágrafo 1.º do artigo 48 da LGPD, a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares deve ser comunicada à autoridade nacional e aos titulares. Essa comunicação deverá conter, no mínimo: "[...] I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial; IV - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas

---

[197] CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance* e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021. p. 306-307.

[198] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p.24-27

[199] STEINBERG, Richar M. **Governance, Risk Management, and *Compliance* It Can't happen to Us-Avoiding Corporate Disaster While Driving Success**. [*S. l.: s. n.*], 2011. p. 115-135.

[200] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

para reverter ou mitigar os efeitos do prejuízo”.[201]

Consoante ao que dispõe a LGPD sobre tratamento de dados com base no legítimo interesse (§ 3.º do art. 10 da LGPD) ou sobre tratamento de dados pessoais sensíveis (art. 38 da LGPD), o Relatório de Impacto à Proteção de Dados (RIPD) é obrigatório. Em outras situações, esse documento será facultativo. Muitas implementações da LGPD estão elaborando o RIPD sempre, fundamentando-se no princípio da responsabilidade e prestação de contas (*accountability*).[202]

4.1.2 Metodologia

Os *assessments* referidos anteriormente neste texto precisam ser integrados a um sistema de gestão de *Compliance* de dados. Assim, verifica-se que o Programa de *Compliance* precisa estar embasado em evidências para que ele possa ser auditado por terceiras pessoas que não estavam presentes quando da definição do projeto, da elaboração do escopo e da implementação das ações necessárias. Por isso a importância de determinar a metodologia que será adotada para definição da avaliação dos riscos. Do ponto de vista do *Risk Assessments* há três metodologias, que serão a seguir estudadas.

4.1.2.1 ISO 31000

Entre as metodologias mais usuais, está a ISO 31000 de Gestão de Riscos, que contém diretrizes, conceitos e orientações de como pode ser realizada a avaliação de risco dentro das organizações. Essa não é uma ISO de requisitos que precisam ser cumpridos, mas uma ISO de diretrizes, ou seja, contém a ideia central para que seja possível, dentro da organização, realizar a avaliação de riscos

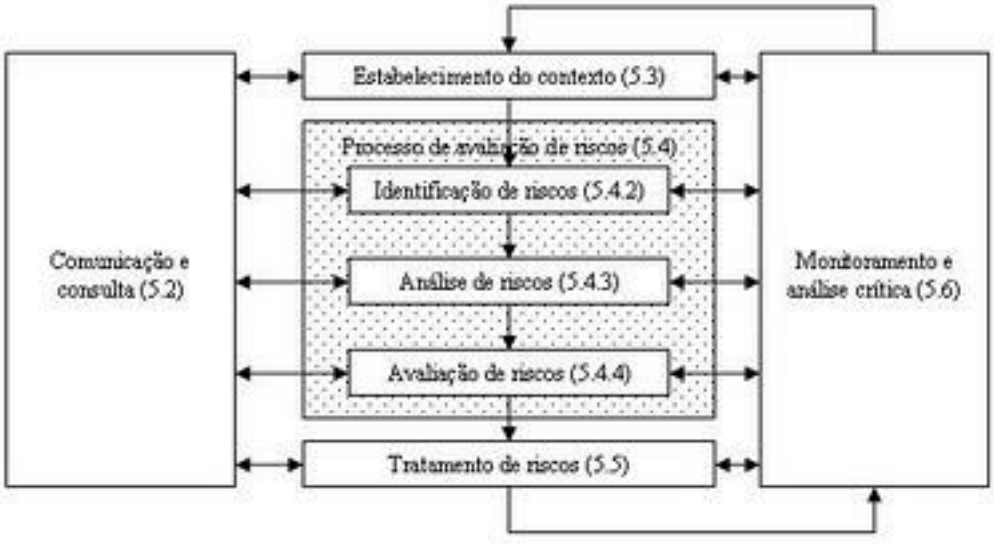
A Figura 1 apresenta as diretrizes com as orientações da ISO 31000.

---

[201] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

[202] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020.

Figura 1 – Orientações ISO 31000



Fonte: RICARDO, José.[203]

A ISO 31000 determina princípios, um *framework* de trabalho e um processo para a gestão dos diversos tipos de risco em todas as organizações, independentemente do seu tamanho. Essa norma foi lançada em 2009 pela International Organization for Standardization com o objetivo de padronizar a gestão de riscos de forma generalizada.[204]

4.1.2.2 COSO

Outra metodologia sugerida para avaliação dos riscos é a COSO (Committee of Sponsoring Organizations of the Treadway Commission),[205] que é uma organização privada criada nos EUA em 1985 para prevenir e evitar fraudes nos procedimentos e processos internos da empresa. Essa metodologia foi uma forma de criar processos e controles internos.

> O gerenciamento de riscos corporativos é um processo conduzido em uma organização pelo conselho de administração, diretoria e demais empregados, aplicado no estabelecimento de estratégias, formuladas para identificar em toda a organização eventos em potencial, capazes

[203] RICARDO, José. Processo de gestão de riscos ISO 31000. **Administradores.com**, [*s. l.*], 27 nov. 2010. Café com ADM. Disponível em: https://administradores.com.br/artigos/processo-de-gestao-de-riscos-iso-31000. Acesso em: 15 jun. 2022.n.p.

[204] OLIVEIRA, Ualison Rébula de *et al.* The ISO 31000 standard in supply chain risk management. **Journal of Cleaner Production**, [*s. l.*], v. 151, p. 616-633, 2017.

[205] SAAVEDRA, Giovani Agostini. ***Compliance* na área da saúde**. Brasil: Lykoscatle, 2016. p. 28.

> de afetá-la, e administrar os riscos de modo a mantê-los compatível com o apetite a risco da organização [...][206]

Essa metodologia permite que seja analisado cada setor da empresa de forma individualizada, com os mesmos objetos em diferentes formas. Embora a COSO possua esse enfoque individual em cada frente de negócio da empresa, por meio dela é possível ter uma visão do todo para se realizar o plano de ação.'

4.1.2.3 Análise de Riscos Parametrizada

No Brasil, o instituto ARC – Auditoria, Riscos e *Compliance* desenvolveu uma metodologia que integra os dois modelos – ISO 31000 e COSO – em um mais abrangente: a Análise de Riscos Parametrizada.[207]

Tal metodologia baseia-se num processo de integração de conhecimentos de segmentos específicos por meio de listas “Standards” de parâmetros que servem de base para avaliar os diversos sistemas, o grau de treinamento e adequabilidade dos recursos humanos envolvidos, bem como a efetividade do processo empregado. Além disso, são sempre levados em consideração os riscos estratégicos da organização e o quanto tais riscos afetam os fatores críticos de sucesso da empresa.

Nessa metodologia, utiliza-se uma fórmula matemática para que possam ser imputadas todas as variáveis analisadas durante a apuração dos riscos e classificar as variáveis por numeração. Ao final, é aplicada uma fórmula matemática para definir a probabilidade, o impacto e onde o risco será alocado na matriz de risco.[208]

4.2 CÓDIGOS DE CONDUTA E ÉTICA, POLÍTICAS E PROCEDIMENTOS INTERNOS, TREINAMENTOS E CANAIS DE DENÚNCIA

Entre os vários elementos de um sistema de gestão de *Compliance* efetivo elencado pelo Decreto n.º 8.420/2015, neste capítulo serão analisados o código de conduta e ética, as políticas internas e os procedimentos, os treinamentos e os canais

---

[206] COSO. **Gerenciamento de Riscos Corporativos** – estrutura integrada. [*S. l.*]: PricewaterhouseCoopers, 2007. p. 4.

[207] INSTITUTO ARC. São Paulo, 2022. Disponível em: http://www.instituto-arc.com/. Acesso em: 19 out. 2022.

[208] SILVA, Nelson Ricardo *et al.* **Análise De Risco Parametrizada 2.0**: Manual prático de Governança voltada para a Gestão de Risco. São Paulo: PoloBooks, 2017. P.55.

de denúncia. No recorte proposto no presente estudo, esses são os elementos mais específicos para a proteção de dados.

O código de conduta e ética consiste em um documento com um conjunto de regras que definem valores e orientam as ações esperadas pelos colaboradores no exercício do seu trabalho e no processo de tomada de decisão. Serve como instrumento de divulgação da missão e dos valores da empresa, o que facilita o entendimento e a prática da cultura organizacional. Esse documento determina também o padrão de comportamento que explicita a cultura da empresa, principalmente em face de seus *stakeholders* (clientes, acionistas, *etc.*).

Essas regras devem ser observadas por todos os funcionários, independentemente de cargo e função, bem como pelos colaboradores e prestadores de serviço da companhia, devendo ser consideradas desde o início da relação com a organização. Devem ser constantemente reforçadas e divulgadas para que sejam, de fato, colocadas em prática.

A forma de construção e organização desse código de conduta se dá por meio da criação de um Comitê, composto por membros de diversos departamentos da empresa. Além disso, deve haver engajamento da alta liderança a fim de que esse documento tenha sucesso e seja seguido. Após a criação do Comitê e após haver engajamento das liderança, deve ser definida a missão, que revela os valores da companhia. Com essa definições será feito o índice do que deve ser seguido, como o funcionamento e a aplicabilidade do código, e o relacionamento dos colaboradores com o mercado, a comunidade, os acionistas, os fornecedores, os médicos e os pacientes.[209]

Outro documento importante são as políticas e procedimentos internos de *Compliance*, que é mais específico e detalhado. Ele é aplicável a um público específico, que são os colaboradores. Seu tema é único, com foco em determinada prática que traga risco para a organização. Esse documento apresenta regras e procedimentos que devem ser estabelecidos e endereçados de uma maneira específica para que seja possível mitigar o risco envolvido em determinada atividade, sempre com data de vigência. Quanto às exceções à política, devem ser aprovadas, por escrito, pelo Departamento de *Compliance*.[210]

---

[209] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020.p.31.

[210] UNITED STATES. Department of Justice. **Evaluation of Corporate *Compliance* Programs**. [*S.*

As razões para que sejam elaboradas as políticas de *Compliance* são: atender aos inúmeros padrões normativos existentes; garantir a conformidade da empresa com as leis e a ética; definir e aclarar expectativas entre empresa e colaborador; fornecer apoio, recurso e informação; auxiliar o colaborador com questões e/ou situações de trabalho; detectar e prevenir comportamentos prejudiciais à empresa; manter compromisso com práticas comerciais éticas e de boa-fé negocial; e alcançar maior solidez nos objetivos estratégicos e processuais da organização.[211]

Em caso de eventual violação da política de *Compliance*, qualquer colaborador que acreditar que ela foi violada deve relatar o assunto ao seu supervisor imediato. Se o supervisor for incapaz ou falhar em solucionar o problema, o colaborador deverá entrar em contato com o Departamento de *Compliance* ou utilizar a ferramenta do canal de denúncias. Nenhum colaborador que relatar qualquer problema, com boas intenções, deve sofrer qualquer represália. Qualquer colaborador que seja identificado como responsável e que venha a violar essa política estará sujeito à ação disciplinar adequada, incluindo desligamento.[212]

Na área da saúde, o principal fator é o risco, que deve ser mitigado. As principais políticas de *Compliance* dentro da área da saúde são: anticorrupção e suborno; contratos de prestação de serviço; itens educacionais; itens de *marketing* e presentes; refeições comerciais; entretenimento ou recreação; produtos com desconto ou gratuitos; patrocínios de eventos (próprios, de fabricantes, de terceiros, de profissionais da saúde) e despesas; interação com terceiros intermediários; privacidade e proteção de dados; patrocínio de eventos; e contribuições de caridade. Este trabalho ficará restrito à proteção de dados.[213]

Ademais, políticas de privacidade longas, obscuras e legalistas aumentam o descrédito de que a privacidade está sendo respeitada. Ainda, para agravar, a política pode ser alterada à vontade, ocorrendo a devida notificação de tal mudança, dentro da própria política, fazendo com que as pessoas leiam a notificação várias vezes,

---

l.], June 2020. Disponível em: https://www.justice.gov/criminal-fraud/page/file/937501/download. Acesso em: 13 set. 2022.n.p.

[211] UNITED STATES. Department of Justice. **Evaluation of Corporate *Compliance* Programs**. [*S. l.*], June 2020. Disponível em: https://www.justice.gov/criminal-fraud/page/file/937501/download. Acesso em: 13 set. 2022.n.p.

[212] ASSI, Marcos. ***Compliance***: como implementar. São Paulo: Trevisan, 2018.

[213] SAAVEDRA, Giovani (org.). **Prevenção à corrupção e *compliance***. 2. ed. São Paulo: ESENI, 2019.n.p.

porém sem a compreender, ou, muitas vezes, nem a leiam.[214]

A respeito da divulgação e do treinamento, poderá ser por meio de palestras, interação por meio de jogos, perguntas e avaliação para um público específico, devendo ser disponibilizados documentos para as pessoas. O conteúdo desse treinamento deverá ser consentido pelos participantes por meio de um termo de compromisso, que deve ser renovado periodicamente, posto que o programa de conformidade deve fazer parte da rotina dos colaboradores.[215]

Com relação ao canal de denúncias, devem ser disponibilizados canais abertos de comunicação de infrações tanto para o titular dos dados pessoais quanto para os colaboradores da organização.

Segundo o Instituto Brasileiro de Governança Corporativa (IBGC):[216]

> O canal de denúncias, previsto e regulamentado no código de conduta da organização, é instrumento relevante para acolher opiniões, críticas, reclamações e denúncias, contribuindo para o combate a fraudes e corrupção e para a efetividade e transparência na comunicação e no relacionamento da organização com as partes interessadas.

Para estruturar programas de *Compliance* de proteção de dados efetivos, todas as medidas acima elencadas, entre outras, devem ser rigorosamente atendidas, sob pena de aplicação de sanção administrativa, porém com atenuante, conforme prevê o artigo 52, § 1.º, IX da LGPD, em casos de ter sido comprovada a adoção de processos e políticas internas.

4.3 DIRETRIZES PARA IMPLEMENTAÇÃO DE *COMPLIANCE* EFETIVO NA ÁREA DA SAÚDE

A Lei Geral de Proteção de Dados pode ser considerada como uma nova fase do *Compliance*, instigando as empresas, não só da área da saúde, a adotarem práticas de segurança técnica capazes de proteger dados pessoais de acessos e evitar situações de acidentais ou de destruição, perda, alteração, comunicação ou

---

[214] NISSENBAUM, Helen. **Privacy in Context Technology, Policy, and the Integrity of Social Life**. [*S. l.*]: Stanford Law Books, 2009. p. 34.

[215] ASSI, Marcos. ***Compliance***: como implementar. São Paulo: Trevisan, 2018.p.67-70.

[216] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/21138/Publicacao-IBGCCodigo-CodigodasMelhoresPraticasdeGC-5aEdicao.pdf. Acesso em: 14 jun. 2022. p. 95.

qualquer forma de tratamento inadequado ou ilícito de dados. As empresas, portanto, precisam implantar mecanismos de governança e privacidade, os quais, indubitavelmente, impactam diretamente na condução de qualquer atividade empresarial.

Tendo como princípios a transparência, a equidade, a prestação de contas e o *Compliance*, a governança corporativa alinha-se à dimensão da responsabilidade social corporativa na condução das atividades organizacionais e tem o *Compliance* como um elemento estratégico determinante para sua concretização.[217]

Assim, governança corporativa e *Compliance* são absolutamente necessários na área de saúde, em que as organizações lidam diariamente com o bem da vida e na qual os erros podem impactar de formas irreversíveis. A governança corporativa e o *Compliance* fomentarão um sistema de gestão que garanta atuação dentro dos níveis de riscos aceitáveis para as atividades nessa área. O fato de tratar-se de uma área altamente regulada faz com que seja necessária uma estrutura de governança ainda mais dinâmica, além de um programa de *Compliance* compreendido de diversos pontos voltados ao segmento em questão.[218]

É justamente por essa sensibilidade maior da área de saúde que ela está submetida a uma ampla regulação da Agência Nacional de Saúde Suplementar (ANS)[219], da Agência Nacional de Vigilância Sanitária (ANVISA)[220], da Superintendência de Seguros Privados (SUSEPE)[221], entre outras.

Os alicerces da governança na área da saúde estão calcados em dois princípios: responsabilidade social e prestação de contas (*accountability).*[222] A responsabilidade social corporativa diz respeito a gerar valor de forma sustentável e

---

[217] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 22.

[218] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 28.

[219] BRASIL. **Lei n.º 9.961, de 28 de janeiro de 2000**. Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências. Brasília, DF: Presidência da República, 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9961.htm. Acesso em: 1 dez. 2021.

[220] BRASIL. Ministério da Saúde. **Agência Nacional de Vigilância Sanitária**. Brasília, DF, 2022. Disponível em: https://www.gov.br/anvisa/pt-br. Acesso em: 19 out. 2022.

[221] BRASIL. Ministério da Economia. **Superintendência de Seguros Privados**. Brasília, DF, 2022. Disponível em: https://www.gov.br/susep/pt-br. Acesso em: 1 nov. 2022.

[222] AHRENS, Herold. **Accountability no âmbito da governança das Organizações públicas não estatais**: o caso do Instituto de matemática pura e aplicada. 2018. Dissertação (Mestrado em Administração) - Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, Faculdade de Brasília, Brasília, 2018. Disponível em: https://repositorio.unb.br/bitstream/10482/33179/3/2018_HeroldAhrens.pdf. Acesso em: 5 set. 2022. n.p.

com prioridades éticas. Isso tem originado movimentos endógenos para uma governança melhor, que sustenta o tripé de sustentabilidade (*triple bottom line of sustentability*) defendendo a importância dos vieses econômico, social e ambiental dos negócios enquanto direcionadores de um processo de gestão que perceba os impactos positivos e negativos nas áreas de atuação corporativa.[223]

O mapeamento de impactos é de suma importância para a implementação de cultura ética e responsável que permeie a estrutura de governança com ferramentas de avaliação, educação, monitoramento e comunicações, incentivos, processos e composição de órgãos societários. A gestão da saúde baseada em premissas adequadas de responsabilidade social facilita a sua execução por setores que estejam passando por dificuldades ou que tratem com *stakeholders* sensíveis (pacientes, médicos, organizações não governamentais e agência reguladora)[224]*.*

Porém, para que se tenha êxito de um sistema de boa governança, as tomadas de decisões carregam muita responsabilidade. Nesse momento, entra em cena outro princípio, o de *accountability.*

Além de se referir a uma prestação de contas, esse termo significa ônus e responsabilizações dos tomadores de decisão e das consequências de seus atos de gestão, que é precedida de educação, treinamento e monitoramento;[225]

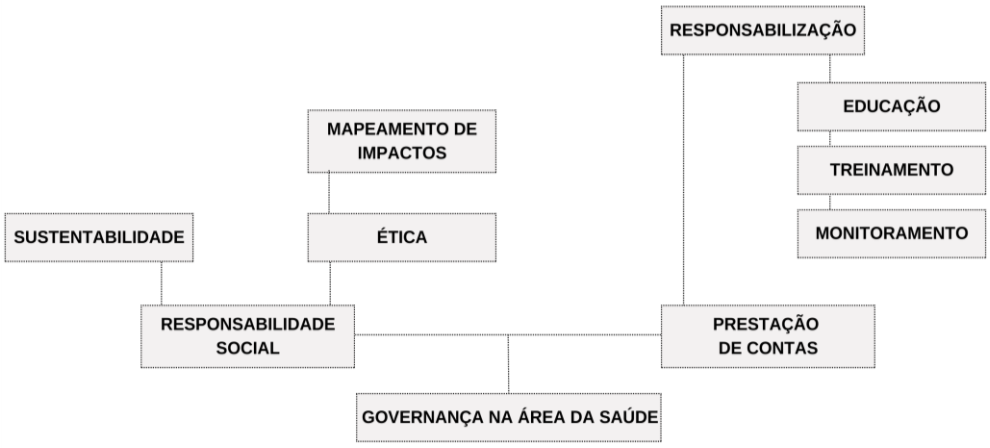
---

[223] CRANE, Andrew; MATTEN, Dirk. **Business Ethics**: Managing corporate citizenship and sustaintability in the age of globalization. 3. ed. Oxford University Press, 2010. Disponível em: https://books.google.com.br/books?id=J8-SDAAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false. Acesso em: 14 jun. 2022. p. 36-37.

[224] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance*** **na área da saúde**. Indaiatuba: Foco, 2020. p. 25.

[225] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance*** **na área da saúde**. Indaiatuba: Foco, 2020. p. 26.

Figura 2 - Fluxograma de Governança Corporativa aplicada à saúde



Fonte: A autora, 2022

O principal executivo e o diretor financeiro de uma empresa, respectivamente, o CEO (*Chief Executive Officer*) e o CFO (*Chief Financial Officer*), na divulgação dos relatórios periódicos previstos em lei, devem se certificar de que: revisaram os relatórios e não existem falsas declarações ou omissões de fatos relevantes; as demonstrações financeiras revelam adequadamente a posição financeira, os resultados das operações e os fluxos de caixa; divulgaram aos auditores e ao comitê de auditoria todas as deficiências significativas que eventualmente existam nos controles internos, bem como quaisquer fraudes evidenciadas ou mudanças significativas ocorridas após a sua avaliação; têm responsabilidade pelo estabelecimento de controles internos, pelos seus desenhos e processos e pela avaliação e monitoramento de sua eficácia. A constituição de um comitê de auditoria para acompanhar a atuação dos auditores e dos números da companhia deve atender às seguintes diretrizes: ter a presença de, pelo menos, um especialista em finanças; ser composto exclusivamente por membros independentes do conselho de administração, não integrantes da direção executiva, sendo que, além dos valores que já recebem pela participação no conselho, não receberão quaisquer outros a título de pagamento pelos aconselhamentos ou consultorias prestados ao comitê; ser responsável pela aprovação prévia dos serviços de auditoria; divulgar, por meio de relatórios periódicos, os resultados de seus trabalhos.[226]

[226] ANDRADE, Adriana; ROSSETTI, José Paschoal. **Governança Corporativa**: Fundamentos, Desenvolvimento e Tendências. São Paulo: Atlas, 2009. p. 183-184.

Conforme o Instituto Brasileiro de Governança Corporativa (IBGC):

> As boas práticas de governança corporativa convertem princípios básicos em recomendações objetivas, alinhando interesses com a finalidade de preservar e otimizar o valor econômico de longo prazo da organização, facilitando seu acesso a recursos e contribuindo para a qualidade da gestão da organização, sua longevidade e o bem comum.[227]

Entendendo os objetivos dos riscos mapeados e tendo consciência dos riscos das suas decisões, o agente corporativo se torna mais cauteloso ao tomar decisões que possam revelar ilícitos, duvidosos ou em seu próprio proveito.

Por fim, sugerem-se alguns pontos como diretrizes para uma construção de boa governança, os quais podem ser aplicados por setores da área da saúde[228]. Destaca-se que, em se tratando de *Compliance* de dados no âmbito da saúde, não há um modelo único a ser seguido, porém, conforme exposto, a doutrina traça alguns elementos mínimos que, somados aos princípios previstos na LGPD, auxiliam na sua implementação:

a) entendimento estratégico do negócio para melhor perceber vulnerabilidades e lacunas de atuação econômica e social;[229]
b) implantação de um programa de boa governança fundado essencialmente em Ética corporativa e sistemas de integridade;[230]
c) atuação pontual com gestão de reponsabilidade social e riscos, de forma a fomentar o crescimento sustentável da organização, bem como mitigar eventuais passivos de atuação;[231]
d) uso de tecnologia adequada para otimização e precisão de troca de

---

[227] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/21138/Publicacao-IBGCCodigo-CodigodasMelhoresPraticasdeGC-5aEdicao.pdf. Acesso em: 14 jun. 2022. p. 20.

[228] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance*** **na área da saúde**. Indaiatuba: Foco, 2020. p. 27.

[229] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance*** **na área da saúde**. Indaiatuba: Foco, 2020. p. 27.

[230] SANTOS; TALIBA, 2018 *apud* FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019. p. 700.

[231] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Lei/L13709.htm. Acesso em: 10 maio 2022.

informações, controle, controles internos e gerenciamento de custos de governança, a fim de garantir melhor utilização de recursos e maior segurança da informação, além de análises da relação de custo x benefício das operações;[232]

e) recrutamento de colaboradores adequados às demandas da empresa quanto à gestão responsável, uma vez que todos os envolvidos no ambiente empresarial (sejam eles prestadores de serviço, representantes, funcionários, fornecedores, dentre outros) devem estar alinhados com as diretrizes éticas, organizacionais e com o padrão de governança corporativa estabelecido;[233]
f) educação e treinamento, para garantia da absorção dos princípios da empresa e concretização de seus efeitos no cotidiano laboral;[234]
g) definição clara de papéis e responsabilidades dos gestores, de modo a fomentar a cooperação entre setores e agentes;[235]
h) monitoramento, por meio de gestores, auditorias internas e externas e órgãos de assessoramento;[236]
i) canais de denúncias, por meio de sistemas eficientes, que garantam a anonimização dos denunciantes e a efetividade dos procedimentos a serem adotados e medidas cabíveis;[237]
j) órgãos de assessoramento (conselhos de ética, sucessões, remunerações, auditoria, risco *etc*.), com formação de equipe técnica, qualificada, adequada e multidisciplinar;[238]
k) *Compliance* officer, cuja principal atribuição é garantir o cumprimento dos

[232] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 27.
[233] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 27.
[234] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 27.
[235] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 27.
[236] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral De Proteção De Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 692.
[237] TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral De Proteção De Dados Pessoais e suas Repercussões no Direito Brasileiro**. São Paulo: Revista dos Tribunais, 2019. p. 693.
[238] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 27

l) procedimentos estabelecidos no programa de Compliance e de boa governança, de forma séria e responsável;[239]

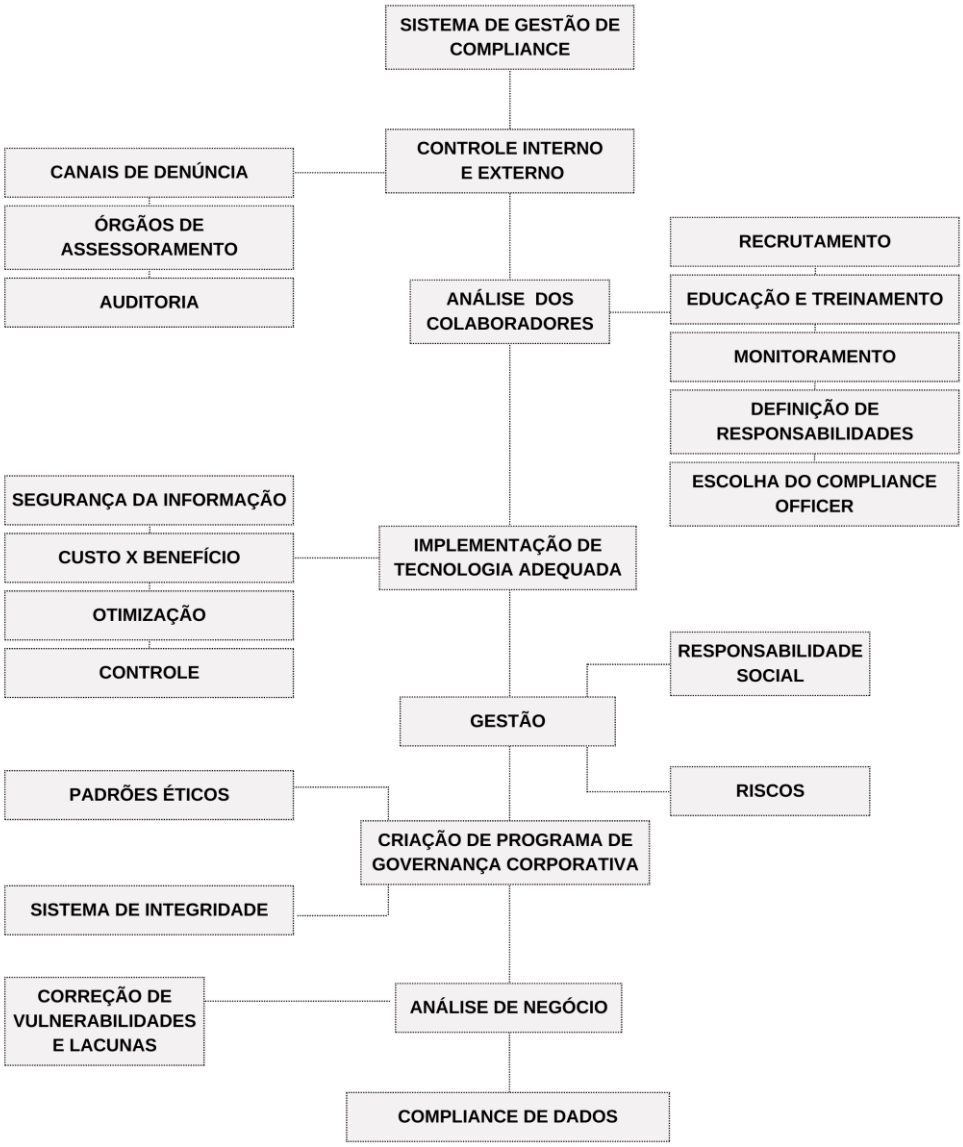
m) sistema de gestão de *Compliance*, destinado a garantir a efetividade do programa.[240]

Para otimizar a compreensão dos itens especificados acima, apresenta-se o seguinte fluxograma:

[239] CRESPO, Liana Irani Affonso Cunha. ***Compliance* officer e efetividade**: sobre as condições necessárias para garantir a ação efetiva do programa de *Compliance*. 2021. Dissertação (Mestrado em Direito Político e Econômico) – Programa de Pós-Graduação em Direito Político e Econômico, Universidade Presbiteriana Mackenzie, São Paulo, 2021. Disponível em: https://dspace.mackenzie.br/handle/10899/28412. Acesso em: 11 set. 2022.

[240] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 27.

Figura 3 - Fluxograma de Compliance de dados



Fonte: A autora, 2022

Desse modo, é necessária a definição de requisitos mínimos para assegurar a efetividade dos programas de *Compliance*, tal como a análise de riscos, código de ética, suporte da alta administração, treinamentos periódicos, cultura corporativa, monitoramento dos controles e processos, canais de comunicação, apuração e punição de condutas contrárias ao programa.

O sistema de *Compliance*, compreendido como "a implementação dos princípios éticos visando maior eficiência, mitigação de riscos e aderência às normas locais, regionais, nacionais e internacionais",[241] é indispensável para empresas

[241] FULLER, Greice Patrícia; FIGUEIREDO, Leidi Priscila. *Compliance* empresarial e tutela penal na

atuantes na área da saúde. Conforme apresentado no presente estudo, os programas de *Compliance* vão além do cumprimento da legislação e demandam aplicação de diretrizes éticas e códigos de condutas voltados às boas práticas empresariais.

Para que sejam considerados efetivos, os programas de *Compliance* devem ser incorporados pelos profissionais, pelas instituições e toda sua cadeia de colaboradores, de modo a garantir que suas disposições façam parte do cotidiano de todos os atuantes. O papel das organizações e seus impactos sociais devem ser muito bem delimitados, e seus objetivos devem ser pautados em padrões preestabelecidos, sendo de amplo conhecimento de todos os envolvidos. Para a disseminação da cultura empresarial, é comum e indicada a formação de um quadro de agentes de governança destinados à propagação dos propósitos, princípios e valores da instituição.[242]

Os agentes de governança devem apresentar conduta proativa, interativa e integrativa, além de boa capacidade de comunicação e liderança. Alocados em áreas estratégicas, que podem variar conforme a atividade e necessidade de cada instituição, eles são os principais *players* para garantir a efetividade do sistema implementado:

> É fundamental que os agentes de governança estabeleçam estratégias de comunicação e programas de treinamento com a finalidade de disseminar, entre as partes interessadas, políticas, procedimentos, normas e práticas baseadas no código de conduta da organização. A essas medidas devem estar associados processos e indicadores formais, a fim de viabilizar o monitoramento dos padrões de conduta adotados, concorrendo para um efetivo engajamento da alta administração nos mecanismos de conformidade da organização e possibilitando que eventuais desvios possam ser evitados ou proativamente identificados, corrigidos e, eventualmente, punidos.[243]

As estratégias de comunicação e disseminação devem ser flexíveis, de modo a garantir maior absorção por parte de todos os atuantes. Os procedimentos a serem adotados não devem ser exaustivos nem estáticos, sob pena de ineficiência do programa.

---

sociedade da informação. **Revista dos Tribunais**, São Paulo, v. 996, p. 573-588, out. 2018. p. 2.

[242] CARLOTO, Selma; GUERRA, Elaine. **Manual Prático de Adequação à LGPD**: Com enfoque nas relações de trabalho. São Paulo: LTr, 2021. p.59-61.

[243] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015. p. 18.

Nesse contexto, a criação de políticas de governança corporativa é essencial para garantir a disseminação de valores e a participação de todos os envolvidos, sejam no papel de sócios, membros da diretoria, conselheiros, fiscalizadores, entre outros. As boas práticas de governança garantem recomendações objetivas, alinhamento de interesses e finalidades e otimização da gestão e tomada de decisões.[244] A governança corporativa abrange princípios basilares, como transparência, equidade e prestação de contas (*accountability*), além de atribuir responsabilidades aos agentes envolvidos.

Outra etapa importante do *Compliance* aliado à governança corporativa é a da elaboração de um código de conduta, cujo conteúdo volta-se à atuação e ao relacionamento interpessoal de todos os envolvidos e estabelece padrões éticos de desempenho de atividades e comportamento na busca pelo alcance do "melhor bem-estar agregado possível para todos aqueles afetados com as atividades da firma, como acionistas, empregados, fornecedores, clientes e terceiros".[245] É por meio do código de conduta que a empresa estabelece procedimentos e limites de tolerância e estipula o que é permitido em determinado ambiente e qual a medida organizacional em caso de infração.

Para a criação de um sistema de *Compliance*, criação de padrões de governança corporativa e elaboração de um código de conduta, é necessário amplo conhecimento da empresa e da sua forma da atuação, bem como a avaliação dos riscos inerentes às suas atividades, principalmente nos setores sociais e ambientais. Em se tratando de empresas voltadas à esfera da saúde, o setor social apresenta grande relevância, motivo pelo qual a governança corporativa e o código de conduta devem englobar políticas de combate à discriminação e incentivar o tratamento humanizado independentemente dos contextos pessoal, social e patológico dos pacientes.

A efetividade da conformidade é adstrita à sua propagação e ao seu acolhimento, o que demanda amplo treinamento e comunicação, também recomendados nos sistemas de *Compliance*. A prática de atos condizentes com a atuação empresarial e com as capacitações realizadas pelos agentes garante melhor

---

[244] INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015. p. 18-20.

[245] PORTO, Éderson Garin. ***Compliance* & Governança Corporativa**: uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020. p. 26.

absorção dos ideais pretendidos. Nesse sentido, também é necessário controles internos e externos, com constantes investigações, a fim de assegurar o cumprimento da regulamentação. O sistema de *Compliance* demanda constantes aprimoramentos, revisões e melhorias:

> Uma investigação é um exercício de averiguação de fatos. Investigações devem determinar, de forma plena e com credibilidade, o que aconteceu em relação a um problema – se, de fato, houve uma conduta imprópria ou não, quais foram as circunstâncias, quem estava envolvido, e se uma violação de leis ou políticas internas ocorreu. Investigações devem ser percebidas como tendo sido rigorosas, independentes e analíticas.[246]

As investigações podem ser fomentadas por canais de denúncias, os quais, por sua vez, devem garantir o sigilo das informações e especificar as etapas de apuração, sempre de forma prudente e fundamentada.

Todavia, um sistema de *Compliance*, antes de reativo, é proativo. A atuação preventiva é garantida por meio do mapeamento de riscos, das revisões e das investigações internas e externas. Sem proatividade não existe conformidade. A identificação de falhas antes que se tornem problemas propicia a adoção de medidas resolutivas céleres e otimizadas. Em uma contextualização prática, é mais apropriado prevenir o extravio de medicamentos em razão de imprudências do que punir o agente causador depois de perfectibilizado o dano. E essa prevenção se dá justamente por meio de instruções prévias, treinamentos e supervisões constantes.[247]

No que diz respeito ao tratamento de dados, sua inserção no sistema de *Compliance* é espontânea, na medida em que conformidade (também) significa alinhamento com a legislação vigente e, existindo a Lei Geral de Proteção de Dados Pessoais, essa deve ser englobada pelo programa, principalmente em empresas na área da saúde, que são responsáveis pelo tratamento de dados pessoais sensíveis, assim reconhecidos em razão de seu caráter suscetível e potencial discriminatório.[248]

Assim como *Compliance*, a Lei Geral de Proteção de Dados Pessoais exige dos agentes de tratamento conduta proativa no sentido de identificar os riscos e atenuar os seus efeitos. Para que haja correta implementação da LGPD, a atuação

---

[246] SERPA, Alexandre Cunha. **Investigações de *Compliance***: antes, durante e depois. [*S. l.*]: LEC, c2021. p. 2

[247] SILVA, Daniel C.; COVAC, José R. **Manual de *Compliance***. São Paulo: Editora de Cultura, 2015.p.68.

[248] ASSI, Marcos. ***Compliance***: como implementar. São Paulo: Trevisan, 2018.p.25-38.

da empresa deve ser bem delimitada, bem como seu papel no tratamento de dados, seja como controladora ou operadora.

O mapeamento de dados é a principal ferramenta utilizada na implementação da LGPD. É por meio dele que são analisadas as coletas, finalidades e necessidades, e justificados os armazenamentos e compartilhamentos. Tão logo mapeados os dados, é possível indicar as bases autorizadoras de tratamento e delinear procedimentos de exclusão de dados desnecessários, cujo armazenamento põe em risco o funcionamento empresarial.[249]

Para que seja lícito, o tratamento de dados deve ser restrito a finalidades e propósitos específicos, com delimitação do período do tratamento e exclusão de todos os dados que venham a se tornar desnecessários, o que deve ser garantido por todos os agentes, sejam controladores ou operadores:

> O término do tratamento é outro ponto importante, e a partir do entendimento do ciclo de vida e do mapeamento dos dados será possível determinar quando os dados deixarão de ser necessários, o que, por lei, exige que sejam eliminados para ajudar a identificar quais dados estão em posse da empresa sem que exista um propósito. Por isso, não é mais necessário o seu armazenamento.[250]

Ao mesmo tempo em que são mapeados os dados, os sistemas de segurança devem ser revisados, uma vez que a própria legislação demanda a adoção de medidas técnicas e administrativas aptas a salvaguardar os interesses dos titulares, principalmente no que diz respeito à sua privacidade. A segurança da informação deve ser condizente com o grau de relevância dos dados tratados pela instituição. Por esse motivo, na esfera da saúde, amplamente ligada ao tratamento de dados pessoais sensíveis, a segurança no tratamento dos dados deve ser robusta e constantemente aprimorada.[251]

Há que se ressaltar que o tratamento de dados não se dá apenas de forma digital, uma vez que dados pessoais são, para fins legais, informações relacionadas à pessoa natural identificada ou identificável, sem distinção do meio utilizado (físico ou eletrônico). Dessa forma, formulários eventualmente preenchidos por pacientes e

---

[249] GDPR Data Mapping: What is it and how to comply. *In:* IT GOVERNANCE. [*S. l.*], c2022. Disponível em: https://www.itgovernance.co.uk/gdpr-data-mapping. Acesso em: 7 abr. 2022.n.p.

[250] DONDA, Daniel. **Guia prático de implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020. p. 80.

[251] DONDA, Daniel. **Guia prático de implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.p.81-90.

armazenados em armários devem ser resguardados com a mesma seriedade do que aqueles que constam em servidores de TI.[252]

Em aspectos físicos, sugere-se a limitação de acesso aos locais de armazenamento, requerimentos de senha e outras formas de identificação, instalação de câmeras de segurança e demais funcionalidades sensoriais. No âmbito da tecnologia da informação, é imprescindível a participação de profissionais da área capazes de diagnosticar as potenciais ameaças e implementar mecanismos de segurança adequados à complexidade da empresa, com redução de riscos de vazamento de dados e segredos de negócios, controles de fraude e formalização de diretrizes. Nesse sentido, sugere-se:

> Criar uma política de segurança da informação; coordenar as atividades de segurança da informação; fazer a gestão de ativos; proteger e classificar a informação; garantir a segurança lógica e física do ambiente; acompanhar a gestão de mudanças; gerenciar a segurança e o controle de acesso; detectar atividades não autorizadas por meio do monitoramento do ambiente; fazer a análise de vulnerabilidades; fazer a gestão de incidentes de segurança; implementar um plano de continuidade do negócio; manter conformidade com normas e leis.[253]

No mesmo propósito do sistema de conformidade, também é possível realizar, no âmbito da Lei Geral de Proteção de Dados Pessoais, treinamentos voltados à segurança da informação, com ensinamentos sobre o uso de *logins* e senhas, a atuação correta em equipamentos da instituição, a proibição de utilização de determinados aplicativos e de acesso a *sites* que coloquem em risco a segurança da rede, a proibição de cópias e armazenamento de informações sem autorização dos responsáveis e outras diretrizes que se mostrem adequadas a cada caso concreto. Todo o quadro de colaboradores deve ser conscientizado a respeito da relevância do tema e também de suas respectivas responsabilidades.[254]

As empresas devem investir em segurança da informação, devendo essa abranger todos os setores da empresa. Uma boa política de segurança deve ser fácil

---

[252] BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 1 set. 2020. Art. 1.º e 3.º.

[253] DONDA, Daniel. **Guia Prático de Implementação da LGPD**: conheça estratégias e soluções para adequar sua empresa em conformidade com a Lei. São Paulo: Labrador, 2020. p. 33-34.

[254] ASSI, Marcos. **Governança, Riscos e *Compliance***: Mudando a Conduta nos Negócios. São Paulo: Saint Paul, 2019.p.51.

de entender a fim de que todos a compreendam e para que seja colocada em prática com rigor e energia passíveis de sanções aos que ousarem violá-la dentro de clínicas, hospitais, *etc*.

Quanto à possibilidade de denúncias, em se tratando de proteção de dados, a própria Agência Nacional de Proteção de Dados (ANPD) disponibiliza, em seu *site*, canal específico para queixas e delações. Todavia, a fim de garantir maior celeridade e efetividade na condução das apurações, sugere-se que a empresa conte com canal próprio de denúncias.[255]

Em se tratando de profissional de saúde autônomo, apesar da complexidade dos sistemas ser mitigada por menor estrutura e fluxo de dados, a legislação não diferencia sua responsabilidade frente ao tratamento de dados. Por esse motivo, seja o agente de tratamento uma grande instituição, uma empresa de médio porte ou um profissional autônomo, o tratamento de dados pessoais deve ser feito com seriedade e responsabilidade, e com a segurança que dele se espera.[256]

Assim, a concretização de um sistema de *Compliance* efetivo é obrigação de todos que atuam dentro de uma organização, não existindo uma receita exata para orientar as empresas sobre a sua implementação, a qual dependerá da avaliação de riscos, pois cada instituição possui suas ameaças e vulnerabilidades.

Por isso a importância do elemento diretivo de governança corporativa, do comprometimento e do apoio da alta liderança, bem como da estruturação e do pleno funcionamento do *Compliance*, padrões de conduta, políticas e procedimentos, educação contínua e comunicação efetiva entre as partes. Com relação às formas de

---

[255] DENÚNCIA de descumprimento da LGPD. *In:* BRASIL. Presidência da República. **Autoridade Nacional de Proteção de Dados**. Brasília, 9 nov. 2021. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-de-descumprimento-da-lgpd. Acesso em: 5 set. 2022.n.p.

[256] "Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
I – a operação de tratamento seja realizada no território nacional;
II – 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 território nacional; ou
III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
§ 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
§ 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei." (BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 out. 2022. Art. 3.º.)

prever e detectar riscos, menciona-se a análise de riscos de *Compliance*, o canal de denúncias ou ouvidoria, o *due diligence* quando das contratações, os registros contábeis, a auditoria, a investigação e o monitoramento contínuo.[257]

[257] CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020. p. 30.

5 CONCLUSÃO

A Lei Geral de Proteção de Dados Pessoais foi implementada no Brasil com objetivo de estabelecer diretrizes a respeito do tratamento de dados, bem como princípios, exigências de segurança e de implementação. Cuidam-se de normas claras e rígidas, que buscam garantir os benefícios que a tecnologias de comunicação e informação propiciam a todos, ao mesmo tempo em que procuram, senão eliminar, ao menos reduzir a possibilidade de utilização de dados pessoais para manipulação das pessoas e influências indevidas.

A existência desta lei no ordenamento jurídico brasileiro decorreu de uma movimentação mundial, mais precisamente, após a entrada em vigor do General Data Protection Regulation (GDPR) Europeu, cuja vigência passou a agilizar a tramitação de Projetos de Lei sobre tratamento de dados pessoais.

O General Data Protection Regulation (GDPR) é considerado um marco a respeito do tratamento de dados mundial, uma vez que passou a exigir, para fins negociais, que outros países implementassem lei específica para esse fim. O referido Regulamento Geral de Proteção de Dados, Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, foi o meio pelo qual a União Europeia veio uniformizar o regime de tratamento de dados, é considerado um requisito essencial para o bom funcionamento do Mercado Único, cujo impacto em relação à proteção da privacidade dos titulares de dados vai para além da União Europeia, a fim de manter as trocas econômicas.

A existência de uma legislação específica no âmbito do Direito brasileiro corresponde ao tema da transparência internacional, com desdobramentos realizados no país por empresas internacionais e nacionais. Desse modo, cuida-se de uma questão de confiabilidade, razão pela qual a segurança da informação e o gerenciamento de risco e os princípios que regem o tema são questões a serem avaliadas.

Com o advento da Lei Geral de Proteção de Dados, o tratamento de dados, no Brasil, foi condicionado ao enquadramento, pelo controlador, às bases autorizadoras previstas no rol taxativo do artigo 7.º da LGPD sendo com relação aos dados pessoais sensíveis, as hipóteses são mais restritivas, uma vez que se está diante de dados de cunho íntimo e que podem apresentar potencial discriminatório.

O tema da proteção de dados é tão salutar que ganhou previsão constitucional

pela Emenda Constitucional n.º 115, de 10 de fevereiro de 2022, a qual alterou a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União a fim de legislar sobre proteção e tratamento de dados pessoais, logo com a promulgação da EC n.º 115/2022, o direito fundamental à proteção de dados pessoais foi alcançada a um direito expressamente positivado na Constituição Federal.

Assim, sejam empresas de grande, médio ou pequeno porte, privadas ou públicas, familiares ou não, todas devem se adequar aos ditames legais e atender às demandas da sociedade, bem como atuar de forma ética e íntegra. A sociedade anseia por empresas mais íntegras, eis que são importantes referências de disseminação cultural e têm a autoridade de induzir seus colaboradores, fornecedores, parceiros e até concorrentes.

Ademais, tem-se uma sociedade cada vez mais direcionada para a economia de dados, e o direito à privacidade tem sido uma constante em todos os assuntos ligados à área da saúde. Por isso, é relevante estar em conformidade com a Lei Geral de Proteção de Dados por ser um requisito legal, mas também porque podem se tornar ativos e passivos de uma empresa, dependendo de sua atuação no mercado.

É indispensável, nesse contexto, a adequação das empresas à Lei Geral de Proteção de Dados Pessoais, sob pena de sofrerem severas punições, seja pelo mercado (que cada vez mais exige postura adequada para transações econômicas), pela sociedade (que pode influenciar na visibilidade da empresa) ou pela possibilidade de aplicação, pela ANPD e pelo Poder Judiciário, de penas pecuniárias altíssimas e indenizações, respectivamente.

O regime de proteção de dados não tem por objetivo apenas tutelar a privacidade dos usuários. A própria lei menciona, em seu art. 1.º, que o seu objetivo diz respeito a proteger “os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural”.

Em seguida, a lei prevê, em seu art. 2.º, os seus fundamentos, os quais são, além da privacidade: a autodeterminação informativa; a liberdade de expressão, de informação, de comunicação e de opinião; a inviolabilidade da intimidade, da honra e da imagem; o desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa; a livre concorrência e a defesa do consumidor; os direitos humanos; o livre desenvolvimento da personalidade; a dignidade e o exercício da cidadania pelas

pessoas naturais.

A respeito do livre desenvolvimento da personalidade, cidadania e dignidade, a lei procura diferenciar muitas das destinações atuais que vêm sendo conferidas aos dados pessoais. Algoritmos, ao processarem dados, são capazes de fazer diagnósticos e classificações dos usuários. Esses diagnósticos e classificações, por sua vez, podem ser utilizados para limitar as possibilidades de vida dos usuários. Além disso, a partir de tais dados, as empresas podem discriminar usuários ou mesmo tentar manipular suas opiniões, crenças ou valores em vários âmbitos, inclusive no político.

Embora a LGPD não trate, pelo menos expressamente, sobre a crescente utilização de algoritmos por agentes empresariais, é inequívoco que os princípios por ela previstos apontam no sentido da necessidade de transparência e prestação de contas sobre qualquer que seja o meio utilizado para o tratamento de dados, o que incluiria o meio algorítmico.

Ademais, insta registrar que, no art. 5.º, a LGPD prevê o relatório de impacto à proteção de dados pessoais, conceituando-o como “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” (inc. XVII), por meio do qual a transparência a respeito do tratamento mais uma vez ganha foco na discussão. Ora, sem a devida transparência sobre como os dados são utilizados, os riscos não podem ser nem suficientemente identificados, nem mitigados.

A movimentação de dados gerou, ainda, armazenamento massificados de dados. Os bancos de dados, nesse contexto, ganharam grande relevância e valor na esfera negocial, oferecendo vantagens na gestão de empresas no âmbito geral e, mais ainda quando se tratam instituições ligadas à saúde da população. Assim, uma política que não proteja os dados pessoais, que permita que eles sejam acessados por terceiros e que não tenha questões de segurança da informação reforçadas acaba sendo uma ameaça à própria organização, seja pelo risco de sanções administrativas ou outras implicações legais, judiciais e indenizatórias que possam decorrer de qualquer questão.

Na área da saúde, recorte dado para o presente estudo, o debate é ainda mais suscetível. Primeiro porque todo e qualquer dado relacionado à saúde do cidadão é

enquadrado como dado pessoal sensível, e segundo porque, em razão do primeiro motivo, a legislação prevê seu tratamento de forma específica, com redobrada cautela e atenção.

Dados de saúde demandam tutela específica, pois têm o condão de deixar o titular mais vulnerável (seja porque apresentam potencial discriminatório ou porque abrangem o que de mais suscetível existe no ser humano: seu bem-estar e sua vitalidade). O cuidado que se exige no tratamento de dados de saúde foi prontamente abrangido pela Lei Geral de Proteção de Dados Pessoais, que os conceituou como sensíveis e determinou procedimento específicos para sua efetivação.

Nesse mesmo sentido, a LGPD vai ao encontro do direito constitucional à proteção de dados, uma vez que proporciona diretrizes para os agentes de tratamento e, ao mesmo tempo, formaliza os direitos dos titulares. A LGPD, ainda, cria um cargo (encarregado) responsável pela comunicação entre titular e agente de tratamento, e estabelece um órgão executivo (ANPD) dedicado ao assunto.

Ressalta-se que o conceito de tratamento é amplo, abrangendo todo e qualquer procedimento realizado com dados pessoais, seja o simples acesso, a coleta, o compartilhamento e até a exclusão. Esse tratamento só pode ser efetivado em caso de enquadramento em uma das bases legais previstas no rol do artigo 7.º da legislação e, em caso de dados pessoais sensíveis, no rol do artigo 11.

Desde logo, esclarece-se que, em relação à tutela da saúde, a análise da hipótese autorizadora contida na alínea “f”, inciso II, do artigo 11, merece melhor destaque. É permitido o tratamento de dados pessoais sensíveis para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária. Sendo assim, médicos, hospitais e clínicas podem, em uma primeira análise, utilizar esse permissivo para o exercício de suas atividades.

É imprescindível a análise das particularidades de cada caso antes da escolha da base autorizadora para tratamento. Todavia, a Lei Geral de Proteção de Dados Pessoais é clara ao autorizar o tratamento de dados pessoais sensíveis para a tutela de saúde sem obrigatoriedade de coleta de consentimento, o qual, por sua vez, também pode ser buscado pelos controladores de forma exclusiva ou cumulativa.

No âmbito prático, apesar de a ANPD ter proporcionado diretrizes diferenciadas para empresas de médio e pequeno porte, o enquadramento à legislação pode se dar

de forma dificultosa, pois muitos agentes de tratamento não estão preparados para, dentro do prazo previsto na legislação, entregar relatórios de impacto ou, em caráter ainda mais preliminar, efetuar o devido mapeamento dos dados, encontrar seu enquadramento legal e efetivar a gestão de todos os riscos inerentes ao seu negócio.

Para fins de exemplificação, tem-se que eventual vazamento de dados de saúde, considerados sensíveis pela própria LGPD, podem gerar diversos danos aos titulares dos dados e também à empresa gestora, responsável pelos dados. Os prejuízos podem ultrapassar — e muito! — as sanções administrativas previstas no artigo 52 da LGPD, uma vez que a problemática pode gerar dever de indenização, sanções judiciais e, ainda, prejuízo à imagem da empresa frente ao mercado de consumo.

Para facilitar e robustecer a implementação da Lei Geral de Proteção de Dados, sugere-se um trabalho simultâneo de *Compliance* de dados, o qual deverá ocorrer de forma multidisciplinar, preventiva e com procedimentos de *checklists* diários. A proteção de dados deve fazer parte da cultura empresarial, e sua importância deve ser compreendida por todos os segmentos.

O sistema de Compliance se mostra fundamental para implementação das boas práticas, que devem ter como pilares fundamentais a integridade, a proteção e a confidencialidade das informações sensíveis de saúde. Os programas de Compliance, quando bem implementados, atuam de forma a mitigar os riscos das instituições, por meio da detecção e prevenção de incidentes e inadequações do tratamento de dados. Outrossim, programas de Compliance possuem como estrutura basilar o cumprimento à legislação, de modo que sua implementação está aliada à implementação da LGPD, pois cuida-se de um imperativo legal.

Assim, a existência de um programa de Compliance que abranja a questão do tratamento de dados é um importantíssimo mecanismo para estruturar, de forma completa, a implementação e fiscalização do cumprimento da Lei Geral de Proteção de Dados Pessoais dentro das empresas.

Para que haja efetividade ao programa de Compliance voltada a área de tratamento de dados ligados à saúde, considerando que se tratam de dados pessoais sensíveis, sugere-se as seguintes diretrizes: buscar entendimento estratégico das necessidade do negócio para melhor perceber a vulnerabilidades e os riscos, bem como as lacunas de atuação econômica, legal e social; implantação de um programa

de boa governança fundado essencialmente em ética corporativa e sistemas de integridade, inclusive em relação a política de tratamento de dados; atuação pontual com gestão de reponsabilidade social e riscos; análise uso de tecnologia adequada para otimização e precisão de troca de informações, adotar controles internos e gerenciamento de custos de governança; promoção de recrutamento de colaboradores adequado às demandas da empresa quanto à gestão responsável; conscientizar através da educação e treinamento; análise da empresa, B2B ou B2C; data mapping; exclusão de dados desnecessários; estabelecimento de políticas; definição clara de papéis e responsabilidades dos gestores; monitoramento; canais de denúncias; órgãos de assessoramento (conselhos de ética, sucessões, remunerações, auditoria, risco *etc*.); nomeação de *Compliance* officer e DPO, em pessoas diferentes para que não haja conflito de interesses; realização de efetivo sistema de gestão de *Compliance*; e, ter subsídios para o adequado tratamento de incidentes que possam acarretar danos aos titulares, proporcionando-lhe segurança jurídica; observar, na adequação à LGPD, os princípios do art. 6º da LGPD, incluindo, mas não se limitando, a finalidade, adequação, transparência e necessidade.

Logo, incluir uma política de tratamento de dados no sistema de Compliance é estar em conformidade, que consequentemente é um cumprimento legal, sendo que a lei estará sendo cumprida se estiver sendo implementada a LGPD, pois do contrário não terá conformidade alguma.

Ponderadas tais questões, tem-se que o ponto de partida para este estudo foram as dúvidas sobre as diretrizes a serem seguidas para a efetivação de programas de *Compliance* envolvendo a proteção de dados, especialmente àquelas relacionadas à saúde, bem como em relação às possibilidades de criação de uma cultura de conformidade dentro das organizações.

Ainda, sob ponto de vista de Compliance digital, temos muitos desafios a serem enfrentados em proteção de dados na área da saúde, sendo eles: integrar a proteção de dados (risco de privacidade e proteção de dados) no sistema de gestão de Compliance; outro deságio é a parte comportamental, que diz respeito aos deslizes éticos de vez em quando, seja porque as pessoas estão distraídos, seja porque são criativas para criar justificativas para seus desvios, e isso costuma ser deixado de lado, mas deveria estar no centro de um programa de Compliance realmente efetivo; ainda temos a necessidade de integração do Compliance ao programa de Governança

e privacidade, conforme inclusive previsto em lei; e, ainda, na área da saúde, mais especificadamente, os desafios são inúmeros e alguns citados aqui: as normas que existem, mas não estão escritas, a exemplo da rastreabilidade, que não existe nenhuma norma da ANVISA a respeito do assunto, (exemplo: nome do paciente na nota fiscal, não há previsão na lei), são práticas da área da saúde que não tem nenhuma norma para ser enquadrada, ou seja, são hábitos de mercado, que as pessoas associam a norma ou seja, sendo um desafio para a LGPD que por vezes não se enquadram em nenhuma base legal, e acaba sendo tratado como legítimo interesse, o tratamento de dados é necessário mas nem sempre se mostra claro qual base legal deve ser enquadrada; outro desafio, são o tratamento de dados e as fraudes, existem diversas exigências do mercado para prevenir as fraudes, mas que acabam expondo dados das pessoas, e novamente, nem sempre haverá base legal para sustentar esse tipo de prática (exemplo: enviar RX para o plano de saúde afim de comprovar se de fato foram colocados os parafusos efetivamente necessários); temos também a necessidade de anonimização de dados e do outro lado devendo manter toda a cadeia de estoque e logística; a telemedicina também é um desafio à parte (exemplo: uso de devices, whatsapp), também não estão previstos1 na norma, como lidar.

Diante de todos os desafios, uma proposta a fim de solucionar seria desenvolver um acordo setorial que fosse chancelado pela ANPD, para ter as peculiaridades da área da saúde bem definidas, pois é muito difícil resolver os problemas individualmente, afim de que esses desafios fossem operacionalizados, criando uma auto regulação por setores. Importante destacar que o elevado fluxo de dados nas relações de saúde assumem grandes proporções e atrai especial atenção sobre a questão.

Apesar do enfoque a respeito do tema, o Brasil ainda se encontra em estágio inicial para a concretização de boas práticas envolvendo o tratamento de dados. Isso significa que o primeiro desafio envolvendo a questão é justamente a conscientização — pública e privada, dos cidadãos e das instituições — da importância e influência que as informações disseminadas exercem sobre cada indivíduo e cada esfera da coletividade.

Especialmente em consultórios médicos, ambientes hospitalares e empresas atuantes na área da saúde (como, por exemplo, planos de saúde), o respeito à

privacidade e intimidade dos pacientes deve ser tido como primordial. Um exemplo da preservação dos direitos dos pacientes, ainda anterior à vigência da Lei Geral de Proteção de Dados Pessoais, é existência de sigilo entre médico e paciente, que implica a não obrigatoriedade de preenchimento da CID (Classificação Internacional de Doenças) em atestados médicos.

Conforme já mencionado, os dados voltados à saúde se relacionam ao que de mais suscetível existe no ser humano. Por esse motivo, o cumprimento às diretrizes legais deve ter redobrada cautela e atenção, o que é possível por meio da implementação concomitante de um sistema de Compliance de dados. Tal procedimento garante não só a higidez das medidas adotadas no âmbito da LGPD, como também auxilia na criação de uma cultura de governança, em mecanismos de fiscalização e promoção de treinamentos dentro de cada setor.

REFERÊNCIAS

AHRENS, Herold. **Accountability no âmbito da governança das Organizações públicas não estatais**: o caso do Instituto de matemática pura e aplicada. 2018. Dissertação (Mestrado em Administração) – Faculdade de Economia, Administração, Contabilidade e Gestão de Políticas Públicas, Faculdade de Brasília, Brasília, 2018. Disponível em: https://repositorio.unb.br/bitstream/10482/33179/3/2018_HeroldAhrens.pdf. Acesso em: 5 set. 2022.

AMARAL, Francisco. **Direito Civil**. São Paulo: Saraiva, 2018.

ANDRADE, Adriana; ROSSETTI, José Paschoal. **Governança Corporativa**: Fundamentos, Desenvolvimento e Tendências. São Paulo: Atlas, 2009.

ASSI, Marcos. ***Compliance***: como implementar. São Paulo: Trevisan, 2018.

ASSI, Marcos. **Governança, Riscos e *Compliance***: Mudando a Conduta nos Negócios. São Paulo: Saint Paul, 2019.

BALLOU, Ronald H. **Gerenciamento da Cadeia de Suprimentos/Logística Empresarial.** São Paulo: Bookman, 2006.

BANDAROVSKY, Bruno Pires. *Compliance* Risk Assessment em 8 passos. s.n. *In:* LEC. Disponível em: https://conteudo.lec.com.br/*Compliance*-risk-assessment-em-8-passos. Acesso em: 14 jun. 2022.

BASRI, Carole. **Corporate *Compliance***. North Carolina: Carolina Academic Press, 2017. *E-book*.

BAUMAN, Zygmunt; LYON, David. **Vigilância líquida**. Argentina: Paidós, 2013.

BERNASIUK, Helen Lentz Ribeiro. **Liberdade de pesquisa genética humana e a necessidade de proteção dos dados genéticos**. Rio de Janeiro: Lumen Juris, 2021.

BEVILÁQUA, Clóvis. **Teoria Geral do Direito Civil**. São Paulo: Servanda, 2015.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: A função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLOCK, Marcella. ***Compliance* e Governança Corporativa.** Rio de Janeiro: Freitas Bastos, 2017.

BRASIL está entre os maiores consumidores de medicamentos. **Global Med**, [*s. l.*], 2021. Disponível em:https://globalmedreport.com.br/2021/05/24/brasil-esta-entre-os-maiores-consumidores-de-medicamentos/ Acesso em: 4 nov. 2021.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 24 jan. 2022.

BRASIL. Autoridade Nacional de Proteção de Dados. **Segurança da informação para agentes de tratamento de pequeno porte.** Brasília, DF: ANPD, out. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-vf.pdf. Acesso em: 2 ago. 2022.

BRASIL. Câmara dos Deputados. **CPI – Máfia das órteses e próteses no Brasil**. Brasília, DF: Câmara dos Deputados, 2015. Disponível em: https://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-mafia-das-orteses-e-proteses-no-brasil. Acesso em: 13 set. 2022.

BRASIL. Câmara dos Deputados. Saúde pública no Brasil ainda sofre com recursos insuficientes. **Agência Câmara de Notícias**, Brasília, 8 jan. 2015. Disponível em: https://www.camara.leg.br/noticias/448436-saude-publica-no-brasil-ainda-sofre-com-recursos-insuficientes/. Acesso em: 9 fev. 2022.

BRASIL. **Decreto n.º 8.420, de 18 de março de 2015**. Regulamenta a Lei n.º 12.846, de 1.º de agosto de 2013, que dispõe sobre a responsabilização administrativa de pessoas jurídicas pela prática de atos contra a administração pública, nacional ou estrangeira e dá outras providências. Brasília, DF: Presidência da República, 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/decreto/d8420.htm. Acesso em: 22 jun. 2022.

BRASIL. **Emenda Constitucional n.º 115, de 10 de fevereiro de 2022**. Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais. Brasília, DF: Presidência da República, 2022. Disponível em: http://www.planalto.gov.br/ccivil_03/consti tuicao/Emendas/Emc/emc115.htm. Acesso em: 02 ago. 2022.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Brasília: SDE/DPDC, 2010.

BRASIL. **Lei n.º 12.842, de 10 de julho de 2013**. Dispõe sobre o exercício da Medicina. Brasília, DF: Presidência da República, 2012. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12842.htm. Acesso em: 20 jun. 2022.

BRASIL. **Lei n.º 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 out. 2022.

BRASIL. **Lei n.º 6.360, de 23 de setembro de 1976**. Dispõe sobre a vigilância sanitária a que ficam sujeitos os medicamentos, as drogas, os insumos farmacêuticos e correlatos, cosméticos, saneantes e outros produtos, e dá outras providências. Brasília, DF: Presidência da República, 1976. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l6360.htm. Acesso em: 1 dez. 2021.

BRASIL. **Lei n.º 8.080, de 19 de setembro de 1990**. Dispõe sobre as condições para a promoção, proteção e recuperação da saúde, a organização e o funcionamento dos serviços correspondentes e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8080.htm. Acesso em: 14 jun. 2022.

BRASIL. **Lei n.º 9.782, de 26 de janeiro de 1999**. Define o Sistema Nacional de Vigilância Sanitária, cria a Agência Nacional de Vigilância Sanitária e dá outras providências. Brasília, DF: Presidência da República, 1999. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9782.htm. Acesso em: 1 dez. 2021.

BRASIL. **Lei n.º 9.961, de 28 de janeiro de 2000**. Cria a Agência Nacional de Saúde Suplementar – ANS e dá outras providências. Brasília, DF: Presidência da República, 2000. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9961.htm. Acesso em: 1 dez. 2021.

BRASIL. Ministério da Economia. **Superintendência de Seguros Privados**. Brasília, DF, 2022. Disponível em: https://www.gov.br/susep/pt-br. Acesso em: 1 nov. 2022.

BRASIL. Ministério da Saúde. **Agência Nacional de Vigilância Sanitária**. Brasília, DF, 2022. Disponível em: https://www.gov.br/anvisa/pt-br. Acesso em: 19 out. 2022.

BRASIL. Ministério da Saúde. *In:* PORTAL brasileiro de dados abertos. Brasília, [202?]. Disponível em: https://dados.gov.br/organization/about/ministerio-da-saude-ms. Acesso em: 13 set. 2022.

BRASIL. Ministério da Saúde. **Portaria n.º 467, de 20 de março de 2020**. Dispõe, em caráter excepcional e temporário, sobre as ações de Telemedicina, com o objetivo de regulamentar e operacionalizar as medidas de enfrentamento da emergência de saúde pública de importância internacional previstas no art. 3.º da Lei n.º 13.979, de 6 de fevereiro de 2020, decorrente da epidemia de COVID-19. Brasília, DF: Gabinete do Ministro, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/Portaria/PRT/Portaria%20n%C2%BA%20467-20-ms.htm. Acesso em: 22 jun. 2022.

BRASIL. Ministério da Saúde. **Transformação digital para o SUS**. s.n. Disponível em: https://datasus.saude.gov.br/. Acesso em: 8 nov. 2021.

BRASIL. **Projeto de Lei n.º 21/2020**. Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil e dá outras providências. Brasília: Senado Federal, 2020. Disponível em: https://www.camara.leg.br/propostas-legislativas/2236340. Acesso em: 15 ago. 2022.

CANOTILHO, J. J. Gomes. **Direito Constitucional e teoria da Constituição**. Coimbra: Almedina, 2017.

CARLINI, Angélica; SAAVEDRA, Giovani Agostini (coord.). ***Compliance* na área da saúde**. Indaiatuba: Foco, 2020.

CARLOTO, Selma; GUERRA, Elaine. **Manual Prático de Adequação à LGPD**: Com enfoque nas relações de trabalho. São Paulo: LTr, 2021.

COIMBRA, Marcelo de Aguiar; MANZI, Vanessa A. **Manual de *Compliance***. Preservando a Boa Governança e a Integridade das Organizações. São Paulo: Atlas, 2010.

COLOMBO, Cristiano; ENGELMANN, W. . Inteligência Artificial em favor da saúde: proteção de dados pessoais e critérios de tratamento em tempos de pandemia. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CÈSAR, Joaquim Portes de Cerqueira (org.). **Inteligência Artificial aplicada ao processo de tomada de decisões**. Belo Horizonte: Editora D'Plácido, 2020. v. 1.

COLOMBO, Cristiano; FACCHINI NETO, Eugênio. Violação dos direitos de personalidade no meio ambiente digital: a influência da jurisprudência europeia na fixação da jurisdição/competência dos tribunais brasileiros. **Civilistica.com**, Rio de Janeiro, v. 8, n. 1, p. 9, 2019. Disponível em: http://civilistica.com/violacao-dos-direitos-de-personalidade/. Acesso em: 5 set. 2022.

COLOMBO, Cristiano; GOULART, Guilherme Damasio. Inteligência artificial aplicada a perfis e publicidade comportamental: proteção de dados pessoais e novas posturas em matéria de discriminação abusiva. *In*: PINTO, Henrique Alves; GUEDES, Jefferson Carús; CERQUEIRA, Joaquim Portes de. (org.). **Inteligência artificial aplicada ao processo de tomada de decisões**. São Paulo: D'Plácido, 2020.

CONFEDERAÇÃO NACIONAL DE SAÚDE. Código de Boas Práticas: proteção de dados para prestadores privados de serviços em saúde. [*S. l.: s. n.*], 2021. Disponível em: http://cnsaude.org.br/wp-content/uploads/2021/03/Boas-Praticas-Protecao-Dados-Prestadores-Privados-CNSaude_ED_2021.pdf. Acesso em: 02 set. 2022.

CONSUMERS INTERNATIONAL. **Consumers International**: Strategy. [*S. l.*]: Consumers International, 2018. Disponível em: https://www.consumersinternational.org/media/155232/strategy-eng.pdf. Acesso em: 7 jul. 2021.

COSO. **Gerenciamento de Riscos Corporativos** – estrutura integrada. [*S. l.*]: PricewaterhouseCoopers, 2007.

COSTA, Luiz. Privacy and the precautionary principle. **Computer Law & Security Review**, [*s. l.*], v. 28, p. 14-24, 2012.

COSTA, Márcio Roberto; TORRES JÚNIOR, Noel. Gestão da Cadeia de Suprimentos de Serviços: uma análise das atividades operacionais logísticas de empresas exibidoras de filmes de longa-metragem de Belo Horizonte. **Gestão da Produção, Operações e Sistemas**, Bauru, Ano 9, n. 3, p. 61-78, jul./set. 2014. Disponível em: https://revista.feb.unesp.br/index.php/gepros/article/viewFile/1050/589. Acesso em: 28 jun. 2020.

COTS, Márcio; OLIVEIRA, Ricardo. **Lei Geral de Proteção de Dados Pessoais Comentada**. 2. ed. São Paulo: Thomson Reuters Brasil, 2019.

COUTINHO, Francisco Pereira; MONIZ, Graça Canto (coord.). **Anuário da proteção de dados**. Lisboa: CEDIS, 2019. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2019/06/anuario-da-protecao-de-dados-2019.pdf. Acesso em: 7 jul. 2021.

CRANE, Andrew; MATTEN, Dirk. **Business Ethics**: Managing corporate citizenship and sustainability in the age of globalization. 3. ed. Oxford University Press, 2010. Disponível em: https://books.google.com.br/books?id=J8-SDAAAQBAJ&printsec=frontcover&redir_esc=y#v=onepage&q&f=false. Acesso em: 14 jun. 2022.

CRESPO, Liana Irani Affonso Cunha. ***Compliance* officer e efetividade**: sobre as condições necessárias para garantir a ação efetiva do programa de *Compliance*. 2021. Dissertação (Mestrado em Direito Político e Econômico) – Programa de Pós-Graduação em Direito Político e Econômico, Universidade Presbiteriana Mackenzie, São Paulo, 2021. Disponível em: https://dspace.mackenzie.br/handle/10899/28412. Acesso em: 11 set. 2022.

CUEVA, Ricardo Villas Boas. Funções e finalidades dos programas de *Compliance. In*: CUEVA, Ricardo Villas Boas; FRAZAO, Ana (coord.). *Compliance*: perspectivas e desafios dos programas de conformidade. Belo Horizonte: Fórum, 2018.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance* e Política de Proteção de Dados**. São Paulo: Thomson Reuters Brasil, 2021.

CUEVA, Ricardo Villas Bôas; FRAZÃO, Ana (coord.). ***Compliance***: Perspectivas e Desafios dos programas de conformidade. Belo Horizonte: Fórum, 2019.

DENÚNCIA de descumprimento da LGPD. *In:* BRASIL. Presidência da República. **Autoridade Nacional de Proteção de Dados**. Brasília, 9 nov. 2021. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/cidadao-titular-de-dados/denuncia-de-descumprimento-da-lgpd. Acesso em: 5 set. 2022.

DEODATO, Sérgio. **A proteção dos dados pessoais de saúde**. Lisboa: Universidade Católica, 2017.

DERMARTINI, Felipe. O que as farmácias fazem com o seu CPF? Governo questiona uso de dados. **Canaltech**, [*s. l.*], 17 nov. 2021. Disponível em: https://canaltech.com.br/seguranca/o-que-as-farmacias-fazem-com-o-seu-cpf-governo-questiona-uso-de-dados-201966/. Acesso em: 13 out. 2022.

DINIZ, Maria Helena. **Curso de direito civil brasileiro**. 26. ed. São Paulo: Saraiva, 2010.

DIREITO à privacidade., *In:* ENCICLOPÉDIA Jurídica da PUCSP. São Paulo, 2022. Disponível em: https://enciclopediajuridica.pucsp.br/verbete/71/edicao-1/direito-a-privacidade. Acesso em: 23 jun. 2022.

DONDA, Daniel. **Guia prático de implementação da LGPD**: tudo o que sua empresa precisa saber para estar em conformidade. São Paulo: Labrador, 2020.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

DONEDA, Danilo. **Manual de proteção de dados pessoais**. Brasília: SDE/DPDC, 2010.

EUROPEAN UNION. Regulamento (UE) 2016/679, de 27 de abril de 2016. General Data Protection Regulation. **Official Journal of the European Union**, Brussels, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL. Acesso em: 22 jun. 2022.

FACHINI NETO, Eugênio; DEMOLINER, Karine Silva. Direito à Privacidade e Novas Tecnologias: Breves Considerações Acerca da Proteção de Dados Pessoais no Brasil e na Europa. **Revista Internacional Consinter de Direito**, [*s. l.*], n. 7, p. 19-40, 2.º semestre de 2018.

FARHAT, Saïd. **Lobby**: o que é, como se faz - ética e transparência junto a governos. São Paulo: Aberje, 2007.

FEDERAÇÃO BRASILEIRA DE HOSPITAIS. **Cenário dos hospitais no Brasil 2019**. [*S. l.: s. n.*], 2019. Disponível em: http://cnsaude.org.br/wp-content/uploads/2019/05/CenarioDosHospitaisNoBrasil2019CNSaudeFBH.pdf. Acesso em: 4 nov. 2021.

FEIGELSON, Bruno; SIQUEIRA, Antonio Henrique Albani. **Comentários à Lei Geral de Proteção de Dados**: Lei 13.709/2018. São Paulo: Thomson Reuters, 2019.

FERMENTÃO, Cleide Aparecida Gomes Rodrigues. Os direitos da personalidade como direitos essenciais e a subjetividade do direito. **Revista Jurídica CESUMAR**, Maringá, v. 6, n. 1, p. 241-266, 2006. Disponível em: https://periodicos.unicesumar.edu.br/index.php/revjuridica/article/view/313. Acesso em: 28 jun. 2022.

FERNANDES, Daniela. Pandemia evidencia que Brasil gasta pouco e mal em saúde pública, diz diretor da OCDE. **UOL**, São Paulo, 24 jul. 2020. Disponível em: https://economia.uol.com.br/noticias/bbc/2020/07/24/pandemia-evidencia-que-brasil-gasta-mal-em-saude-publica-diz-diretor-da-ocde.htm. Acesso em: 4 nov. 2021.

FRAZÃO, Ana. Programas de *Compliance* e Critérios de Responsabilização de Pessoas Jurídicas por Atos Ilícitos Administrativos. *In*: ROSSETI, Maristela Abla. PITTA, André Grunspun (coord.). **Governança corporativa**: avanços e retrocessos.

São Paulo: Quartier Latin, 2017.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. *Compliance* de dados pessoais. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

FULLER, Greice Patrícia; FIGUEIREDO, Leidi Priscila. *Compliance* empresarial e tutela penal na sociedade da informação. **Revista dos Tribunais**, São Paulo, v. 996, p. 573-588, out. 2018.

GALVANI, Nathalia. Google anuncia plataforma de coleta de dados em tempo real sobre a COVID-19. **Estado de Minas**, [*s. l.*], 26 fev. 2021. Tecnologia. Disponível em: https://www.em.com.br/app/noticia/tecnologia/2021/02/26/interna_tecnologia,1241263/google-anuncia-plataforma-de-coleta-de-dados-em-tempo-real-sobre-a-covid-19.shtml Acesso em: 22 jun. 2022.

GARCIA, Lara Rocha *et al.* **LGPD**: Guia para implementação. São Paulo: Blucher, 2020.

GDPR Data Mapping: What is it and how to comply. *In:* IT GOVERNANCE. [*S. l.*], c2022. Disponível em: https://www.itgovernance.co.uk/gdpr-data-mapping. Acesso em: 7 abr. 2022.

GIOVANELLA, Ligia *et al.* Saúde da família: limites e possibilidades para uma abordagem integral de atenção primária à saúde no Brasil. **Ciência da Saúde Coletiva**, [*s. l.*], v. 14, n. 3, jun. 2009. Disponível em: https://www.scielo.br/j/csc/a/XLjsqcLYxFDf8Y6ktM4Gs3G/?lang=pt. Acesso em: 14 jun. 2022.

GUIA de Boas Práticas – Lei Geral de Proteção de Dados (LGPD). *In:* BRASIL. **Governo Digital.** [Brasília, 2020]. Disponível em: https://www.gov.br/governodigital/pt-br/governanca-de-dados/guia-de-boas-praticas-lei-geral-de-protecao-de-dados-lgpd. Acesso em: 31 ago. 2020.

HEALEY, Robert. **Data Mapping and GDPR *Compliance***: What your business needs to know. United Kingdom, Aug. 2022. Disponível em: https://formiti.com/data-mapping-and-gdpr-*compliance*-what-your-business-needs-to-know/. Acesso em: 13 out. 2022.

INSTITUTO ARC. São Paulo, 2022. Disponível em: http://www.instituto-arc.com/. Acesso em: 19 out. 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das melhores práticas de governança corporativa**. 5. ed. São Paulo: IBGC, 2015. Disponível em: https://conhecimento.ibgc.org.br/Lists/Publicacoes/Attachments/21138/Publicacao-IBGCCodigo-CodigodasMelhoresPraticasdeGC-5aEdicao.pdf. Acesso em: 14 jun. 2022.

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Gerenciamento de Riscos Corporativos**: evolução em governança estratégia. São Paulo: IBCG, 2017.

JANKAVSKI, André. Novo ministro da Saúde é escolhido: quanto essas trocas afetam a economia?. **CNN Brasil**, Brasília, 16 mar. 2021. Disponível em: https://www.cnnbrasil.com.br/business/novo-ministro-da-saude-e-escolhido-quanto-essas-trocas-afetam-a-economia/. Acesso em: 13 set. 2022.

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da lei nº 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Thomson Reuters Brasil, 2019.

KRAUS, R. S. **Statistical Déjà Vu**: The National Data Center Proposal of 1965 and Its Descendants. Miami: [*s. n.*], 2011. Disponível em: https://www.census.gov/history/pdf/kraus-natdatacenter.pdf. Acesso em: 29 jun. 2022.

LAEBER, Márcio Rafael Silva. Proteção de dados pessoais: o direito à autodeterminação informativa. **Revista de Direito Bancário e do Mercado de Capitais**, São Paulo, n. 37, p. 59, jul. 2007.

LEMOS, Ricardo. Gerenciamento de Riscos Corporativos. *In:* LAMBOY, Christian K. (coord.). **Manual de *Compliance***. São Paulo: Via Ética, 2018.

LOPES, Iago Franca; BEUREN, Ilse Maria; VICENTE, Ernesto Fernando Rodrigues. Associação da Evidenciação do Gerenciamento de Riscos com Governança Corporativa e Desempenho em Empresas com ADRs. **Revista Evidenciação Contábil & Finanças**, *[s. l.]*, v. 9, n. 1, p. 5–21, 2021. Disponível em: https://periodicos.ufpb.br/ojs2/index.php/recfin/article/view/52215. Acesso em: 7 jul. 2021.

MACHADO, Cristiani Vieira; LIMA, Luciana Dias de; BAPTISTA, Tatiana Wargas de Faria. Princípios organizativos e instâncias de gestão do SUS. *In:* QUALIFICAÇÃO de gestores do SUS. [*S. l.: s. n.*]. p. 47-72. Disponível em: http://www5.ensp.fiocruz.br/biblioteca/dados/txt_339793983.pdf. Acesso em: 19 nov. 2021.

MAGRANI, Eduardo. **Entre Dados e Robôs**: Ética e Privacidade na Era da Hiperconectividade. [*S. l.*]: Arquipelago Editorial, 2019. (Pautas em Direito Vol. 5).

MARQUES, Antônio Jorge de Souza *et al.* **Direito à saúde, cobertura universal e integralidade possível**. [*S. l.: s. n.*], 2016. Disponível em: https://www.almg.gov.br/export/sites/default/acompanhe/eventos/hotsites/2016/encontro_internacional_saude/documentos/textos_referencia/00_palavra_dos_organizadores.pdf. Acesso em: 3 set. 2022.

MENDES, Laura Schertel *et al.* (coord.). **Proteção de dados para prestadores privados em saúde**. [*S. l.*]: Confederação Nacional de Saúde, 2021.

MENDES, Laura Schertel Ferreira; DONEDA, Danilo César Maganhoto. Comentário

à nova Lei de Proteção de Dados (Lei 13.709/2018): o novo paradigma da Proteção de Dados no Brasil. **Revista de Direito do Consumidor**, São Paulo, v. 27, n. 120, p. 555-587, nov./dez. 2018.

MIRAGEM, Bruno. A internet das coisas e os riscos do admirável mundo novo. **Consultor Jurídico**. São Paulo, 29 mar. 2017. Disponível em: https://www.conjur.com.br/2017-mar-29/garantias-consumo-internet-coisas-riscos-admiravel-mundo. Acesso em: 7 jul. 2021.

MIRANDA, Pontes de. **Tratado de direito privado**. São Paulo: Revista dos Tribunais, 2012.

MONTEIRO, António Pinto. A proteção do consumidor em Portugal e na União Europeia: o olhar de um europeu. *In:* INSTITUTO ÍTALO-IBERO-BRASILEIRO DE ESTUDOS JURÍDICOS. [*S. l., s. n.*], 12 jul. 2022. Disponível em: https://institutoiib.org/protecao-do-consumidor/. Acesso em: 11 set. 2022.

NEVETT, Joshua. Coronavírus: o presidente revelou meu diagnóstico de covid-19 ao vivo na TV. **BBC**, São Paulo, 6 maio 2020. Disponível em: https://www.bbc.com/portuguese/internacional-52561909. Acesso em: 22 jun. 2022.

NISSENBAUM, Helen. **Privacy in Context Technology, Policy, and the Integrity of Social Life**. [*S. l.*]: Stanford Law Books, 2009.

O QUE os consumidores e as empresas sabem sobre LGPD e o que estão fazendo a respeito?. **Serasa experian**, São Paulo, 16 jul. 2019. Disponível em: https://www.serasaexperian.com.br/conteudos/protecao-de-dados/pesquisa-o-que-os-consumidores-e-as-empresas-sabem-sobre-lgpd-e-o-que-estao-fazendo-a-respeito/. Acesso em: 25 out. 2022.

OLIVEIRA, Andréa Cristina de Jesus. Breve histórico sobre o desenvolvimento do lobbying no Brasil. **Revista de Informação Legislativa**, Brasília, v. 42, n. 168, p. 29-43, out. 2005. Disponível em: https://pergamum.tjrs.jus.br/pergamumweb/vinculos/00000d/00000d2e.pdf. Acesso em: 2 ago. 2022.

OLIVEIRA, Ualison Rébula de *et al.* The ISO 31000 standard in supply chain risk management. **Journal of Cleaner Production**, [*s. l.*], v. 151, p. 616-633, 2017.

PAIVA, Maria Teresa Pacheco Sampaio de. A Importância da Disseminação da Cultura da Proteção de Dados. **Âmbito Jurídico**, São Paulo, 1 maio 2022. Disponível em: https://ambitojuridico.com.br/cadernos/direito-civil/a-importancia-da-disseminacao-da-cultura-da-protecao-de-dados-2/ Acesso em: 13 out. 2022.

PARLAMENTO EUROPEU. **Directiva 95/46/CE, de 24 de outubro de 1995**. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial, Luxemburgo, n.º L 281 de 23/11/1995 p. 0031 – 0050. Disponível em: https://eurlex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:31995L0046. Acesso em: 21 jun. 2022.

PINHEIRO, Patrícia P. **Proteção de dados pessoais**: comentários à lei n.

13.709/2018 LGPD. São Paulo: Saraiva Educação, 2018.

PINTO, Gabriel Nogueira Portella Nunes. LGPD e o impacto nas micro e pequenas empresas. **Revista Governança e *Compliance***, Rio de Janeiro, v. 4, n. 8, p. 16-17, abr. 2021. Disponível em: https://acrj.org.br/wpcontent/uploads/2021/04/revista_governanca_*Compliance*_abr_2021_14_04.pdf. Acesso em: 7 jun. 2021.

PIURCOSKY, Fabrício Peloso *et al*. A lei geral de proteção de dados pessoais em empresas brasileiras: uma análise de múltiplos casos. **Suma neg**., Bogotá, v. 10, n. 23, p. 89-99, s.n.Disponível em: http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2215-910X2019000300089&lng=en&nrm=iso. Acesso em: 5 maio 2022.

PORTO, Éderson Garin. ***Compliance* & Governança Corporativa**: uma abordagem prática e objetiva. Porto Alegre: Lawboratory, 2020.

POULLET, Y.; ASINARI, M. V. P.; PALAZZI, P. A. Derecho a la indimidad y protección de datos personales. Buenos Aires: Heliasta, 2014.

PRIVACY. *In:* STANFORD Encyclopedia of Philosophy Archive. [*S. l.*], Spring 2018. Disponível em: https://plato.stanford.edu/archives/spr2018/entries/privacy/. Acesso em: 20 jun. 2022.

PROTEÇÃO de dados pessoais: privacidade versus avanço tecnológico Rio de Janeiro: Fundação Konrad Adenauer, outubro 2019. (Cadernos Adenauer xx, n. 3).

REINALDO FILHO, Demócrito. A Diretiva Europeia sobre a proteção de dados pessoais. **Jus Navigandi**, Teresina, 6 fev. 2013. Disponível em: https://jus.com.br/artigos/23669/a-diretiva-europeia-sobre-protecao-de-dados-pessoais. Acesso em: 12 set. 2022.

RICARDO, José. Processo de gestão de riscos ISO 31000. **Administradores.com**, [*s. l.*], 27 nov. 2010. Café com ADM. Disponível em: https://administradores.com.br/artigos/processo-de-gestao-de-riscos-iso-31000. Acesso em: 15 jun. 2022.

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Rio de Janeiro: Renovar, 2008.

RUGGLES, R. *et al.* **Report of the Committee on the Preservation and Use of Economic Data (1965)**. [*S. l.: s. n.*]. Disponível em: https://ia800200.us.archive.org/31/items/ReportOfTheCommitteeOnThePre servation AndUseOfEconomicData1965/Ruggles_econdata_1965.pdf. Acesso em: 29 jun. 2022.

SAAVEDRA, Giovani (org.). **Prevenção à corrupção e *compliance***. 2. ed. São Paulo: ESENI, 2019.

SAAVEDRA, Giovani Agostini. ***Compliance* na área da saúde**. Brasil: Lykoscatle, 2016.

SAFARI. **La chasse aux Français 40 ans après**. [*S. l.*], 2018. Disponível em: https://donneesouvertes.info/2018/01/26/safari-la-chasse-aux-francais-40-ans-apres. Acesso em: 29 jun. 2022.

SAITO, R.; SCHIOZER, R. F. Uso de derivativos em empresas não-financeiras listadas em bolsa no Brasil. **RAUSP Management Journal**, [*s. l.*], v. 42, n. 1, p. 97-107, 2007.

SARLET, Ingo. Fundamentos constitucionais: o direito à proteção de dados. In: DONEDA, Danilo et al. Tratado de proteção de dados pessoais. Rio de Janeiro: Forense, 2021.

SCHERTEL, Laura Mendes; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista dos Tribunais**, São Paulo, v. 120, p. 469-483, 2018.

SCHMIDT, Eric; COHEN, Jared. **The New Digital Age**: Reshaping the Future of People, Nations and Business. London: John Murray, 2014.

SCHREIBER, Anderson. **Direitos da Personalidade**. 3. ed. São Paulo: Atlas, 2014.

SCHWAB, Klaus. **A quarta revolução industrial**. São Paulo: Edipro, 2016.

SER gestor municipal do SUS. [*S. l.: s. n.*], abr. 2021. Disponível em: https://gestaosus.suprema.edu.br/ser-gestor-sus.pdf. Acesso em: 13 set. 2022.

SERPA, Alexandre Cunha. **Investigações de *Compliance***: antes, durante e depois. [*S. l.*]: LEC, c2021.

SILVA, Daniel C.; COVAC, José R. **Manual de *Compliance***. São Paulo: Editora de Cultura, 2015.

SILVA, Nelson Ricardo *et al.* **Análise De Risco Parametrizada 2.0**: Manual prático de Governança voltada para a Gestão de Risco. São Paulo: PoloBooks, 2017.

SIMITIS, S. Il contesto giuridico e político della tutela della privacy. **Rivista Critica**

SOUSA, Paulo (org.). **Segurança do paciente**: conhecendo os riscos nas organizações de saúde 2. ed. Rio de Janeiro: Fiocruz, 2019.

STEINBERG, Richar M. **Governance, Risk Management, and *Compliance* It Can't happen to Us-Avoiding Corporate Disaster While Driving Success**. [*S. l.: s. n.*], 2011.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**, Rio de Janeiro, v. 9, n. 1, 2020. Disponível em: http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/. Acesso em: 28 jun. 2021.

TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato. **A Lei Geral De Proteção De Dados Pessoais e suas Repercussões no Direito Brasileiro**. São

Paulo: Revista dos Tribunais, 2019.

TRILHO, Alvaro. **Gerenciamento de Riscos e o Papel do profissional de Riscos**. IBGC Análises & Tendências, [*s. l.*], 4. ed., jul. 2018. Disponível em: https://www.bibliotecadeseguranca.com.br/wp-content/uploads/2018/08/ibcg-analises-e-tendencias-gerenciamento-de-riscos-no-4-2018.pdf. Acesso em: 22 jun. 2022.

UNITED STATES. Department of Justice. **Evaluation of Corporate *Compliance* Programs**. [*S. l.*], June 2020. Disponível em: https://www.justice.gov/criminal-fraud/page/file/937501/download. Acesso em: 13 set. 2022.

VALENTE, Fernanda. STF barra MP que previa compartilhamento de dados pessoais com IBGE. **Consultor Jurídico**, São Paulo, 7 maio 2020. Disponível em: https://www.conjur.com.br/2020-mai-07/stf-barra-mp-previa-compartilhamento-dados-pessoais-ibge. Acesso em: 11 set. 2022.

VERDÉLIO, Andreia. Brasil gasta 3,8% do PIB em saúde pública. **Agência Brasil**, Brasília, 1 nov. 2018. Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2018-11/brasil-gasta-38-do-pib-em-saude-publica. Acesso em: 4 nov. 2021.

WARREN, Samuel D.; BRANDEIS, Louis D. Right to Privacy. **Harvard Law Review**, Boston, v. 4, n. 5, p. 193-220, Dec. 1890. Disponível em: https://www.cs.cornell.edu/~shmat/courses/ cs5436/warren-brandeis.pdf?. Acesso em: 16 jun. 2021.

WORLD BANK WDI 2.12 - Health Systems. *In:* KAGGLE. [*S. l.*], 2020. Disponível em: https://www.kaggle.com/danevans/world-bank-wdi-212-health-systems. Acesso em: 4 nov. 2021.